Thy Brother Came with Subtlety: How a Cause of Action Against Companies Who Leak Data Can Increase Security in the Digital Age*

I. INTRODUCTION

In the digital age, perhaps more than ever, knowledge is power. The global economy generates a staggering amount of data every year.[1] In 2011, enough data sprang forth from global commerce—1.8 zetabytes—that if the data were a single high-definition movie, that movie would take a person 47 million years to watch.[2] This amount is expected to double every year.[3] Amidst such a large amount of information leaks are inevitable, with some being "personal information" such as a name, social security number, driver's license, a bank or credit account number, medical information, or health insurance information.[4] The data flood is everywhere and the levies cannot hold. When personal data is leaked, that victim should, in limited circumstances, have a remedy against the company that allowed the leak to happen.

Such data leaks are becoming commonplace. On New Years Day 2014, users of the smartphone application—commonly referred to as an "app"—Snapchat,[5] woke to the news that phone numbers and usernames associated

* *Matthew Moriarty*. J.D. Candidate 2014, University of Kansas School of Law; M.S.J. Candidate 2014, University of Kansas William Allen White School of Journalism and Mass Communication; B.A. 2001, University of North Carolina at Chapel Hill. I would like to thank Professor William E. Westerbeke for his valuable feedback, encouragement, and time in developing this comment. And thank you to Professor M.A. (Mike) Kautsch for his assistance and time in nourishing and shaping a vague idea into a workable thesis. Thanks also to *The University of Kansas Law Review* board and staff for their countless hours of work. Finally, thank you to my family for their endless support through the years and for making me laugh.

1. *Demystifying Big Data: A Practical Guide to Transforming the Business of Government*, TECHAMERICA FOUND. FED. BIG DATA COMM'N 9 (Oct. 3, 2012), http://www.techamerica.org/Docs/fileManager.cfm?f=techamerica-bigdatareport-final.pdf.

2. *Id.*

3. *Id.*

4. *See, e.g.*, CAL. CIVIL CODE § 1798.29(g)(1)–(5) (West 2012) (defining personal information in a data breach notification law).

5. Snapchat is an application that allows users to send photographs to other users that may be seen for only a limited amount of time.

with 4.6 million accounts had been leaked.[6] A few weeks earlier, the retail giant Target announced a leak of credit card and other information that may affect up to 110 million customers.[7] In February 2013, in response to the suicide of Internet activist Aaron Swartz, the hacker-activist group known as Anonymous hacked into the Federal Reserve Web site and posted online personal information about bank executives including login information, credentials, IP addresses, and contact information.[8] A few months earlier, the group claimed it had hacked the laptop of an FBI agent and gained access to the personal data of over 1 million Apple users.[9] Though the FBI disputed the claim,[10] the news sent chills down the spines of millions of iPhone, iPad, iMac, and iTunes users worldwide. A small Florida publishing company called Blue Toad that creates apps for Apple products revealed that it was likely the unwitting source of the information gained by Anonymous.[11] Many app developers use Apple's Unique Device Identifiers (UDIDs) to help keep track of their users, and Blue Toad is no different.[12] Blue Toad believed that hackers gained access to servers where the company stored customer information, including the UDIDs, and stole the information.[13] Anonymous used the data to accuse—falsely, it appears—the

6. Brian Fung, *A Snapchat Security Breach Affects 4.6 Million Users. Did Snapchat Drag Its Feet on a Fix?*, WASH. POST (Jan. 1, 2014, 11:16 AM), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix.

7. *See* Tiffany Hsu, *Target Traces Data Breach to Credentials Stolen From Vendor*, L.A. TIMES (Jan. 29, 2014, 4:02 PM), http://www.latimes.com/business/money/la-fi-mo-target-data-breach-vendor-20140129,0,8026.story#axzz2sGkyx68S (reporting that cyberthieves accessed information from as many as 40 million credit cards and names, addresses, and email addresses of another 70 million customers).

8. Andres Jauregui, *Anonymous OpLastResort Claims Hack on Government Site, Posts 4,000 Bank Exec Credentials*, HUFFINGTON POST (Feb. 4, 2013, 2:25 PM), http://www.huffingtonpost.com/2013/02/04/anonymous-oplastresort-hacks-government-posts-bank-credential_n_2615605.html.

9. Matthew Shaer, *Apple, FBI Play Down Alleged Anonymous Hack*, CHRISTIAN SCIENCE MONITOR (Sept. 5, 2012), http://www.csmonitor.com/Innovation/Horizons/2012/0905/Apple-FBI-play-down-alleged-Anonymous-hack.

10. *Id.*

11. Nicole Perlroth, *Company Says It, Not F.B.I., Was Hacking Victim*, N.Y. TIMES (Sept. 10, 2012), http://www.nytimes.com/2012/09/11/technology/company-says-it-not-fbi-was-hacking-victim.html?_r=0; Kerry Sanders & Bob Sullivan, *Exclusive: The Real Source of Apple Device IDs Leaked by Anonymous Last Week*, REDTAPE CHRONICLES ON NBCNEWS (Sept. 10, 2012, 9:00 AM), http://redtape.nbcnews.com/_news/2012/09/10/13781440-exclusive-the-real-source-of-apple-device-ids-leaked-by-anonymous-last-week?lite.

12. *See* Sanders & Sullivan, *supra* note 11 (explaining that researchers discovered during 2011 that many app developers use Apple's UDIDs to keep track of users).

13. *Id.*

federal government of spying on its own citizens.[14] Anonymous uses data leaks to make political statements, but as far as is known, they have yet to visit actual harm on anyone, such as by using that personally identifiable information to steal a person's identity.

Journalist Jeff Jarvis believes that advancing technology is requiring society to answer questions it may not yet be prepared to answer.[15] He wrote: "Technology is forcing us to question centuries-old assumptions about the roles of the individual and society: our rights, privileges, powers, responsibilities, concerns, and prospects."[16] In the legal world, courts on every level are struggling with how to apply existing law to new and ever-changing technology.[17] For example, a judge in the U.S. District Court for the Eastern District of Pennsylvania recently tossed out most of a suit filed by a former employee over a LinkedIn[18] account.[19] The fired employee discovered the day after her firing that the company had accessed her LinkedIn account, changed the password, and replaced her name and photograph with those of her replacement.[20] She claimed that the company violated federal computer hacking laws by transferring the profile to her replacement.[21] However, after dismissing the federal claims, the court chose to use its supplemental jurisdiction to hear the plaintiff's state law claims, including one for conversion, indicating on some level that a LinkedIn account may be property.[22] In another instance of a court grappling with

14. *Id.* Ironically, Anonymous could support this position fairly easily without relying on false accusations. *See* Mike Masnick, *The U.S. Government Today Has More Data on the Average American Than the Stazi Did on East Germans*, TECHDIRT (Oct. 3, 2012, 1:13 PM), http://www.techdirt.com/articles/20121003/10091120581/us-government-today-has-more-data-average-american-than-stasi-did-east-germans.shtml.

15. JEFF JARVIS, PUBLIC PARTS: HOW SHARING IN THE DIGITAL AGE IMPROVES THE WAY WE WORK AND LIVE 9 (Simon & Schuster eds., 1st ed. 2011).

16. *Id.*

17. *See* Mike Tolson, *Chief Justice Roberts: Technology Among Top Issues for Court*, HOUSTON CHRONICLE (Oct. 17, 2012, 11:22 PM), http://www.chron.com/news/houston-texas/houston/article/Chief-Justice-Roberts-Court-not-so-politicized-3957626.php (reporting on an informal chat by U.S. Supreme Court Chief Justice John Roberts at Rice University concerning some of the most difficult issues facing the Court).

18. LinkedIn is an online social networking Web site designed to cater to professionals. It bills itself as "the world's largest professional network on the Internet in over 200 countries and territories." *See* LINKEDIN, www.linkedin.com/about-us (last visited Mar. 25, 2014).

19. Eagle v. Morgan, No. 11-4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013); Debra Cassens Weiss, *Judge Tosses Fired Employee's Computer Hacking Claim Over Takeover of Her LinkedIn Account*, A.B.A. J. (Oct. 10, 2012, 5:15 AM), http://www.abajournal.com/news/article/judge_tosses_fired_employees_computer_fraud_claim_over_takeover_linkedin.

20. Eagle v. Morgan, No. 11-4303, 2012 WL 4739436, at *1-2 (E.D. Pa. Oct. 4, 2012).

21. *Id.*

22. *Id.* at *9.

technological issues, the judge in the high-profile Treyvon Martin murder case ruled in 2012 that she would not issue a gag order to prevent the defendant's counsel from using social media and blogging to comment on the case.[23] It is no wonder that U.S. Supreme Court Chief Justice John Roberts has said that technology and its application to the law is one of the most difficult issues facing the Court today.[24]

Meanwhile, companies have long seen the utility of gathering knowledge about their customers.[25] They collect data such as names, addresses, credit card numbers, usernames, passwords, and even Social Security numbers for a variety of reasons, sometimes even to create revenue.[26] Companies like BlueKai, Rapleaf, Invidi, and eXelate are adept at measuring clicks, swipes, mouseovers, and voice commands through the use of digital tracking tools, such as cookies, for the purpose of selling that information to other companies.[27] This information has value not just to the company holding it, but also to those seeking information about potential customers. For instance, if a small business owner wanted to figure out the best place to open a new pet store, the owner could buy a marketing report about a designated area. The report might reveal which city blocks get the most foot or car traffic from people whose Web browsing history reveals that they own pets.[28]

As technology improves, companies gather more and more information. For example, IBM owns a patent on a system using radio-frequency identification (RFID) technology that would begin collecting data on a customer the moment they enter a store,[29] the idea apparently being that

23. Rene Stutzman, *Judge Denies Gag Order in George Zimmerman Murder Case*, ORLANDO SENTINEL (Oct. 29, 2012, 6:05 PM), http://www.orlandosentinel.com/news/local/trayvon-martin/os-george-zimmerman-gag-order-decision-20121029,0,813572.story.

24. Tolson, *supra* note 17.

25. *See, e.g.*, *New Internet, Mobile Technologies and Impact on Public Policy: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of the H. Comm. on the Judiciary*, 112th Cong. (2012) (statement of Chris Babel, Chief Executive Officer of TRUSTe), *available at* 2012 WL 2314267 (testifying before Congress that "[t]oday's companies are racing ahead to harness the aggregate power of vast databases of personal data. Personal data is a critical asset for businesses and leveraging that data can yield tangible benefits for both business and consumers. For example, by leveraging its clinical and cost data, Kaiser Permanente was able to attribute 27,000 deaths to Vioxx and pull the drug off the market.").

26. *See* David Goldman, *Your Phone Company Is Selling Your Personal Data*, CNN MONEY (Nov. 1, 2011, 10:14 AM), http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm (explaining how Verizon Wireless recently changed its privacy policy to allow it to sell customer's location, Web browsing, and video watching data).

27. *See* JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH 4–5 (2011).

28. Goldman, *supra* note 26.

29. ROBERT VAMOSI, WHEN GADGETS BETRAY US: THE DARK SIDE OF OUR INFATUATION

rather than wait for a person to scan a customer loyalty card, the RFID can instantly recognize the customer and direct them to discounted or previously purchased items.[30] Such technological improvements, combined with the variety of incentives for the companies, have virtually ensured that customer tracking will only increase.

The practice of gathering all of this information brings up serious privacy concerns.[31] When people are surveyed after being informed of the extent of data mining they have likely been subjected to, they often say they are "creeped out."[32] It engenders distrust in companies and in government, which has allowed this spying to go on.[33] According to Joseph Turow, Robert Lewis Shayon Professor of Communication at the University of Pennsylvania's Annenberg School for Communication, "when companies track people without their knowledge, sell their data without letting them know what they are doing or securing their permission, and then use those data to decide which of those people are targets or waste, we have a serious social problem."[34] Understanding how privacy has changed as a legal concept in modern times is something that has been difficult for courts to sort through.[35] U.S. Supreme Court Justice Sonia Sotomayor intimated in a concurring opinion in 2012 that a person's expectation of privacy might have changed due to advancing technology.[36] She called into question the premise that people have no reasonable expectation of privacy in information voluntarily given to third parties.[37]

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[38]

WITH NEW TECHNOLOGIES 127 (2011).

30. *Id.* at 129.

31. *See generally* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283 (2003) (discussing privacy problems inherent in the digital age).

32. TUROW, *supra* note 27, at 7.

33. *Id.* at 7–8.

34. *Id.* at 7.

35. *See, e.g.*, United States v. Jones, 132 S. Ct. 945 (2012) (discussing a person's reasonable expectation of privacy with regard to Global Positioning System (GPS) tracking).

36. *Id.* at 957 (Sotomayor, J., concurring).

37. *Id.*

38. *Id.*

However, whether these companies are violating a person's expectation of privacy is not the subject of this Comment. Instead, it is concerned that companies possessing this personal data may carelessly create risk. The risk of identity theft naturally follows from data leaks including personally identifiable information. Some commentators have already called for courts to recognize a company's duty to protect customer data.[39] In fact, courts have made minor steps in that direction.[40] This has led some to conclude that protecting data is "no longer just good business practice[,] [i]t is becoming a legal obligation."[41] At a minimum, if companies are going to continue to allow personal information to fall into the wrong hands, it should fall to those companies to make those adversely affected whole.

Nearly every state in the union has enacted notification laws that create an explicit duty that companies must notify customers as soon as they become aware that a data leak has occurred.[42] The intention of the state legislatures may simply be to ensure that those people who have been the victim of a data leak have time to take necessary measures like canceling their credit cards and changing their passwords. But that puts the entire onus on the victim to rectify the situation, ignores the inconvenience and loss to those victims, and does little to encourage companies to protect customer data with these statutes. The recent and continuing data leaks suggest the current statutory framework is insufficient to prevent future leaks.[43] As

39. *See* Derek A. Bishop, Comment, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J. L. COM. & TECH. 7, 25 (2006) (arguing that because data theft has become increasingly foreseeable, companies ought to make it a practice to safeguard customer information in order to avoid liability).

40. *See infra* Part III.B.

41. Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on the Key Legal Trends*, *in* 1 NINTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW 13, 24 (2008).

42. Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 64 n.3 (2011) (noting that "only four states do not have a data breach notification law: Alabama, Kentucky, New Mexico and South Dakota"). *See also* Scott Berinato, *CSO Disclosure Series: Data Breach Notification Laws, State by State*, CSO SECURITY AND RISK (Feb. 12, 2008), http://www.csoonline.com/article/221322/cso-disclosure-series-data-breach-notification-laws-state-by-state (featuring an interactive map of all states that have enacted data breach notification laws).

43. *See* Conor Shine, *Zappos in Damage-control Mode After Computer Security Breach*, LAS VEGAS SUN (Jan. 16, 2012, 4:58 PM), http://www.lasvegassun.com/news/2012/jan/16/zappos-damage-control-mode-after-computer-security (online retailer Zappos.com announced a security breach involving the personal information of 24 million customers); Adam Samson, *LinkedIn Confirms Data Breach*, FOX BUSINESS (June 6, 2012), http://www.foxbusiness.com/technology/2012/06/06/linkedin-investigating-report-major-data-breach (professional networking site LinkedIn admitted to a breach following reports that 6.5 million passwords hit the Internet); *Yahoo Probes Report of Password Security Breach*, INFOSECURITY (July 12, 2012), http://www.infosecurity-magazine.com/view/26945/yahoo-probes-report-of-password-security-breach (Yahoo! responded to claims that a hacker stole e-mails and passwords from Yahoo!

more and more individuals shift their personal information to cloud-based data storage systems,[44] the threat of identity theft or other malicious uses of data shows significant signs of growth.

Courts recognizing a company's duty to protect customer data and imposing liability in limited cases would provide a strong incentive for companies to spend resources on protecting data that could potentially be put to illicit use in the wrong hands. But courts have been reluctant to reach such a holding, as it would expose large companies to massive lawsuits.[45] With the millions of customers affected by such leaks, it is not difficult to imagine a large company going bankrupt due to a single data leak unless the liability is somehow limited. Some have suggested the best answer would be the federal government stepping in and enacting a data breach notification law.[46] However, similar state laws are now ubiquitous[47] and have failed to plug such leaks. Barring an unforeseen event, there simply does not seem to be the political will for Congress to enact a bill that places such a burden on companies.[48] Therefore, the solution should come from the judiciary.

The first step should be for courts to recognize that companies that collect and store personal data of their customers have a duty to protect that data. This finding of an affirmative duty could stem from a special relationship or from finding that the company has undertaken affirmative steps to provide protection as a service.[49] From there, courts should

---

Voices, a software that enables users to post videos and slideshows).

44. *See* Arif Mohamed, *A History of Cloud Computing*, COMPUTER WEEKLY (Mar. 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing (noting that cloud-based computing has been around since the 1960s. J.C.R. Licklider, the man credited by some as the inventor of cloud computing, foresaw it as a way for "everyone on the globe to be interconnected and accessing programs and data at any site, from anywhere[.]"); s*ee, e.g.*, Sean Ludwig, *Cisco: Global Cloud Traffic Will Increase 12-fold by 2015*, VENTUREBEAT (Nov. 29, 2011, 5:00 AM), http://venturebeat.com/2011/11/29/cisco-global-cloud-traffic (estimating that cloud-based computer traffic will increase 12 times by 2015).

45. *See* Shine, *supra* note 43 (online retailer Zappos's data leak affected 24 million customers); Samson, *supra* note 43 (LinkedIn admitted to data breach that affected 6.5 million users).

46. *See* Amanda Draper, Comment, *Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law*, 40 J. MARSHALL L. REV. 681, 697–701 (2007) (arguing that such a law would offer the customer an opportunity to fix the problem while maintaining the company's ability to conduct business).

47. Burdon, *supra* note 42, at 64 n.3.

48. Despite persistent calls for federal legislation, Congress has not passed such a law. In 2005, Microsoft Senior Vice President, General Counsel, and Corporate Secretary Brad Smith recommended in a position paper that the federal government enact privacy legislation to protect consumers. *See* Brad Smith, *Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation*, MICROSOFT (Nov. 2005), https://www.cdt.org/privacy/20051103microsoftprivacy.pdf.

49. *See infra* Part III.C.

recognize a negligence cause of action against companies who allow customers' personal information to leak. However, courts should limit liability in several ways. First, courts should avoid a problem of unlimited liability by requiring the plaintiff to make a showing of actual harm—such as theft of identity—and that the data leak is the proximate cause of the harm.[50] Courts should further limit the liability by applying a reasonableness standard that protects those companies making reasonable efforts to secure the sensitive customer data.[51] Part II of this Comment will discuss the crime of identity theft, how it has changed in the modern era, and how the law has attempted to adapt along the way. Part III will discuss the reasons why courts should recognize a duty to protect data and how courts can limit the cause of action by requiring only reasonable efforts on behalf of the business and proof of actual harm by the plaintiff.

II. BACKGROUND

A. History

"And he said, Thy brother came with subtlety, and hath taken away thy blessing."[52] Isaac, son of Abraham, spoke those words in the Holy Bible, to Esau following what some call the first documented instance of identity theft.[53] The story goes: Jacob, seeking the blessing of the firstborn, with the help of his mother, covered his hands and neck with ram skins so as to resemble the hairy Esau.[54] He visited his blind father on his deathbed pretending to be the firstborn Esau.[55] Isaac blessed Jacob saying, "Let people serve thee, and nations bow down to thee: be lord over thy brethren, and let thy mother's sons bow down to thee: cursed *be* every one that curseth thee, and blessed *be* he that blesseth thee."[56] Thereafter, Jacob became Isaac's primary heir, and Esau was left to swear revenge.[57]

Identity thieves today use some of the same tactics. They strike with subtlety and deception to fool people into giving them what rightfully

50. *See infra* Part III.F.

51. *See infra* Part III.E.

52. *Genesis* 27:35 (King James).

53. Jake Stroup, *A Brief History of Identity Theft: How We Got Where We Are*, ABOUT.COM, http://idtheft.about.com/od/identitytheft101/a/A-Brief-History-Of-Identity-Theft.htm (last visit Mar. 19, 2014).

54. *Genesis* 27:16 (King James).

55. *Id.* at 18–19.

56. *Id.* at 29.

57. *Id.* at 1–37.

belongs to another. Identity thieves use others' personal information to allow them to commit a variety of illegal acts, usually fraud.[58] Assistant United States Attorney Sean B. Hoar defines identity theft as the theft of information such as a name, date of birth, Social Security number, or credit card number.[59] Identity theft is estimated to be one of the fastest growing crimes in the country.[60] The Federal Trade Commission (FTC) said that forty-two percent of its complaints filed during the year 2000 had to do with identity theft.[61] A 2003 FTC study estimated that 9.9 million Americans had personal information stolen in 2002 and found an exponential increase in information theft between 2000 and 2002.[62]

Despite the ever-growing threat, people are voluntarily putting more and more of their personal information online because of the tremendous benefits that can await those willing to disregard privacy in favor of sharing.[63] Journalist Jeff Jarvis wrote: "Because I am public, I have made new friends and reconnected with old ones. I have received work and made money—including this book and the last. I have tested ideas, spread those ideas, and gotten credit (and blame)."[64] It's not just outgoing young Americans putting information online, though they are on the forefront of the movement.[65]

> All around the world, we are already living increasingly public lives, sharing our thoughts, photos, videos, locations, purchases, and recommendations on Facebook, Twitter, Flickr, YouTube, Foursquare, and platforms offered by other companies in the sharing industry. These people aren't sharing all this because they're reckless exhibitionists, mass narcissists, senseless drunks (well, not usually), or insane. They are doing it for a reason: They realize rewards from being

58. *See* Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1429 (2001) (discussing the adoption of the Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a)(7), designed to prevent "fraudulent creation, use, or transfer of identification documents" and the theft or criminal use of personal information).

59. *Id.* at 1423.

60. *Id.* at 1423–24.

61. *Id.*

62. Jennifer Lynch, Note, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 261 (2005) ("Identity theft is one of the fastest growing crimes in the United States. A broad survey commissioned by the Federal Trade Commission (FTC) in September 2003, estimated that 9.9 million Americans had had their personal information stolen in the prior year, collectively costing businesses $47.6 billion and consumers $5.0 billion.").

63. *See* JARVIS, *supra* note 15, at 1–4.

64. *Id.* at 2–3.

65. *Id.* at 8.

open and making the connections technology now affords.[66]

Meanwhile, companies are gathering, creating, and using more data than ever.[67] The advertising industry is "guiding one of history's most massive stealth efforts in social profiling."[68] It includes computers, networks, and software "as well as the *data*, *messages*, *and information* that is typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems."[69] The information companies' collection includes "financial information, personal information, tax-related records, employee information, transaction information, and trade secret and other confidential information."[70]

Many companies have begun to engage in the process known as data mining, either in-house or by hiring data brokers.[71] Data mining is the process of gathering, analyzing, and sharing an Internet user's online and offline behaviors, including purchasing records and tastes.[72] For an example of how data mining works and how quickly the information gathered can be put to work, look no further than the 2012 presidential election. A community college student and supporter of President Barack Obama told the New York Times that after visiting mittromney.com, he almost immediately started seeing advertisements on other Web sites asking him to donate money to Mitt Romney's campaign.[73] Turow has written that although many people may actually enjoy being targeted for advertising, there should be concern over the intrusion.[74] "Every day most if not all Americans who use the [I]nternet, along with hundreds of millions of other users from all over the planet, are being quietly peeked at, poked, analyzed, and tagged as they move through the online world."[75]

66. *Id.* at 9.

67. *See* Smedinghoff, *supra* note 41, at 19 ("[I]n today's business environment, virtually all of a company's daily transactions and all of its key records are created, used, communicated, and stored in electronic form using networked computer technology.").

68. TUROW, *supra* note 27, at 1.

69. Smedinghoff, *supra* note 41, at 27.

70. *Id.*

71. *See* Natasha Singer, *The Data-Mining Industry Kicks Off a Public Relations Campaign*, N.Y. TIMES BITS BLOG (Oct. 15, 2012, 11:00 AM), http://bits.blogs.nytimes.com/2012/10/15/the-data-mining-industry-kicks-off-a-public-relations-campaign/.

72. *Id.*

73. Natasha Singer & Charles Duhigg, *Tracking Voters' Clicks Online to Try to Sway Them*, N.Y. TIMES (Oct. 27, 2012), http://www.nytimes.com/2012/10/28/us/politics/tracking-clicks-online-to-try-to-sway-voters.html?ref=politics&_r=0.

74. TUROW, *supra* note 27, at 1–2.

75. *Id.* at 2.

Companies, unlike political campaigns, often gather all of this data in order to reduce costs and increase productivity.[76] When a company collects information on customers, it now stores that information in a database on a server.[77] It "greatly enhances the potential for unauthorized access, use, disclosure, and alteration" of customer data.[78] A hacker who gains access to that database suddenly might have enough information to steal hundreds of thousands of identities, or to sell that information to others who might seek to do so. Several large, high-profile data leaks have occurred in the past several years.[79] In response, the victims of such data leaks are alleging that they have a cause of action against the companies in the possession of such data and are filing complaints seeking damages.[80] The lawsuits allege that the named company had a duty to protect the data and that the company acted negligently by releasing it or failing to prevent thieves from accessing it.[81] Although these lawsuits raise questions of statutory and contract law, the primary focus of this Comment is the claim that the companies have a common law duty to protect customers' personal information.

B. Identity Theft in the Digital Age

Since the advent of the Internet, identity theft has gone high-tech. Not so long ago, people could reliably combat identity theft by taking such simple steps as shredding their credit card statements before disposing of them.[82] Identity thieves dove into dumpsters, stole purses or wallets, or opened mail before owners could check their mailboxes.[83] Thieves today

76. Smedinghoff, *supra* note 41, at 19.

77. *See Crunching the Numbers: Banks Know a Lot More About Their Customers. That Information May be Valuable in More Ways Than One*, THE ECONOMIST (May 19, 2012), http://www.economist.com/node/21554743 (taking an in-depth look at how companies are attempting to handle and use the massive amounts of data they collect and store in databases).

78. Smedinghoff, *supra* note 41, at 19.

79. Snapchat leaked 4.6 million users' contact information in 2014. Fung, *supra* note 6. Target's security breach compromised 40 million customers' credit card information in 2013. Hsu, *supra* note 7. In 2012, Zappos.com, LinkedIn, and Yahoo.com all experienced breaches impacting millions of customers or users. *See* Shine, *supra* note 43; Samson, *supra* note 43; *Yahoo probes report of password security breach*, *supra* note 43.

80. *See, e.g.*, Complaint, Szpyrka v. LinkedIn Corp., No. CV 12 3088 HRL, 2012 WL 2169325 (N.D. Cal. June 15, 2012); Complaint, Lawrence v. Zappos.com, Inc., No. 3_12CV00355, 2012 WL 2839874 (D. Nev. Jan. 26, 2012).

81. Complaint, Szpyrka, *supra* note 80; Complaint, Lawrence, *supra* note 80.

82. *See, e.g.*, *What to Shred and When to Shred it*, BETTER BUSINESS BUREAU (Apr. 8, 2008), http://canton.bbb.org/article/what-to-shred-and-when-to-shred-it-4210 (giving tips on what documents to shred to help avoid identity theft).

83. Stephanie Byers, Note, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141, 143 (2001).

often use techniques like watching people enter their credit card numbers into a phone, pretexting—which is either calling a financial institution pretending to be a customer or calling a person pretending to be a financial institution—or simply becoming an employee of a large company that tracks consumer data, such as a bank.[84]

The digital age has only increased the avenues potential identity thieves may use to gather a person's information. A recent study by Miniwatts Marketing Group found that Internet usage grew during the last eleven years by over 100% in every region on the planet, with the most dramatic growth found in Africa (2,988.4%) and the Middle East (2,244.8%).[85] The slowest growing area, North America, still grew by 152.6%.[86] Meanwhile, the threat so-called "cyber criminals" pose to the private sector continues to grow.[87] A firm that specializes in anti-malware believes that 2011 was the worst year ever for security breaches.[88] Malware refers to harmful computer programs like viruses, Trojan horses, tracking software, etc. Nevertheless, people put more and more of themselves online.[89] Industry experts expect cloud-based computing to grow exponentially in the next three years,[90] but, security is not growing nearly as fast. A 2011 survey found that 66% of businesses have not implemented any data-loss prevention tools.[91] Considering the rise

84. *See* Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 MARQ. L. REV. 847, 850–51 (2005) ("The rise in identity theft has occurred in a large part because of the increased sophistication and anonymity of identity thieves.").

85. INTERNET WORLD USAGE AND POPULATION STATISTICS, http://www.internetworldstats.com/stats.htm (last visited Mar. 20, 2014). The Miniwatts Marketing group compared data on Internet usage published by Nielsen Online, the International Telecommunications Union and other sources with census data in order to come up with its figures. *Id.* Miniwatts Marketing Group is a Limited Liability Company formed in 1997 to research Internet use for marketing purposes. MINIWATTS MARKETING GROUP, http://www.miniwatts.com/about_us.htm (last visited Mar. 20, 2014).

86. INTERNET WORLD USAGE AND POPULATION STATISTICS, http://www.internetworldstats.com/stats.htm (last visited Mar. 20, 2014).

87. *See Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism*, Statement Before the Subcomm. on Crime and Terrorism of the S. Judiciary Comm., 112th Cong. (Apr. 12, 2011), (statement of Gordon M. Snow, Asst. Dir., Cyber Division, Federal Bureau of Investigation), *available at* http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism ("Cyber criminal threats to the U.S. result in significant economic losses.").

88. *Privacy Violations Biggest Security Threat in 2012*, PANDALABS (Dec. 15, 2011), http://press.pandasecurity.com/news/privacy-violations-biggest-security-threat-in-2012-reports-pandalabs/.

89. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (noting that "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"); *see* JARVIS, *supra* note 15, at 1–4 (2011).

90. Ludwig, *supra* note 44.

91. Survey, *Plugging the Data Leaks: 2011 Global Information Security Survey*, ERNST &

of online "hacktivists" such as Anonymous, coupled with the ever-increasing number of Internet users as well as the increasing number of those users who use cloud-based data storage services, the potential for data abuse seems to only be growing.

Skilled identity thieves use a number of techniques to gain access to personal information. Packet sniffing, for example, is the practice of intercepting traffic on a network.[92] The information gained can lead to identity theft.[93] People using free WiFi might be putting themselves at risk of identity theft because public connections are less secure than those protected by password.[94] In fact, unprotected wireless signals are a boon to those looking to steal identities.[95] Though most Web sites use encryption software to keep credit card numbers safe, hackers can use cookies (tracking software) to get access to information—like credit card numbers or bank account numbers and passwords—even though you might think you are entering it into a secure Web site.[96] Another way identity thieves gain access to information is through the use of a key-logger, software that records keystrokes.[97] If a thief successfully manages to install a key-logger on a computer, the thief can record any keystroke desired from that computer.[98]

Encrypted information also may not be as secure as most people presume. Thanks to advances in computing power, "an individual with a modern dual-core processor in a Dell laptop, loaded with the right software, can defeat a twenty-year-old encryption algorithm not in a matter of days but in a matter of minutes."[99] Even the federal government is not immune. Identity thieves are skilled at filing fraudulent tax returns.[100] Last year, the

---

YOUNG (2011), http://www.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey—-Plugging-the-data-leaks.

92. *Visa Data Security Alert: Top Vulnerability—Packet Sniffing*, VISA (Feb. 2, 2009), http://usa.visa.com/download/merchants/20090202_packet_sniffing.pdf.

93. *Id.*

94. Analisa Nazareno, *How Free Wi-Fi Can Put You at Risk*, MSN MONEY (Nov. 8, 2011, 2:31 PM), http://money.msn.com/identity-theft/how-free-wi-fi-can-put-you-at-risk-credit-cards.aspx.

95. *See* VAMOSI, *supra* note 29, at XVII (explaining the ease with which a wireless signal can be cloned: "With no authentication and often with little or no encryption, or with trivial encryption, I can become you without ever coming into physical contact with you or your papers or effects.").

96. *Id.*

97. Charlie Sorrel, *DIY Key-Logger Kit Lets You Spy From Afar*, WIRED GADGET LAB BLOG (July 23, 2009, 5:05 AM), http://www.wired.com/gadgetlab/2009/07/diy-key-logger-kit-lets-you-spy-from-afar.

98. *See id.* (discussing the ease with which a key-logger can be installed if a person has physical access to the computer).

99. VAMOSI, *supra* note 29, at XIV.

100. Blake Ellis, *IRS Pays Billions in Refunds to Identity Thieves*, CNN MONEY (Aug. 2, 2012,

Internal Revenue Service paid out $5.2 billion in refunds to potentially fraudulent tax returns.[101] Identity thieves can file thousands of tax returns just with a fake address—an audit conducted by the Treasury Inspector General for Tax Administration found that the same Lansing, Michigan, address was used on 2,137 different tax returns.[102]

C. How the Law Has Responded

In an attempt to plug these leaks, most state legislatures have enacted breach notification laws. According to the National Conference of State Legislatures, forty-six states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands all have data notification laws.[103] Only Alabama, Kentucky, New Mexico, and South Dakota have yet to enact such laws.[104] California was the first state to enact such a statute in 2002 and it has become something of a model.[105] It requires companies to disclose any breach of computerized data if it includes personal information reasonably believed to have been acquired by an unauthorized person.[106] It defines "personal information" as a person's first name, or first initial, in combination with the person's last name and one of the following: social security number, driver's license, an account number, medical information, or health insurance information.[107]

The majority of states follow the California model.[108] However, some laws are less specific on how they impose security obligations. Take, for example, the Uniform Electronic Transactions Act—proposed by the National Conference of Commissioners on Uniform State Laws and adopted by every state except New York, Illinois, and Oregon—a law intended to provide some guidance for businesses conducting transactions with e-signatures.[109] Some view this law as the beginning of a patchwork of laws

---

5:41 PM), http://money.cnn.com/2012/08/02/pf/taxes/irs-identity-theft/index.htm.

101. *Id.*

102. *Id.*

103. *State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Aug. 20, 2012), http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

104. *Id.*

105. CAL. CIV. CODE § 1798.29 (West 2012).

106. *Id.* § 1798.29(a).

107. *Id.* § 1798.29(g)(1)(A)–(E).

108. *See* Berinato, *supra* note 42.

109. *Uniform Electronic Transactions Act*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/uniform-electronic-transactions-acts.aspx. (last visited Mar. 20, 2014).

that will together impose a duty to keep data secured.[110] However, what the law really does is tell companies how to satisfy the requirement to keep a record of an electronic transaction when another law requires such a record to be kept.[111] It is an area of the law where confusion reigns.

In response, commentators have called for the federal government to enact an overarching data leak notification law.[112] Some federal laws do require a company or organization to provide security for the information they possess. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was the first federal law to require healthcare providers to secure information belonging to their patients, who are essentially their customers.[113] Three years later, Congress passed the Gramm-Leach-Bililey Act (GLB), which placed regulations upon financial businesses.[114] It imposes upon every financial institution "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[115] Each of these laws was followed by security regulations—GLB in 2001 and HIPAA in 2003—that instruct companies how to implement the security provisions of the acts.[116]

In addition, in 2002, the FTC began filing enforcement actions against companies for allegedly failing to provide adequate security for information.[117] When Congress created the FTC in 1914, it empowered the commission to prevent persons, partnerships, and corporations (but not banks or credit unions) from engaging in unfair or deceptive trade practices.[118] The theory behind the enforcement actions against companies for failing to provide security for personal information was that companies claimed to be able to secure data and were therefore engaged in deceptive trade practices[119]—an argument that has also frequently arisen in recent

110. Smedinghoff, *supra* note 41, at 21.

111. *See, e.g.*, CAL. CIV. CODE § 1633.12(a) (West 2000).

112. Amanda Draper, Comment, *Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law*, 40 J. MARSHALL L. REV. 681, 702 (2007).

113. 42 U.S.C. § 1320d-2 (1996).

114. 15 U.S.C. § 6801 (1999).

115. *Id.*

116. Smedinghoff, *supra* note 41, at 24–25.

117. *See, e.g.*, Sunbelt Lending Servs., Inc., No. C-4129 (F.T.C. 2005), *available at* http://www.ftc.gov/os/caselist/0423153/050107do0423153.pdf; MTS, Inc., d/b/a Tower Records/Books/Video, No. C-4110 (F.T.C. 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf; Guess?, Inc., No. C-4091 (F.T.C. 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf.

118. 15 U.S.C. § 45(a)(1)–(2) (2006).

119. Smedinghoff, *supra* note 41, at 24–25.

class action suits.[120] In June 2005, the FTC began claiming that a failure to provide adequate security was an *unfair* trade practice, even in the absence of any false representation as to the company's security prowess.[121] Some have seen this as a significant widening of the FTC's scope of enforcement.[122]

The law internationally has developed at a faster rate than the law in America. In Europe, the European Union Data Protection Directive mandates that all companies possessing personal information have a general duty to protect it.[123] Article 17(1) of the Directive tells Member States that they must adopt legislation that requires those who control data to protect it:

> Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[124]

Other countries—like Canada, Japan, Argentina, South Korea, Hong Kong, and Australia—have also chosen to impose a duty on companies to protect customer data.[125]

Some United States courts have recognized something like a duty to protect consumer data, leading some commentators to believe that the trend in the law is headed toward courts generally recognizing the duty.[126] For

120. *See, e.g.*, Complaint, *Szpyrka*, *supra* note 80; Complaint, *Lawrence*, *supra* note 80.

121. Complaint at 3, CardSystems Solutions, Inc., No. C-4168, (F.T.C. 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf; Complaint at 3, DSW Inc., No. C-4157, 3 (F.T.C. 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf; Complaint at 9, United States v. ChoicePoint, Inc., 1:06-CV-0198, (F.T.C. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf; Complaint at 3, BJ's Wholesale Club, Inc., No. C-4148, (F.T.C. 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

122. Smedinghoff, *supra* note 41, at 25–26.

123. Council Directive 95/46/EC, art. 17(1) (1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT (last visited Mar. 20, 2014).

124. *Id.*

125. Smedinghoff, *supra* note 41, at 28–29.

126. *Id.* at 20.

example, the Michigan Court of Appeals found in 2005 that a union owed a duty to protect the personal information of its members.[127] In *Catsouras v. Department of California Highway Patrol*, the California Court of Appeals found a somewhat similar duty when it said that Highway Patrol officers owed a duty to the family of an accident victim not to post graphic pictures of the deceased online for "lurid titillation."[128] A Minnesota court also allowed a company to concede that, because of its own policies, the company owed customers a duty of reasonable care with information.[129] A United States district court in Tennessee found in an identity theft case that a financial institution owed a duty to verify the "authenticity and accuracy" of an application for a credit card when injury is foreseeable and preventable.[130] Finally, a bankruptcy court has found that the security of data is important when considering whether an electronic record will be admissible.[131]

The proliferation of data leaks along with the growing belief that companies owe a duty to protect that information has led to the rise of large class-action lawsuits seeking damages. On April 28, 2009, a Starbucks employee filed suit against the company on behalf of a class alleging "failure to adequately safeguard its employees' sensitive, personal information, including social security numbers."[132] The lawsuit involved the theft of one laptop that contained information on approximately 97,000 employees.[133] The complaint contended that it is now industry standard to encrypt such data and that the company's "failure to maintain reasonable and adequate security procedures to protect against the theft of . . . [personally identifiable information] has put Plaintiff and the proposed Class Members at an increased and imminent risk of becoming victims of identity theft

127. Bell v. Mich. Council 25 of Am. Fed'n of State, Cnty, Mun. Emps., AFL-CIO, Local 1023, No. 246684, 2005 WL 356306, at *5 (Mich. Ct. App. Feb. 15, 2005) ("[D]efendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information, information which could be easily used to appropriate a person's identity.").

128. 104 Cal. Rptr. 3d 352, 376 (Cal. Ct. App. 2010).

129. *See* Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *3 (D. Minn. Feb. 7, 2006) (the company conceded that its own policy required it to use reasonable care).

130. Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) ("Because the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, the Court finds that under Tennessee negligence law, Defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card.").

131. *In re* Vee Vinhnee, 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005).

132. Complaint at ¶1, Lalli v. Starbucks Corp., No. C09-00389 (RAJ), 2009 WL 5072589 (W.D. Wash. 2009).

133. *Id.* at ¶83.

crimes, fraud, and abuse."[134] The complaint alleged that Starbucks had a common law duty to protect its employees' personal information and by not conforming to industry standards, it breached that duty.[135]

In early 2012, a Zappos.com (Zappos) customer filed a class-action suit against the online retailer in response to a hack that may have exposed partial credit card numbers of 24 million customers.[136] The suit alleged that Zappos owed a duty to keep customer information "in a safe and secure condition" away from the threat of unknown third persons.[137] It recently survived a motion to compel arbitration, filed by Zappos, along with co-defendant Amazon (the world's largest online retailer),[138] based on an arbitration clause in the Zappos Terms of Use.[139] Ultimately, because the agreed upon arbitration Terms of Use was illusory and a "highly inconspicuous link buried in a sea of links," the court found that the Terms of Use failed to provide notice. As a result, the judge refused to compel arbitration.[140]

In 2012, a user of the online professional networking Web site LinkedIn filed a class-action complaint against that company following a data leak of approximately 6.5 million customers' information, including e-mail addresses, passwords, and log-in credentials.[141] Like the Starbucks complaint, this complaint also alleged that a company possessing personal data failed to comply with industry protection standards.[142] The complaint included several causes of action, one being negligence or gross negligence.[143] It reads: "By agreeing to accept Plaintiff and the other Class and SubClass members' sensitive [personally identifiable information], Defendant assumed a duty, which required it to exercise reasonable care to secure and safeguard that information and to utilize industry standard protocols and technology to do so."[144]

In response to the threat of leaving data unsecured, many companies had

134. *Id.* at ¶6.

135. *Id.* at ¶¶46–54.

136. Complaint, *Lawrence*, *supra* note 80, at ¶18.

137. *Id.* at ¶51.

138. Danielle Kucera, *Amazon Shares Rise on Operating Loss Below Estimates*, BLOOMBERG (Oct. 26, 2012, 3:18 PM), http://www.bloomberg.com/news/2012-10-25/amazon-posts-loss-as-livingsocial-stake-loses-value.html.

139. *In re* Zappos.com Inc., Customer Data Sec. Breach Litig., 893 F. Supp. 2d 1058, 1064 (D. Nev. 2012).

140. *Id.* at 1066.

141. Complaint, Szpyrka *supra* note 80, at ¶25.

142. *Id.* at ¶¶102–05.

143. *Id.* at ¶¶101–15.

144. *Id.* at ¶103.

already taken it upon themselves to take steps to increase the security of customer data.[145] Some companies have even taken it a step farther and asked the federal government to step in. For example, in a 2005 position paper, Microsoft Senior Vice President, General Counsel, and Corporate Secretary Brad Smith called on the federal government to enact privacy legislation to protect consumers.[146] So far, the federal government has declined to do so.

III. ANALYSIS

Because of the growing threat of identity theft due to data leaks coming from companies, the law must respond in an effective manner. Information security has been called "a time bomb waiting to explode."[147] But the ever-expanding body of law[148] addressing data security has failed to plug the leaks, as evidenced by the fact that in early 2014, retail giant Target announced a leak that may affect up to 110 million customers.[149] The Target leak is one of a number of high-profile data leaks threatening millions of people with harm.[150] In order to address this growing problem, courts should begin recognizing a duty to protect customer data that would allow customers to sue companies for negligence following a breach.

Courts could most effectively do this by: 1) acknowledging that identity theft is a foreseeable result of a data leak or by considering their gathering of data as an undertaking to provide protection, 2) clearly defining what constitutes reasonable efforts to protect data, 3) limiting liability by requiring actual harm, and 4) requiring that the leak be the proximate cause of the harm.

A. The Basics of a Negligence Claim

At its most basic, a complaint that alleges that a party had a duty and failed to adequately perform that duty is a tort action for negligence.[151] The elements of negligence are: 1) the existence of a duty, 2) breach of that duty, 3) said breach caused an alleged injury, 4) and said injury resulted in

145. *See* Smedinghoff, *supra* note 41, at 23–24.

146. Smith, *supra* note 48.

147. Smedinghoff, *supra* note 41, at 19.

148. *Id.* at 21.

149. *See* Hsu, *supra* note 7.

150. Shaer, *supra* note 9; Shine, *supra* note 43; Samson, *supra* note 43; *Yahoo probes report of password security breach*, *supra* note 43.

151. BLACK'S LAW DICTIONARY 1133 (9th ed. 2009) (negligence).

damages.[152] Generally, a legal duty is "the obligation to conform to a standard of conduct under the law for the protection of others against unreasonable risks of harm."[153] The duty to protect consumer data would go beyond this standard because it would impose an affirmative duty to take action to prevent harm from happening. This is rare in tort law.[154] As University of Arizona College of Law professor Dan Dobbs explains:

> Unless the defendant has assumed a duty to act, or stands in a special relationship to the plaintiff, defendants are not liable in tort for a pure failure to act for the plaintiff's benefit. The fact that the defendant foresees harm to a particular individual from his failure to act does not change the general rule.[155]

This general rule has its critics and loopholes. Some have argued, at least, that courts should impose a duty upon people to assist in the case of an emergency.[156] Also, courts are more likely to find an affirmative duty if they find that two parties had a special relationship[157] or that one undertook to render services to another.[158] In addition, courts historically are reluctant to extend negligence law to financial losses.[159]

Negligence actions require that the breach be the legal, or proximate cause as well as the cause-in-fact of the harm.[160] Proximate cause, in a way, is a limit on liability based primarily on foreseeability.[161] Think, for example, of the Butterfly Effect—the theory that the flapping wing of a butterfly on one continent can set off a chain reaction that can alter the weather patterns on another continent and lead to a tornado.[162] There, the butterfly would be the cause-in-fact of the tornado, but would not be legally

152. Rasnick v. Krishna Hospitability, Inc., 713 S.E.2d 835, 837 (Ga. 2011).

153. *Id.*

154. *See* Francis H. Bohlen, *The Moral Duty to Aid Others as a Basis of Tort Liability*, 56 U. PA. L. REV. 217, 219 (1908) (explaining that the law has not recognized a duty to aid the unfortunate).

155. DAN B. DOBBS, THE LAW OF TORTS 853 (2000).

156. Thomas C. Galligan, Jr., *Aiding and Altruism: A Mythopsycholegal Analysis*, 27 U. MICH. J.L. REFORM 439, 520 (1994).

157. RESTATEMENT (SECOND) OF TORTS § 315 (1965).

158. *Id.* § 324A.

159. *See, e.g.*, Tietsworth v. Harley-Davidson, Inc., 677 N.W.2d 233, 241 (Wis. 2004) (applying the economic-loss doctrine, a "judicially-created remedies principle that operates generally to preclude contracting parties from pursuing tort recovery for purely economic or commercial losses" to bar a tort claim).

160. DOBBS, *supra* note 155, at 443.

161. *Id.* at 444.

162. Larry Bradley, *The Butterfly Effect*, CHAOS & FRACTALS (2010), http://www.stsci.edu/~lbradley/seminar/butterfly.html.

held responsible because the tornado is not a foreseeable consequence. An important aspect of proximate cause law is the concept of the superseding cause.[163] When a second actor's unforeseeable action causes an injury, the second actor is solely liable.[164] When the second actor is a criminal, courts may impose a heightened standard of foreseeability.[165] The District of Columbia Court of Appeals explained that "heightened foreseeability factors directly into the duty analysis because a defendant is only liable for the intervening criminal acts of another 'if the criminal act is so foreseeable that a duty arises to guard against it.'"[166] In essence, the law of negligence allows courts flexibility to find a cause of action and tools to limit recovery to those who really deserve it.

B. Recent Case Law Makes It Clear that a Duty to Protect Customer Data Likely Does Not Yet Exist

Most courts have not specifically said that companies have a duty to protect customers' personal data. The Federal District of Nevada came close, however. The court declined to grant summary judgment in the Zappos litigation, finding that the plaintiffs' allegations that Zappos had failed to properly safeguard its customers' personal data sufficiently support the breach element of the plaintiffs' negligence claim.[167] In reaching this determination, the court stated that Zappos owed its customers a duty to act reasonably and prudentially, implying that failure to safeguard customers' personal data could be considered to be unreasonable or imprudent behavior.[168] Other courts have found security of data to be legally important. For example, in *In re Vee Vinhnee*,[169] the Ninth Circuit Bankruptcy Appellate Panel was faced with the problem of determining if a digital business record could be admitted into evidence as an exception to the hearsay rule.[170] The court relied on Professor Edward J. Imwinkelried's eleven-step foundation for determining if a paper record should be

163. DOBBS, *supra* note 155, at 444.

164. *Id.*

165. *See, e.g.*, Bd. of Trs. of Univ. of Dist. of Columbia v. DiSalvo, 974 A.2d 868, 870 (D.C. 2009).

166. *Id.* at 871 (quoting McKethan v. Wash. Metro. Area Transit Auth., 588 A.2d 708, 717 (D.C. 1991)).

167. *In re* Zappos.com, No. 3:12-CV-00325-RJC-VPC, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013).

168. *Id.*

169. 336 B.R. 437 (B.A.P. 9th Cir. 2005).

170. *Id.* at 444.

admissible[171] saying that the ultimate determination for a computerized record would be the same, writing: "[I]t all boils down to the same question of assurance that the record is what it purports to be."[172] The court drew attention to Prof. Imwinkelried's fourth step—"The procedure has built-in safeguards to ensure accuracy and identify errors[]"—saying that the step "warrants amplification" and is "more complex than first appears."[173] The court ultimately upheld the trial court's decision not to allow computer evidence into the record, stating that the declaration included:

> no information regarding American Express' computer policy and system control procedures, including control of access to the pertinent databases, control of access to the pertinent programs, recording and logging of changes to the data, backup practices, and audit procedures utilized to assure the continuing integrity of the records. All of these matters are pertinent to the accuracy of the computer in the retention and retrieval of the information at issue.[174]

Therefore, in paying specific attention to "system control procedures," the court made it clear that the level of security associated with electronic records has legal significance, at least with regard to allowing such records into evidence. The court in essence required a showing of safeguards prior to allowing computerized evidence into the record.[175] Some believe that the level of security around such records will continue to be an important factor in whether they will be admissible.[176] However, though this is evidence that the security level of data will occasionally be of import to courts, it fails to indicate that the Ninth Circuit would be willing to go further and recognize a duty to protect customer data. In fact, the best it can hope to do is give an indication that courts might use Prof. Imwinkelried's test to determine if a company had taken reasonable efforts to secure data.

Though some have claimed that case law on this subject indicates a growing trend toward businesses owing a duty to protect customer data,[177] this is not necessarily the case. In fact, though some courts have taken baby steps in that direction—occasionally mentioning the growing threat of identity theft as part of their decision-making process[178]—they are careful to

171. EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03 [2] (5th ed. 2002).
172. *Vee Vinhnee*, 336 B.R. at 445.
173. *Id.* at 446.
174. *Id.* at 449.
175. *Id.* at 446–47.
176. Smedinghoff, *supra* note 41, at 26.
177. *Id.* at 24.
178. *See* Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) (noting the

point out that their holdings are limited to the facts at hand and seem reluctant to set such a precedent.[179]

The Court of Appeals of Michigan found in *Bell v. Michigan Council* that the union did owe a duty to protect its members from identity theft "by providing some safeguards to ensure the security of their most essential confidential identifying information."[180] The plaintiffs in *Bell*—911 operators employed by the City of Detroit and members of the local union—all were victims of identity theft in 1999.[181] However, the data leak that occurred in *Bell* had nothing to do with the Internet or digital data. There, data thieves gained access to the plaintiffs' Social Security numbers the old fashioned way: an employee's daughter found a notebook with the Social Security numbers of the county's 911 operators.[182] In addition, the court specifically said it was limiting its holding to cases where the defendant knew confidential information was leaving the building and there were no procedures in place to protect that information.[183]

Furthermore, *Bell* does not involve a company. The court found that the union owed a duty, but a union and a member have a different relationship than a company and a customer. The opinion mentioned that membership in the union was essentially mandatory,[184] whereas customers have the choice to do business with any company they so choose. Another factor keeping this case from standing for the assertion that there is a duty to protect customer data is that it is an unpublished opinion, and therefore, not even binding on lower Michigan courts.

The case *Guin v. Brazos Higher Educ. Serv. Corp.*,[185] which some contend stands for the assertion that a duty of care may be established by

---

increase in identity theft and characterizing banks and credit card issuers as "the first, and often last, line of defense in preventing the devastating damage that identity theft inflicts"); Bell v. Mich. Council 25 of the Am. Fed'n of State, Cnty, & Mun. Emps., AFL-CIO, Local 1023, No. 246684, 2005 WL 356306, at *4 (Mich. Ct. App. Feb. 15, 2005) (noting that "[t]he crime of identity theft has been gaining momentum in recent years due to the accessibility of identifying personal information, mainly through computer use").

179. *See, e.g.*, *Wolfe*, 485 F. Supp. 2d at 882 (recognizing a duty but stating that it "merely requires Defendant to implement reasonable and cost-effective verification methods that can prevent criminals, in some instances, from obtaining a credit card with a stolen identity"); *Bell*, 2005 WL 356306, at *5 (limiting its holding to "the facts of this case where defendant knew confidential information was leaving its premises and no procedures were in place to ensure the security of the information").

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

181. *Id.* at *1.

182. *Id.*

183. *Id.* at *5.

184. *Id* at *1.

185. No. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006).

statute,[186] in fact stands for only the assertion that a company can concede that its own policies can create a duty to keep private information confidential.[187] There, a student loan company, Brazos Higher Education Service (Brazos), informed customers that its data might have been compromised. An employee suffered a break-in and a laptop that might have included some sensitive customer data was among the items stolen.[188] Brazos's privacy policy promised to "restrict access to nonpublic personal information to authorized persons who need to know such information."[189] A customer sued Brazos following the data leak, arguing, in part, that Brazos violated a statutory duty created by the GLB Act. However, there was never any indication that he or any other customer experienced any fraud or identity theft as a result of the leak.[190] The company conceded, for the purposes of a summary judgment motion only, that the GLB Act and its own policy required it to provide reasonable care,[191] but argued that it did provide such care.[192] The court agreed, noting that a break-in in a safe neighborhood is not foreseeable.[193] Furthermore, the court pointed out that the customer did not suffer any harm.[194] The court issued summary judgment in Brazos's favor.[195]

So, rather than saying that the company owed the customer a duty because of the GLB Act, the *Brazos* court allowed the company to impose a duty upon itself. The court simply chose not to disagree with the company and examined the rest of the negligence claim, which it quickly disposed of, finding no breach or harm: hardly a ringing endorsement for the existence of a duty to protect consumer information tort.

Even when courts have specifically found a duty to protect customers from identity theft, that duty has not been in regard to the collection, storage, and protection of consumer data. For example, the court in *Wolfe v. MBNA America Bank*[196] found that the bank owed a duty to the plaintiff to verify

186. Smedinghoff, *supra* note 41, at 26.

187. *See Guin*, 2006 WL 288483, at *4 ("Brazos concedes that under this policy, it owed Guin a duty of reasonable care, but argues that it acted with reasonable care in handling Guin's personal information. (citation omitted) The Court agrees.").

188. *Id.* at *2.

189. *Id.* at *4.

190. *Id.* at *2.

191. *Id.* at *4.

192. *Id.*

193. *Id.*

194. *Id.* at *6.

195. *Id.*

196. 485 F. Supp. 2d 874 (W.D. Tenn. 2007).

the authenticity of the information included in a credit card application.[197] The court even cited the increasing risk of identity theft as part of its decision.[198] However, the court stressed that it was not imposing a duty upon the bank to prevent all identity theft.[199] There, the bank issued a credit card to a person using the plaintiff's name but an address where the plaintiff was not living and had never lived.[200] The court said that whether the bank had violated that duty was a question for the trier of fact.[201]

By analogy, one could claim that by recognizing a duty to protect customers in certain situations from identity theft, the *Wolfe* court would also recognize a duty to protect information that could be used for identity theft. However, it seems unlikely that the *Wolfe* court itself would stand behind that proposition. It made sure to specify that it was not imposing a duty on a company to prevent identity theft, saying: "this duty to verify does not impose . . . a duty to prevent all identity theft."[202] It is much more likely that the court was imposing a duty to take some basic steps prior to issuing a credit card. If the company in *Wolfe* had simply checked the address on the application, no identity theft would have occurred.

Thus, security and safeguards surrounding electronic data have become important legal concepts, yet companies probably do not have a legal duty to provide such security or safeguards.

C. The Relationship Between a Company and a Customer May Give Rise to an Affirmative Duty

The general rule that tort law does not require one to take action to prevent harm befalling another is rarely excepted, often only when there is a "special relationship" between the two parties.[203] The classic example of a special relationship is that of parent and child. Parents, the law has long observed, owe a duty to their children to provide a minimum of care.[204] For example, in 1992, the Sixth Circuit found that a surrogacy broker owed an affirmative duty to reduce the risk of harm to the child, surrogate mother,

197. *Id.* at 882.
198. *See id.*
199. *Id.*
200. *Id.* at 878.
201. *Id.* at 882.
202. *Id.*
203. DOBBS, *supra* note 155, at 853–54.
204. *See, e.g.*, Holodook v. Spencer, 324 N.E.2d 338, 342–43 (N.Y. 1974) (discussing the many duties that arise from the parent–child relationship).

and contracting father.[205] The law also recognizes several other relationships that give rise to an affirmative duty. For example, a common carrier has a duty to protect passengers against unreasonable risk and provide care if they are harmed.[206] The same is true for the relationship between an innkeeper and guest, a possessor of land open to the public and members of the public on that land, and one who voluntarily takes custody of another.[207] With the rise of identity theft in the United States and the growth of the Internet,[208] has the time come to say that when a company collects and possesses customer personal information there is a special relationship that gives rise to an affirmative duty?

Certainly, some business relationships give rise to an affirmative duty. It has already been mentioned that common carriers have a duty to their passengers, and innkeepers have a duty to their guests. However, is the relationship between a company and consumer similar enough to extend a duty by analogy? Some courts recognize that businesses have a special relationship with customers when they are on the premises of a business.[209] Here, a company is taking possession of personal data and moving it to a holding area—usually a server—somewhat like a common carrier. But this is a tenuous relationship at best. Or, is it that in an increasingly digital world—one in which people preparing a will are now urged to consider the fate of their online identities once their physical being has gone[210]—a company that takes possession of personal information is, in some ways, acting as an innkeeper for that digital identity? To take it a step further, when a company gathers personal information on one of its customers—information like name, address, social security number, passwords, etc.—is the company voluntarily taking care of that customer's online avatar? At the least, we can recognize that identity in the digital age is a fluid and changing concept.

Perhaps the best way for a court to come to the conclusion that it should

205. Stiver v. Parker, 975 F.2d 261, 270 (6th Cir. 1992).

206. RESTATEMENT (SECOND) OF TORTS § 314A (1965).

207. *Id.*

208. *See supra* Part II.B.

209. *See, e.g.*, Morris v. De La Torre, 113 P.3d 1182, 1188 (Cal. 2005) (saying that "a proprietor nevertheless owes a special-relationship-based duty to undertake reasonable and minimally burdensome measures to assist customers or invitees who face danger from imminent or ongoing criminal assaultive conduct occurring upon the premises"); *contra* Anders v. Trester, 562 N.W.2d 45, 48 (Minn. Ct. App. 1997) (holding that "a mere merchant-customer relationship does not impose upon a merchant a duty to protect its customers").

210. Becky Yerak, *Digital Assets Often Forgotten During Estate Planning*, PITTSBURGH POST-GAZETTE (Aug. 31, 2012, 4:00 AM), http://www.post-gazette.com/stories/business/news/digital-assets-often-forgotten-during-estate-planning-651249.

disregard the general tort law rule that entities are not required to take action to prevent harm befalling another is to say that when a company receives, gathers, and stores personal information on its customers it has undertaken to render services necessary for the protection of the person or his or her things.[211] Take, for example, the court in *Guin v. Brazos*, which relied on the existence of safeguards as an indication that the company used reasonable care to rule in favor of the company.[212] Are those safeguards not an undertaking?

The problem with all of these approaches is that affirmative duties historically recognized by tort law require the powerful party in the special relationship to protect only against unreasonable risk of physical harm.[213] No physical harm could possibly come from a company–customer relationship that takes place in its entirety online. Identity theft may have horrible consequences for its victims,[214] but it is a financial crime in nature. That being said, courts have found affirmative duties in a variety of instances. It should not be difficult to find such a duty, especially in conjunction with the forthcoming section.

D. Data Thefts Are Foreseeable

Identity theft is foreseeable when a data leak occurs that includes personal information. As has been established, one of the reasons that courts have been so reluctant to recognize such a duty is likely because traditional tort law loathes imposing affirmative duties upon others to protect individuals.[215] In 1908, University of Pennsylvania legal scholar Francis H. Bohlen stated that "[t]here is no distinction more deeply rooted in common law" than the difference between active misconduct and passive inaction.[216] However, as already demonstrated, courts do occasionally find affirmative duties, especially if there is a special relationship or an undertaking between the two parties. But, to some courts, foreseeability of risk is the most

211. *See* RESTATEMENT (SECOND) OF TORTS § 324A (1965) (assigning liability to one who causes harm as a result of one's negligent performance of an undertaking).

212. Guin v. Brazos Higher Educ. Serv. Corp., No. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006); *see also* Complaint, *Szpyrka*, *supra* note 80 (claiming that LinkedIn violated a duty because "protections necessary to secure and safeguard databases were well-known within the industry and had been successfully used to protect sensitive [personally identifiable information] for years").

213. RESTATEMENT (SECOND) OF TORTS § 314A (1965).

214. *See infra* Part III.F.

215. *See supra* Part III.C.

216. Harold F. McNiece & John V. Thornton, *Affirmative Duties in Tort*, 58 YALE L.J. 1272, 1272 (1949) (quoting Bohlen, *supra* note 154, at 219).

important part of the test to determine if there is a duty.[217] For example, the Fourth Court of Appeals of Texas said that the "question of duty turns on the foreseeability of harmful consequences, which is the underlying basis for negligence."[218] The California Court of Appeals for the First District has said: "As a general principle, a defendant owes a duty of care to all persons who are foreseeably endangered by his conduct, with respect to all risks which make the conduct unreasonably dangerous."[219] With regard to identity theft, at least one court has indicated that identity theft is a foreseeable result of a data leak.[220] In *Cobell v. Norton*, the United States Court of Appeals, District of Columbia Circuit, treated data theft as a foreseeable consequence in its analysis of an injunction that prevented the federal government from connecting a database of trust accounts of 500,000 Native Americans to a network until the government could prove that the network was secure.[221] Though the court never used the word foreseeable and vacated the injunction on procedural grounds, it stated that "the Secretary, as a fiduciary, is required to maintain and preserve [individual Indian trust data]."[222]

Though *Cobell* here stands for the assertion that identity theft can be foreseeable, it must be pointed out that the court found that the parties in *Cobell* had a special fiduciary relationship. In *Cobell*, the Secretary of the Interior and the other defendants were trustees of funds held in trust for half a million Native Americans.[223] Nevertheless, this did not change the trial court's support for a temporary restraining order and preliminary injunction until a Special Master certified that all the data was secure.[224]

In a quasi-judicial administrative hearing, the Maine Public Utilities Commission found that an attack by a program called a "worm" was foreseeable.[225] The commission found that the company, Verizon, had sufficient warning about the worm and failed to take action to secure its

217. *See* Giraldo v. Cal. Dept. of Corr. & Rehab., 85 Cal. Rptr. 3d 371, 381 (Cal. Ct. App. 2008).

218. Allright San Antonio Parking, Inc. v. Kendrick, 981 S.W.2d 250, 252 (Tex. Ct. App. 1998).

219. *Giraldo*, 85 Cal. Rptr. 3d at 381 (internal quotations omitted) (quoting Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 342 (Cal. 1976)).

220. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004); *see also* Appellees' Brief at *48, Cobell v. Norton, No. 05-5388, 2006 WL 574389 (D.C. Cir. Mar. 3, 2006) (arguing that 500,000 Native Americans were put at risk).

221. *Cobell*, 391 F.3d at 253–54.

222. *Id.* at 254.

223. *Id.* at 253; *see also* Appellees' Brief, *Cobell*, *supra* note 220, at *48.

224. *Cobell*, 391 F.3d at 255.

225. Jane Strachan, *Cybersecurity Obligations*, 20 ME. B.J. 90, 94 (2005) (citing *In re* Verizon Related Reduction Claim, Maine Pub. Utils. Comm'n, No. 2000-849 (Apr. 30, 2003)).

systems.[226] There, the damage the worm caused was disruption of service.[227] Why would a worm that interrupts service be foreseeable but a hacker bent on identity theft not be foreseeable? Hackers often use programs such as worms, viruses, and key-loggers to gain access to personal information.[228] Would the commission really suggest that an identity thief gaining information through the use of a worm is foreseeable, but one gaining information due to a key-logger is not? There is little difference between a foreseeable worm that disrupts service and a foreseeable hacker that steals information.

The foreseeability of identity theft is a concept that is dancing on the fringes of legality. It is time for courts to recognize the foreseeability of identity theft. It is one of the fastest growing crimes in the country,[229] and has negatively affected millions of Americans during the last decade with no signs of abating.[230] Another indicator that data leaks are becoming rapidly foreseeable is the efforts that companies make to prevent such losses. Many companies have policies in place to protect data.[231] Ironic though it may be, those seeking to recover from companies where data had leaked are alleging that the very existence of safeguards to prevent data leaks is evidence that those leaks were foreseeable. For example, the complaint against LinkedIn claimed the leak was foreseeable "particularly in light of the fact that protections necessary to secure and safeguard databases were well-known within the industry and had been successfully used to protect sensitive [personally identifiable information] for years prior to this breach."[232]

Here we have companies taking the initiative to gather, collect, and store valuable information—perhaps without adequate security—that is potentially extremely damaging in the wrong hands. Recent events have proven that this information has a tendency to leak. Therefore, it is reasonable to say that these companies should foresee the risk of identity theft and take steps to prevent it.

226. *Id.*

227. *Id.* at 91.

228. *See supra* Part II.B (discussing the many tools at the disposal of an identity thief).

229. Hoar, *supra* note 58, at 1423–24.

230. *See supra* Part II.A.

231. *See, e.g.*, Guin v. Brazos Higher Educ. Serv. Corp., No. 05-668 RHK/JSM, 2006 WL 288483, at *3–4 (D. Minn. Feb. 7, 2006) (relying on the existence of safeguards as indication that the company did use reasonable care); *see also* Smedinghoff, *supra* note 41, at 23–24.

232. Complaint, *Szpyrka*, *supra* note 80, at ¶107.

E. Defining Reasonable Efforts

If courts do choose to recognize a common law duty to protect consumer data, as this Comment is suggesting, a judicially created standard should only require companies to take reasonable efforts, giving the companies a defense to potentially huge claims and unreasonable liability. Imagine, for example, that a large company collects certain information about its customers and keeps that information on networked computers. The company pays the best computer programmers it can find a competitive wage to encrypt the information. It also provides other security measures like passwords and firewalls. Nevertheless, these security measures fail, and a hacker gains access to potentially damaging information. Should that company be liable?

It should not. Hackers make it a point to stay one step ahead of the security measures seeking to defeat them.[233] As former Justice Department official Mark Rasch opined: "Only the dumb ones get caught."[234] It is unreasonable to think that companies would have to protect against the world's most skilled computer hacker, just like it would be unreasonable to hold a museum liable after getting hit by the world's greatest cat burglar. That being said, it is not enough that companies take minimal efforts to protect personal information. Courts should require reasonable efforts.

Reasonable, in this case, should be defined by the industry standard.[235] The complaint against LinkedIn gives an idea of what the industry standard is currently.[236] It describes a process called adding "salt" to a password before storing passwords in a hashing format.[237] Hash functions are algorithms that create a unique representation of information, known as a hash value, which can act as a stand-in for a stored password.[238] "Salting" refers to a process of assigning random values to the password before running it through the hashing algorithm.[239] More common and secure than

233. *See, e.g.*, Michael J. Martinez, *Microsoft Watched but Couldn't Catch Hacker*, ABCNEWS (Oct. 31, 2012), http://abcnews.go.com/Technology/story?id=119324&page=1 (detailing the company's efforts to track down a hacker who'd gained access to code for a product in development for about 12 days).

234. *Id.*

235. *Cf.* Anderson v. Owens-Corning Fiberglas Corp., 810 P.2d 549, 551 (Cal. 1991). The defense is analogous to the "state-of-the-art" defense raised in this products liability case. Companies use it to assert that "even those at the vanguard of scientific knowledge at the time the products were sold could not have known" of the risk. *Id.*

236. Complaint, *Szpyrka*, *supra* note 80, at ¶¶16–19.

237. *Id.* at ¶17.

238. CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY 293 (2010).

239. Complaint, *Szpyrka*, *supra* note 80, at ¶17.

that is to salt the password before reducing it to a hash format and then salt the resulting hash value before storing the information on a separate and secure server.[240] According to the *Szpyrka* complaint, this process is the current industry standard.[241]

What is clear—and possibly the only thing that is clear—from this description is that courts could easily find themselves mired in a pit of jargon if they marry themselves to a specific procedure, especially since procedures are likely to change with technology. It should be enough to require an industry standard and indicate that it can be shown by expert testimony. In addition, when courts recognize industry standards as evidence of reasonable efforts toward securing data, they should stress that industry standards are likely to change and that the security requirements may be tighter or looser depending on the type of data and how significant the risk of identity theft would be if it were to leak. For example, say a hacker wrote and distributed a program that could easily defeat the salting and hashing methods of protecting data discussed previously.[242] If salting and hashing continued to be the industry standard even though there were more secure methods available to protect data, the courts would likely find adherence to the industry standard falls below the amount of protection required by the duty.

Therefore, by requiring reasonable efforts, courts can insure that companies go far enough to protect data, while still providing them with a defense to a claim that would arise in the event of a security breach that could not reasonably be prevented.

F. Requiring a Showing of Actual Harm and Proximate Cause

Another way to limit the liability of this new cause of action is to require actual harm and proximate cause. Of the many recent lawsuits filed against large companies in the wake of huge data leaks, most allege only that information leaked, not that those involved actually had their identities stolen.[243] There is no doubt that the plaintiffs in these suits have gone through stressful times and had to take quick action due to the data leaks.[244]

240. *Id.* at ¶18.

241. *Id.*

242. *See* VAMOSI, *supra* note 29, at XIV (discussing the ease with which a modern laptop can defeat an older encryption method).

243. *See, e.g.*, Complaint, *Szpyrka*, *supra* note 80; Complaint, *Lawrence*, *supra* note 80.

244. *See* Hoar, *supra* note 58, at 1425 (indicating that victims of identity theft may not even know they have been victimized until they apply for a loan); Lynch, *supra* note 62, at 260 (noting that identity theft victims suffer financially but also that the crimes "exact a price on the victim in

But, if these people have not faced serious adverse consequences, such as having their identities stolen, they are the wrong group of plaintiffs. The plaintiffs filing these lawsuits claim a company is liable simply for the fact that information made its way out into the larger world even though no real harm has come from it. Though this Comment argues that courts should recognize a company's duty to its customers to protect their data, liability must be limited if it is to be an equitable solution. Holding a company responsible for every single instance of personal information leaking out to the Internet casts far too wide a net. When the leaks occur, they often involve millions of customers.[245] Making a company liable to every customer who has data leaked is an untenable solution. Such an all-encompassing cause of action imposes too much liability on companies and would make it much harder, if not impossible, for them to do business online.

Such a huge cause of action puts the jury in a difficult situation as well. Say, for example, that the 110 million customers affected by the Target leak—though there has been no evidence of identity theft—band together, file a class-action lawsuit, and win. How does the jury then make that class whole? Let's say the jury is generous and requires the company to pay out $110 million to the class. That's $1 per person, not including attorney fees. But an award large enough to impact the entire class is also likely to be so large it could cripple the company—all for a leak that, in the end, proved harmless.

That is why a showing of actual harm must be required. If a customer does suffer identity theft, it should not be difficult to show such harm. Identity theft can be extremely damaging. Robert S. Lasnik, Chief Judge of the United States District Court for the Western District of Washington—while sentencing a Starbucks employee found guilty of taking part in an identity theft ring in 2006—took the opportunity to highlight some of the damage that an identity thief can do.[246] He said, "identity theft can create huge emotional problems for people. We often think of bank fraud as just against a bank or just money, but it damages real people."[247] Identity theft, he added, breaks up families by causing rifts between husbands and

time and money spent trying to rebuild her credit and good name").

245. *See supra* Part II.A.

246. *Member of ID Theft Ring That Preyed on Starbucks' Employees Sentenced to Prison*, UNITED STATES ATTORNEY'S OFFICE, WESTERN DISTRICT OF WASHINGTON (June 2, 2006), http://www.usdoj.gov/usao/waw/press/2006/jun/nguyen.htm.

247. *Id.*

wives.[248] Judge Lasnik left out plenty of the ills of identity theft. The U.S. Social Security Administration will issue a new social security number to a victim of identity theft,[249] but it is no cure-all. The Social Security Administration does not destroy the old number and files the new with the old, to ensure that the person receives credit for earnings under the old number.[250] In addition, getting faulty information off a credit report is a difficult and time-consuming process.[251] Three main companies are responsible for keeping track of your credit report: Equifax, Experian, and TransUnion.[252] The Fair Credit Reporting Act requires these companies to provide a free copy of one's credit report upon request.[253] To make such a request, one must provide his or her name, address, social security number, and date of birth.[254] That's the easy part. If something on the report is wrong, one must tell the reporting company in writing—sent by certified mail—exactly what is wrong, and provide copies of documents that support this contention.[255] The company will then conduct its own investigation, usually within thirty days, in which it works with the company that provided the inaccurate information.[256] For example, take a victim of identity theft who had a maxed-out and overdue credit card show up on their credit report that was actually applied for and used by the identity thief. That victim would be at the mercy of the credit reporting company and the company issuing the credit card to sort out what actually occurred. If the investigation does not solve the problem, one can ask for a statement of dispute to be included in his or her file.[257] The frustration of this process can lead to social ills. Identity theft leads to stress and feelings of insecurity.[258]

248. *Id.*

249. *How Do I Replace My Social Security Card*, SOCIAL SECURITY, https://faq.ssa.gov/link/portal/34011/34019/Article/1944/How-do-I-replace-my-Social-Security-card (last visited Mar. 20, 2014).

250. *Changing Your Social Security Number*, END STALKING IN AMERICA, http://www.esia.net/Social_Security_Numbers.htm (last visited Mar. 20, 2014).

251. *Consumer Information: Disputing Errors on Credit Reports*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm (last visited Mar. 20, 2014).

252. *Id.*

253. 15 U.S.C. § 1681 (West 2012).

254. *Consumer Information: Disputing Errors on Credit Reports*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm (last visited Mar. 20, 2014).

255. *Id.*

256. *Id.*

257. *Id.*

258. *See, e.g.*, *Stress from Identity Theft*, PROTECT MY ID, http://www.protectmyid.com/identity-theft-protection-resources/identity-recovery/dealing-with-stress.aspx (last visited Mar. 20, 2014)

That harm must also be proximate. A cause of action such as this should not subject a company to never-ending liability. There must be a cutoff point from which a person cannot recover. For example, if there is a leak and a person's information is included in the leak, then twenty years pass before their identity is stolen, that person should not be able to recover. When faced with this uniquely challenging modern problem of liability for large data leaks, courts should fall back on the basics of tort law to determine whether the duty exists. Since *Palsgraff v. Long Island R. Co.*, courts have followed Judge Benjamin N. Cardozo's axiom to ask if "there was a natural and continuous sequence between cause and effect."[259]

It should be remembered that once the identity theft is discovered, the vast amount of the burden of identity theft falls on the customer's financial institution.[260] Chief Judge Lasnik eloquently explained the ills of identity theft while sentencing the Starbucks employee to fifty-four months in prison.[261] But, that was a criminal matter. He was not indicating the type of damages that a court should recognize in a civil suit for negligence.

The type of damage alleged in the most recent data leak complaints tends to be unspecific. In the LinkedIn case, for example, the complaint alleged that the harm befell the class suing the company because their personal information was "subject to public disclosure without consent" and that they "lost money in the form of monthly fees."[262] Nowhere does the complaint allege that the victims of the data leak had also become victims of identity theft. Indeed, what occurred during this leak was that hackers posted hashed passwords online in their hashed format, however, the complaint alleges that the hashing was not salted and therefore weak, allowing people to break the code within a few hours.[263]

Here we have a clear demarcation of what the courts should recognize as actual harm and what they should not. The mere posting of data online that may or may not be useful to nefarious individuals is not enough to maintain a cause of action. However, the showing of actual financial loss, as

(noting that "[a]t one point or another, victims of identity theft may feel overwhelmed by the physiological pain of loss, helplessness, anger, isolation, betrayal, rage, and even embarrassment").

259. 162 N.E. 99, 104 (N.Y. 1928).

260. *See Member of ID Theft Ring That Preyed on Starbucks' Employees Sentenced to Prison*, UNITED STATES ATTORNEY'S OFFICE, WESTERN DISTRICT OF WASHINGTON (June 2, 2006), http://www.usdoj.gov/usao/waw/press/2006/jun/nguyen.htm. (noting that for some victims "it took months of work to repair their credit history and reverse the charges on legitimate checks that had bounced").

261. *Id.*

262. Complaint, *Szpyrka*, *supra* note 80, at ¶¶25, 109.

263. *Id.*

the LinkedIn complaint alleged with regard to monthly fees,[264] is an example of actual damages.

The classic example would be one of a company losing control of personal information either by accident or through the efforts of a computer hacker, and that information making its way to an identity thief who thereafter used it to obtain a credit card in a customer's name. Courts should recognize a cause of action against the company with regard to the amount of money lost due to the falsely issued credit card, the value to the customer of any decline in credit rating, and damages to make the victim whole again. The value of a decline in credit rating should be a question for the jury.

In essence, courts must exercise caution in recognizing this duty to prevent the leak itself from being considered the damage that completes the tort. Rather, the customer has a claim only when actual damage, such as identity theft, occurs as a result of the leak and that damage is proximate to the leak.

G. The Cause of Action

In summation, there should be a cause of action against companies that negligently fail to protect customer data. When confronted with this issue a court should make the following ruling: A company that through the ordinary course of business collects, stores, analyzes, and uses customer personal information—defined as a collection of information such as the customer's name, address, passwords, social security number, credit and bank account numbers, and the like—has an affirmative duty to take reasonable efforts to provide security for said information. A company breaching that duty is liable to those customers who suffered actual harm, such as being a victim of identity theft, as a result of the breach.

This cause of action gives companies and consumers a clear sense of what standards apply. It does not open companies up to so much liability that they would feel the need to cease their data gathering practices. It merely requires them to take reasonable efforts, likely defined by the industry standard, provided, of course, that the industry standard is not itself negligent. In addition, it may even work to companies' advantage if customers feel more confident sharing their personal information online.

264. *Id.* at ¶62.

IV. CONCLUSION

In the digital age, the economy runs on information.[265] A recent spate of high-profile data leaks has made it clear that leaks of personal information stored by large companies are a problem that will likely continue.[266] With the rise of identity theft in the new millennium, that information must be protected from those who would seek to use it for nefarious purposes. As commentator Thomas J. Smedinghoff argues, "The privacy of a person's data is illusory at best if there is no security for the data."[267]

Companies leaking customer information, whether by accident or due to the actions of Internet hackers, remain a significant social ill that seems to be growing in scope.[268] Legislative efforts to plug these leaks have primarily focused on leak notification laws at the state level and federal laws concerning categories of data (e.g., HIPAA (concerning medical information) and GLB Act (financial)).[269] The easiest and best solution to this problem would be for courts to create a stronger incentive for companies to protect this data by recognizing that companies have a duty to keep information from getting into the wrong hands. Though case law may be headed in the direction of courts imposing a duty upon companies to protect consumer data, a la the European strategy for preventing data leaks, courts have gone to great effort to limit their rulings to the specific facts before them and therefore not create a precedent on this significant issue.[270]

Courts should recognize a cause of action for victims of data leaks first, by admitting that identity theft is a foreseeable risk when such data is leaked; second, by defining how a company can take reasonable efforts to protect data in terms of industry standards; and third, by limiting liability by requiring actual harm.[271]

The word "leak" often is misleading when referring to the amount of data in question. Often, it is more like a torrent impacting millions of people.[272] It would be foolish to hold companies liable to each and every person, especially if no one is actually harmed. This change in the law, although it imposes an affirmative duty upon companies to protect

265. *Demystifying Big Data*, *supra* note 1, at 9.
266. *See supra* Part I.
267. Smedinghoff, *supra* note 41, at 27.
268. *See supra* Part II.B.
269. *See supra* Part II.C.
270. *See supra* Part III.B.
271. *See supra* Part III.G.
272. *See supra* note 43 and accompanying text.

individuals, is necessary in the digital age.