NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 10, ISSUE 1: FALL 2008

"DO YOU REALLY NEED MY SOCIAL SECURITY NUMBER?" DATA COLLECTION PRACTICES IN THE DIGITAL AGE

Jonathan J. Darrow[1] ***& Stephen D. Lichtenstein***[2]

But he that filches from me my good name
Robs me of that which not enriches him
And makes me poor indeed.[3]

I. INTRODUCTION

Today, in both the traditional and e-commerce digital environments, an individual's social security number is obtained as a matter of course in order to uniquely identify both the individual and his or her account. Whether one is seeking dental care, obtaining a parking permit, securing an apartment, or simply renting a video, the service-providing entity will frequently obtain a social security number as a prerequisite to doing business. Until recently, there were virtually no laws restricting the ability of entities unrelated to the Social Security Administration to request, use, collect, or handle the number. At times the government even promoted or required its expanded use.[4] This haphazard, laissez-faire approach to the social security number has evolved into a data collection practice that spans the gamut of organizations, from government agencies to non-profits, employers to financial services institutions, universities to health service providers, as well as credit card companies, retailers, and many others.[5] Aptly

---

[1] Assistant Professor of Business Law, Plymouth State University; Harvard University (LL.M. candidate 2009), Duke University (J.D.), Boston College (M.B.A.), Cornell University (B.S.)

[2] Chair and Professor of Law, Department of Law, Taxation and Financial Planning, Bentley University (Waltham, MA)

[3] William Shakespeare, *Othello*, act III, sc. 3.

[4] *See, e.g.*, 42 U.S.C. § 405(c)(2)(D)(i)(I) (2006) (authorizing the use of the social security number for the purpose of identifying blood donors).

[5] While the focus of this article is the social security number, data collection practices that potentially disperse an individual's information across the globe

characterizing the current state of affairs, one legal scholar noted that "[a] person cannot function normally in today's United States without a social security number."[6] Even the government has conceded that the disclosure of a social security number is a virtual necessity to engage in a wide range of everyday activities in modern society, including obtaining a job.[7] One commentator summed it up nicely: "If you are at all an active participant in the modern economy, the list of companies that have your [Social Security Number] is depressingly long."[8]

It was not always so. To the contrary, the widespread purposes for which social security numbers are now used vastly exceed the original intent of the number as simply a means for administering the social security system.[9] Enacted in 1935, the animating purpose of the Social Security Act was:

> [t]o provide for the general welfare by establishing a system of Federal old-age benefits, and by enabling the several States to make more adequate provision for aged persons, blind persons, dependent and crippled children, maternal and child welfare, public health, and the administration of their unemployment compensation laws; to establish a Social Security Board; to raise revenue; and for other purposes.[10]

---

are by no means limited to this number. Other key pieces of unchangeable personal information frequently collected include names, dates of birth, mother's maiden names, driver's license numbers, and any other personal information the organization believes relevant. Many of the principles articulated herein are equally applicable to these other data. *See infra* Part III.B.

[6] Ira Bloom, *Freedom of Information Laws in the Digital Age: The Death Knell of Information Privacy*, 12 RICH. J.L. & TECH. 9, 46 (2006).

[7] Kathleen S. Swendiman, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*, CRS REPORT FOR CONGRESS, Feb. 21, 2008, at 3, *available at* http://fas.org/sgp/crs/misc/RL30318.pdf [hereinafter CRS REPORT FOR CONGRESS] ("[I]t would be very difficult to work or engage in many activities in this country without a SSN.").

[8] Mike Krause, *Social Security Numbers: Original Intent or Identity Theft?*, INDEPENDENCE INSTITUTE, Dec. 22, 2006, http://www.i2i.org/main/article.php?article_id=1346.

[9] *Social Security Numbers: Private Sector Entities Frequently Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, GAO REPORT 04-11, Jan. 2004, at 8, *available at* http://www.gao.gov/new.items/d0411.pdf.

[10] Social Security Act, Pub. L. No. 74-271, 49 Stat. 620 (1935).

The Social Security Act was never intended to create a national identification system for general usage.[11] It was not until eight years after its passage, in 1943, that President Roosevelt inaugurated an era of expanding use of the social security number by authorizing other federal agencies to use these numbers whenever the agency head deemed it advisable.[12] Even so, federal use of the social security number did not substantially accelerate until the 1960s, when the Internal Revenue Service, Veterans Administration, and other federal agencies began using it as the official record-keeping number.[13] Despite increasing use of the number, social security cards continued to warn against use for identification purposes. From 1946 until 1972 social security cards bore the cautionary legend "NOT FOR IDENTIFICATION."[14] This language did little to alter behavior, however, and eventually the legend was removed.[15]

The use of social security numbers by entities other than the Social Security Administration is not inherently objectionable, and social security numbers are in many ways ideally suited as unique identifiers. The numbers themselves are essentially arbitrary[16] and thus essentially impossible to guess or calculate. Because no two people possess the same number,[17] the potential confusion that might occur if names were used in their place can be avoided.

---

[11] *See* Steven Levy & Brad Stone, *Grand Theft Identity*, NEWSWEEK, July 4, 2005, *available at* http://www.newsweek.com/id/50433 (quoting Rep. E. Clay Shaw Jr.).

[12] Exec. Order No. 9397, 8 Fed. Reg. 16095 (Nov. 30, 1943).

[13] CRS REPORT FOR CONGRESS, *supra* note 7, at 18.

[14] History, SOCIAL SECURITY ONLINE, http://www.ssa.gov/history/hfaq.html (last visited May 29, 2008).

[15] CRS REPORT FOR CONGRESS, *supra* note 7, at 5.

[16] History, SOCIAL SECURITY ONLINE, *supra* note 14. The first three digits of an individual's social security number are based on the geographic region of residence at the time the number was assigned. The remaining digits "are more or less randomly assigned." *Id*.

[17] Social security numbers are not reused even after a holder's death. *History*, SOCIAL SECURITY ONLINE, *supra* note 14. However, sometimes more than one person may use a social security number either on purpose, as in the case of identity theft, or accidentally. *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, Pub. No. 05-10064, at 4 (Oct. 2007), *available at* http://www.ssa.gov/pubs/10064.pdf.

Unlike names and addresses, social security numbers generally do not change and thus provide consistency over time.[18] They are intangible and have no intrinsic value, and therefore do not by themselves constitute a target for theft. Almost all citizens have one.[19] Moreover, the existence and use of a common identifier is virtually indispensable in allowing organizations, whether public or private, to differentiate one individual from another. For example, libraries must have a means for identifying who is borrowing a book; banks must be able to match deposits to accounts; and universities must be able to track application materials and academic records. A unique identifier allows these types of transactions and processes to occur efficiently. Not surprisingly, the social security number has been credited with facilitating coordination among government agencies and aiding in statistical research efforts.[20]

The problem arises less from the fact that many organizations use the social security number as a means of account identification, and more from its simultaneous use as a password or "key" that allows the holder to access or "unlock" the account. As more and more institutions adopt the social security number, its effectiveness as a password becomes greatly diminished.[21] Reflecting the unfortunate reality that a single number can provide access to multiple accounts, commentators have lamented that the social security number has become a "skeleton key" for identity theft

---

[18] Social security numbers can be changed in certain circumstances, such as where a domestic violence victim is being harassed or abused. *See New Numbers for Domestic Violence Victims*, SOCIAL SECURITY ADMINISTRATION, Pub. No. 05-10093, at 1, *available at* www.ssa.gov/pubs/10093.pdf.

[19] It is estimated that 277 million individuals currently possess a social security number. *Social Security Numbers: Private Sector Entities Frequently Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, GAO REPORT 04-11, Jan. 2004, at 4.

[20] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO REPORT 02-352, May 2002, at 16, *available at* http://www.gao.gov/new.items/d02352.pdf.

[21] For an enlightened explanation of identification theory and why social security numbers make poor keys, see Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 95-100 (2001).

criminals.[22] Even more troubling, the availability of the number increases in direct proportion to its use as a key. Any organization that wishes to use an individual's social security number must make at least one copy of it; this copy is frequently stored in a computer system that may be accessible by a global workforce of employees. Given that thousands of organizations collect the number and share it with affiliates, contractors, government entities and others, the number's vulnerability to loss, employee misuse, or theft by third parties quickly becomes apparent. The advent of the Internet and the proliferation of outsourcing have only magnified the speed and extent of dispersal of the social security number. Just as the weakest link will make a chain give way, the institution with the most lax security procedures or least honest employees may be the only thing standing between a thief and the contents of an individual's bank account and private records.[23]

How secure would one feel if she gave the key to her home to every government agency, health care provider, credit card company, and other business organization with whom she had a direct or indirect relationship? What would one do if a copy of this key could be located, inexpensively or even for free on the internet, by anyone with basic information who is willing to look for it? Yet this is exactly the system that has been created via the use of the social security number as a password that can provide the holder with access to an individual's financial resources, retirement accounts, private health information, and more. Worse yet, unlike locks which can be changed if a key is lost or falls into the wrong hands, the social security number is virtually unchangeable.[24]

---

[22] Levy & Stone, *supra* note 11.

[23] *See* Michael Quint, *Bank Robbers' Latest Weapon: Social Security Numbers*, N.Y. TIMES, Sept. 27, 1992, *available at* http://query.nytimes.com /gst/fullpage.html?res=9E0CE2D81F39F934A1575AC0A964958260; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1254 (2003) (describing the social security number as a "magic key that can unlock vast stores of records as well as financial accounts").

[24] Jonathan Krim, *Net Aids Access to Sensitive ID Data: Social Security Numbers Are Widely Available*, WASHINGTONPOST.COM, Apr. 4, 2005, http://

This article begins in Part II by highlighting the problems of identity theft and explaining how widespread use of the social security number creates an elevated risk of loss. The impact of recent trends in electronic data aggregation and outsourcing are emphasized. Part III explores the existing legal framework and recently enacted laws affecting social security number collection, display, and storage, and argues that these laws are generally inadequate. In Part IV, an analytical framework is proposed that would place the risk of loss on the party that is in the best position to avoid the loss. Federal laws consistent with this framework are proposed that would increase security and reduce risk of loss, all while minimizing the costs borne by organizations that collect and use data.

II. A GROWING PROBLEM

A. *Personal Data and Identity Theft*

The alarming magnitude of identity theft has been widely recognized and documented.[25] State legislatures began to acknowledge the problem of identity theft in 1996, when Arizona became the first state in the nation to enact a statute criminalizing

---

www.washingtonpost.com/wp-dyn/articles/A23686-2005Apr3.html. Also unlike a lost key, the social security number cannot be changed merely because it has been lost or stolen. *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, Pub. No. 05-10064, Oct. 2007, at 6, *available at* http://www.ssa.gov/pubs/10064.pdf. There must be evidence that (1) someone is in fact wrongfully using the number and (2) that the individual to whom the number belongs is being disadvantaged by the wrongful use. *Id*.

[25] *See, e.g.*, Guin v. Brazos Higher Educ. Servs., 2006 WL 288483, at *6 (D. Minn. Feb. 7, 2006) (noting the "increasing problem of widespread identity theft"); Ellen Nakashima & Ylan Q. Mui, *Data Theft Grows to Biggest Ever*, WASH. POST, Mar. 30, 2007, *available at* http://www.washingtonpost .com/wp-dyn/content/article/2007/03/29/AR2007032900237.html; Jon Cohen, *Poll: Identity Theft Concerns Rise*, ABC NEWS, Mar. 17, 2005, http://abcnews.go.com/Business/PollVault/story?id=590413&page=1; Caroline E. Mayer, *FTC Says Identity Theft is Rampant: 10 Million Cases in the Past Year, Survey Concludes*, WASHINGTON POST, Sept. 4, 2003, *available at* http://emoglen.law.columbia.edu/LIS/archive/crime/A22781-2003Sep3.html.

the theft of one's identity.[26] By 2007, all fifty states had some form of identity theft legislation on the books.[27] Attesting to the significance of the problem and the fact that identity theft substantially affects interstate commerce, Congress passed the Identity Theft and Assumption Deterrence Act of 1998, which criminalized identity theft at the federal level and authorized the Federal Trade Commission (FTC) to track the incidence of identity theft nationwide.[28] Pursuant to this authority, the FTC issued its first identity theft report, covering calendar year 2000, which reflected approximately 28,000 cases of identity theft.[29] In seven years, the number of consumer identity theft reports to the FTC increased nearly ten-fold, to over 258,000.[30] However, the number of FTC-reported cases grossly understates the pervasiveness of identity theft. Reflecting the fact that not all cases of identity theft are reported, the Federal Bureau of Investigation claims that more than ten million individuals are victimized by identity theft annually.[31]

---

[26] ARIZ. REV. STAT. ANN. § 13-2008 (2008). *See* Catherine Pastrikos, *Identity Theft Statutes: Which will Protect Americans the Most?*, 67 ALB. L. REV. 1137, 1138 (2004) (noting that Arizona was the first state to enact an identity theft statute).

[27] *Combating Identity Theft: A Strategic Plan*, THE PRESIDENT'S IDENTITY THEFT TASK FORCE, Apr. 2007, at 53, *available at* http://www.identitytheft.gov/reports/StrategicPlan.pdf [hereinafter PRESIDENT'S IDENTITY THEFT TASK FORCE].

[28] Identity Theft & Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028 and 28 U.S.C. § 994).

[29] *Identity Theft Complaint Data*, FED. TRADE COMM'N, Jan. to Dec. 2000, at 1, *available at* http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf. Of 40,000 complaints received, 69%—or approximately 28,000—were victims' complaints (the remaining 31% were requests for information related to identity theft prevention).

[30] *Consumer Fraud and Identity Theft Complaint Data*, FED. TRADE COMM'N, Jan. to Dec. 2007, *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2007.pdf.

[31] *How to Protect Your Good Name from Identity Theft*, FED. BUREAU OF INVESTIGATION, Oct. 20, 2004, http://www.fbi.gov/page2/oct04/preventidt102104.htm; *see also* Neal Walters & George Gaberlavage, *Protecting Social Security Numbers from Identity Theft*, AARP, Sept. 2005, http://www.aarp.org/research/frauds-scams/fraud/fs122_id_theft.html.

Financial losses from identity theft are as staggering as the number of individuals affected. The FTC estimates that the total cost to society exceeds $50 billion per year.[32] These figures include losses both to consumer victims and to businesses that are defrauded by the identity thief. According to a Department of Justice estimate, losses to households from identity theft over a particular six-month period were $3.2 billion.[33] A study cited by the Government Accountability Office (GAO) reported that organizations whose data storage systems were breached sustained an average loss of $1.4 million per breach,[34] and the number and size of breaches have been increasing exponentially.[35] As far back as 1997, a single credit card company reported that the losses to its member banks from identity theft approached $400 million per year.[36] Identity theft has been described as not only the fastest-

[32] *See A National Strategy to Combat Identity Theft*, DEP'T OF JUSTICE, May 2006, at 1, *available at* http://www.cops.usdoj.gov/files/ric/Publications/e03062303.pdf. Losses to citizens of other countries can be equally staggering. *See* Karen Dearne, *ID Theft Hits $1 Billion: ABS*, AUSTRALIANIT, http://www.australianit.news.com.au/story/0,24897,23952995-5013044,00.html (reporting $977 million in fraud losses to Australians during 2007, including identity theft losses).

[33] *Identity Theft 2004*, *Bureau of Justice Statistics Bulletin*, DEPARTMENT OF JUSTICE, Apr. 19, 2006, at 1, http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

[34] *Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO REPORT 07-737, June 2007, at 6, *available at* http://www.gao.gov/new.items/d07737.pdf.

[35] *See* Courtney Mabeus, *OMB Reports Big Increase in Data Breaches in 2007*, FED. TIMES, Mar. 1. 2008, http://www.federaltimes.com/index.php?S=3399508; Tom Zeller, *An Ominous Milestone: 100 Million Data Leaks*, N.Y. TIMES, Dec. 18, 2006, *available at* http://www.nytimes.com/2006/12/18/technology/18link.html.

[36] Identity Theft and Assumption Deterrence Act of 1998, 144 Cong. Rec. H9994-01, 1998 WL 694715 (daily ed. Oct. 7, 1998) (statement of U.S Congresswoman Rep. Betty McCollum (4th Dist. MN)).

growing financial crime in the United States,[37] but also as the fastest-growing crime in the United States.[38]

There is no doubt that the social security number is central to the commission of the crime of identity theft. According to a 2002 GAO Report, the social security number is one of three pieces of information most sought after by identity thieves.[39] The Identity Theft Resource Center, a national non-profit that is organized for the purpose of preventing identity theft, includes the social security number in its definition of identity theft: "a crime in which an impostor obtains key pieces of . . . information . . . such as Social Security numbers . . . and uses them for [her] own personal gain."[40] Jones Day, an international law firm employing more than 2,000 attorneys, describes the social security number as "the No. 1 identifier used by criminals in identity theft."[41] During the congressional testimony leading up to the passage of the 1998 Federal Identity Theft and Assumption Deterrence Act, repeated references were made to the social security number and the problems that arise when it is obtained by identity thieves.[42] Tellingly, the Social Security Administration itself counsels against the disclosure of the social security number as a means to avoid identity theft,[43] and "discourages banks and businesses from

---

[37] Press Release, N.Y. State Governor's Press Releases, *Governor Patterson Unveils Legislation to Strengthen New York's Identity Theft Laws* (May 21, 2008), http://www.ny.gov/governor/press/press_0521081.html.

[38] Identity Theft and Assumption Deterrence Act of 1998, 144 Cong. Rec. H9995-01, 1998 WL 694715 (daily ed. Oct. 7, 1998) (statement of U.S Congressman Rep. John Shadegg (3rd Dist. AZ)).

[39] *Social Security Numbers: Government Benefits from SSN Use, supra* note 20, at 9 (describing the other two pieces of information as names and birth certificates).

[40] Identity Theft Resource Center, http://www.idtheftcenter.org/ (last visited June 1, 2008).

[41] Mauricio F. Paez, *New York Enacts Social Security Number Protection Law*, JONES DAY COMMENTARIES, Oct. 2006, http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S3778.

[42] *See* Identity Theft and Assumption Deterrence Act of 1998, 144 Cong. Rec. H9993-01, 1998 WL 694715 (daily ed. Oct. 7, 1998).

[43] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, Pub. No. 05-10064 (Oct. 2007) http://www.ssa.gov/pubs/10064.pdf.

using the number as proof of identification."[44] Finally, the President's Identity Theft Task Force described the social security number as "critical,"[45] the "key,"[46] and the "most valuable commodity for an identity thief,"[47] and called for a reduction in the unnecessary use of the number.[48]

B. *The Data Aggregation Explosion*

Identity theft is nothing new and has certainly existed in one form or another for centuries or longer.[49] Nor are recorded birthdays, mother's maiden names, or even social security numbers a particularly recent phenomenon. What has changed is that, within the last two decades, evolving business practices and a dynamic business environment have converged with technological advances to create conditions ripe for data theft and identity misuse on an unprecedented scale. So fundamental and transformative are these changes that they have inspired the moniker of the modern era, variously referred to as the information age, the internet age, or—as in the title to this article—the digital age.

As the digital age dawned and electronic records replaced paper records, the volume of consumer information that could be practically stored increased by several orders of magnitude. Electronic records require less space, are less expensive to reproduce and transfer, and are more easily searchable than were paper records.[50] The ability to share data electronically meant that national organizations that collected information locally could centralize computer databases for customer convenience or simply

---

[44] Michael Quint, *supra* note 23.

[45] THE PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 42.

[46] THE PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 23.

[47] THE PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 4.

[48] THE PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 23.

[49] *Identity Theft Reporting System*, UTAH ATTY. GEN.'S OFFICE, http://www.idtheft.utah.gov/pn/module-PS-viewpub-tid-2-pid-1.htm (last visited June 1, 2008).

[50] Bloom, *supra* note 6, at 12 ("Digital technology has made the ability to obtain, collect, compile, manipulate, mine, and transfer data vastly easier . . . .").

for business efficiency.[51] This customer information-sharing became so important that a whole category of business software developed to manage digitized customer information, called customer relationship management (CRM) software.[52] Nor was collected information exclusively retained by the collecting entity. Recognizing the value of customer information, businesses[53] and even state governments[54] began to package and sell consumer information to third parties in enormous volumes. In 2006, the GAO identified fifty-three websites that specifically offer to sell a person's social security number.[55]

At the same time electronic data storage and sharing were becoming easier, cheaper, and more common, businesses across a broad range of industries were growing dramatically in size via mergers and acquisitions,[56] thereby further magnifying the

---

[51] *Social Security Numbers: Private Sector Entities Frequently Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, GAO REPORT 04-11, Jan. 2004, at 4.

[52] *See* Chris Gaither, *Software to Track Customers' Needs Helped Firms React*, N.Y. TIMES, Oct. 1, 2001, at C1, *available at* http://query.nytimes.com/gst/fullpage.html?res=940CE3DF153DF932A35753C1A9679C8B63&sec=&spon=&pagewanted=all (describing the market for CRM software as a "$6.5 billion . . . industry").

[53] Just one data broker, ChoicePoint, has assembled literally billions of pieces of information about millions of individuals, and offers this information for sale to more than 50,000 customers. Robert O'Harrow, Jr., *In Age of Security, Firms Mine Wealth of Personal Data*, WASH. POST, January 20, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html; *see also* Evan Perez & Rick Brooks, *File Sharing: For Big Vendor of Personal Data, A Theft Lays Bare the Downside*, WALL ST. J., May 3, 2005, at A1 ("ChoicePoint Inc. has 19 billion data files, full of personal information about nearly every American adult.").

[54] *See infra* Part III.C.3.

[55] *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs*, GAO-06-495, May 17, 2006, at 3.

[56] *See* Robert Pitofsky, FTC Chairman, Federal Trade Commission, Prepared Remarks, *Merger Competition and Policy—The Way Ahead* (Aug. 4, 1998) (transcript available at http://www.ftc.gov/speeches/pitofsky/canada.sp2.shtm) ("[T]he United States set an all-time record last year when roughly 3,700 proposed mergers . . . were filed with the . . . Federal Trade Commission. Many

aggregation of data. Big box retailers emerged on the scene while already sizeable domestic companies expanded their reach around the globe.[57] Nor was database growth limited to the private sector. Increasingly, government entities at all levels saw the need for, and practicality of, electronic data sharing.[58]

The Internet provided an unneeded boost in this already thriving data aggregation explosion.[59] Not only could the Internet facilitate the sharing and distribution of data,[60] it could also provide a cost-effective means for data collection. The Internet and stand-alone electronic terminals allowed businesses to shift the cost of data collection and entry from employees to consumers. As long as appropriate software was in place, an enormous volume of data could be voluntarily entered by consumers at virtually no cost to the business, all while increasing the number of customers that could be serviced per unit time. Whether entering personal data at a United Parcel Service shipping terminal or completing the ubiquitous web registration, the consumer populace was henceforth conscripted to enter terabytes of information as part of the process of completing a transaction. Declining to provide information was

---

of us thought that the merger wave could become no greater than in 1997. To my surprise, merger filings . . . have increased [since then] . . . .").

[57] *See* William M. Bulkeley, *Cut Down to Size: `Category Killers' Go From Lethal to Lame In the Space of a Decade*, WALL ST. J., Mar. 9, 2000, at A1 ("'[C]ategory killers' . . . remade the retailing landscape in the 1990s" by "underpricing department stores and mom-and-pops . . . ."). Concerns over increasing business size are not new. Emile Zola's classic 1883 novel "Au Bonheur des Dames" described the difficulties faced by small stores as a new form of business – known as the department store – was coming of age. *See* EMILE ZOLA, AU BONHEUR DES DAMES (Larousse 2006) (1883).

[58] *Social Security Numbers: Government Benefits from SSN Use*, *supra* note 20, at 15 ("[T]he majority of agencies at all three levels of government reported sharing information containing SSNs . . . ."); Bloom, *supra* note 6, at 5 ("[S]tate and local governments increasingly create comprehensive databases . . . containing . . . vast amounts of personal data . . . .").

[59] Bloom, *supra* note 6, at 2; Dearne, *supra* note 32 ("[P]ersonal fraud is a growing crime type due to the rapid expansion and availability of the internet, and the increase in electronic storage, transmission and sharing of data.").

[60] The internet has been used in eBay-like fashion as a means of connecting buyers and sellers of stolen identities. *See* Charles Herman, *Online Identity Theft Ring Out of the Shadows*, ABC NEWS, June 29, 2006, http://abcnews.go.com/Technology/story?id=2136453.

not an option, unless one was willing to forgo a large and ever-increasing portion of everyday products and services.

Unfortunately, the aggregation of vast amounts of data is like the hoarding of treasure: while few will bother to pick up a penny lying on the sidewalk, a bank vault full of cash will draw thieves and imposters from far afield. Similarly, a large data warehouse will attract thieves who might not find it worthwhile to rifle through a mailbox to obtain the data of a single individual.

The treasure of personal information is in turn a key that enables thieves to access more traditional forms of treasure, such as the cash in a savings account. Robbers that might once have been thwarted by the steel, concrete, and sophisticated devices guarding traditional bank vaults can now use others' personal information to induce banks to hand over the cash willingly. Moreover, while laws protect physical embodiments of value such as cash, the value of non-secret data is largely unrecognized by law. As a result, vast treasure troves of vault-defeating personal information may be virtually unguarded.[61] This is only the beginning of the allure of identity theft. Making the crime even more attractive to thieves is the fact that the "bank" will point the finger, at least initially, at the wrong thief: the victim of the identity theft, rather than the perpetrator. Not surprisingly, a recent year witnessed twice as many identity thefts as traditional robberies.[62]

C. *"Information Wants to Be Free"*

In 1984 Stewart Brand proclaimed that "information wants to be free."[63] This characterization is particularly appropriate in the

---

[61] Jonathan Krim, *Ubiquitous Technology, Bad Practices Drive Up Data Theft*, WASH. POST, June 22, 2005, at D1, D5, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/06/21/AR2005062101615_3.html (noting the weak security protecting personal data).

[62] Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN ST. L. REV. 779, 783-84 (2007).

[63] *See* Laura N. Gasaway, *Values Conflict in the Digital Environment: Librarians Versus Copyright Holders*, 24 COLUM.-VLA J.L. & ARTS 115, 133 n.104 (2000).

context of personal consumer information such as the social security number, where restricting distribution of the information once it has been provided to a data-collecting entity is about as easy as convincing the media not to air breaking news. This is partially due to the fact that information sharing in most industries is virtually unrestricted. Even where federal legislation places restrictions on the transfer of personal information, organizations are generally free to share that information with affiliates, subcontractors, and other third parties so long as certain conditions are met.[64]

In some cases, information *must* be made available to the public by laws such as the Freedom of Information Act[65] or the social security statute itself.[66] In other cases, government records are made available to enhance public trust, encourage accountability, and promote the integrity of judicial and other government processes.[67] In order to provide greater public service and access, government records that were once publicly accessible only via in-person site visits are increasingly being made available online.[68] While this facilitates legitimate access to information, it can also act as a boon to those with less scrupulous motives. In one notable incident, the names, addresses, phone numbers, and social security numbers of Washington State police officers were assembled from publicly available records and posted on the

[64] *See, e.g.*, 15 U.S.C. § 6802 (2008) (Financial institutions may disclose non-public personal information to both affiliated and unaffiliated third parties provided certain conditions "are met, including limitations on reuse and sharing for marketing purposes.").

[65] Freedom of Information Act, Pub. L. No. 89-554 (1966) (codified as amended at 5 U.S.C. § 552 (2008)).

[66] *See* 42 U.S.C. § 405 (2006) (describing several purposes for which the social security number may or must be disclosed).

[67] *Social Security Numbers: Government Benefits from SSN Use*, *supra* note 20, at 12.

[68] Bloom, *supra* note 6, at 8 (explaining that publicly available paper records – as opposed to electronic records – were relegated to "practical obscurity" due to high search costs and other factors); *Social Security Numbers: Government Benefits from SSN Use*, *supra* note 20, at 8.

Internet.[69] Such troubling behavior is facilitated by the forty-one states and 75% of United States counties that display social security numbers in public records.[70]

Where information is not shared voluntarily, it may be stolen or misused.[71] Collected data stored in electronic form is in many ways more vulnerable to theft than old-fashioned paper records. First, theft of enormous volumes of electronic data can be accomplished quickly by downloading to a flash drive or to a networked computer. Second, data thieves need not physically "break-in" to an office where records are stored, and may instead surreptitiously hack into computer networks while maintaining a safe distance.[72] In this sense, it is fitting that Stewart Brand made his now-famous statement at a hackers' conference.[73] Third, theft by disgruntled or opportunistic employees is made easier by having data in electronic form. Rather than having to stand at the photocopy machine with incriminating files in hand, employees may be able to download directly from their workstations or home office, which is an activity an observer may have difficulty differentiating from the performance of ordinary job

---

[69] Adam Liptak, *A Web Site Causes Unease in Police*, N.Y. TIMES, July 12, 2003, at A12, *available at* http://query.nytimes.com/gst/fullpage.html?res=9802E2D91E3DF931A25754C0A9659C8B63.

[70] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 24.

[71] Social security numbers may also be inadvertently exposed when employees download file sharing services such as LimeWire. *See* Brian Krebs, *Justice Breyer Is Among Victims in Data Breach Caused by File Sharing*, WASH. POST, July 9, 2008, at A1, A12, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/ AR2008070802997_pf.html (reporting that Pfizer, the Walter Reed Army Medical Center, and a McLean, Virginia investment firm have all experienced this type of breach).

[72] *See, e.g.*, Jordan Robertson, *Citibank ATM Breach Reveals PIN Security Problems*, ASSOCIATED PRESS, http://www.nydailynews.com/money/2008/07/01/2008-07-01_citibank_atm_breach_reveals_pin_security.html, July 3, 2008 (reporting that hackers stole millions of dollars after breaking into a bank's ATM network and gaining access to customers' unencrypted personal identification numbers).

[73] *See* Katie Hafner, *A New Way of Verifying Old and Familiar Sayings*, N.Y. TIMES, Feb. 1, 2001, at G8, *available at* http://query.nytimes.com/gst/fullpage.html?res=9407E7DC163EF932A35751C0A9679C8B63 ("information wants to be free").

responsibilities.[74] Fourth, electronic data theft can be accomplished without leaving obvious evidence of the theft, and data breaches may therefore go unnoticed for long periods of time. Not surprisingly, "[t]he FTC and law enforcement agencies have found that merchants and retailers are increasingly vulnerable to disgruntled or dishonest employees with access to huge databases full of Social Security numbers that can be sold illegally or used for fraud."[75]

Two cases illustrate just how easy it is for a dishonest employee to abscond with private information. In 1993 a California resident became a victim as a result of completing intake forms at her doctor's office.[76] The doctor's receptionist misappropriated the patient's social security number and moved to Las Vegas where the number was used to commit identity theft.[77] A decade later, a salesman used a Colorado customer's birth date and social security number to obtain a surgical procedure and then left the $40,000 tab to the customer.[78] These two examples are exceptional in the sense that the perpetrator of the identity theft was known. In the majority of cases, victims do not know how, when, or by whom their private information was obtained.[79]

---

[74] Krause, *supra* note 8 (citing a study revealing that "nearly twenty three percent of identity theft cases . . . were the result of 'dishonest employees'"); Brian Krebs, *Data Breaches Are up 69% This Year, Nonprofit Says*, WASH. POST, July 1, 2008, at D3, *available at* http://www. washingtonpost.com/wp-dyn/content/article/2008/06/30/AR2008063002123_pf .html (identifying that the percentage of breaches caused by employee theft more than doubled from 2007 to the first half of 2008).

[75] William McCall, *Identity Theft Often Begins with Social Security Number*, ASSOCIATED PRESS, Jan. 5, 2004, *available at* http://www.usatoday.com/tech/news/2004-01-05-ssn-id-theft_x.htm.

[76] *See* TRW, Inc. v. Andrews, 534 U.S. 19 (2000).

[77] *Id.*

[78] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 25.

[79] *Prepared Statement of the FTC on Identity Theft*, Sept. 13, 2000, § II.A., http://www.ftc.gov/os/2000/09/idthefttest.htm.

D. *Outsourcing*

Not only have enormous data-aggregation centers emerged, but outsourcing has led to the sharing of personal data with contractors and business partners, who may in turn share information with their contractors and business partners.[80] As the internet renders geographic limitations a nullity, private information may cross national borders with startling facility where it is safeguarded only by the honesty of a distant employee or a host country's privacy laws. Even where such laws exist and employees are generally honest, a large sum of money offered as a bribe in return for information may be tempting indeed to someone earning a few dollars per hour as a customer service representative.[81]

Dishonest or desperate employees may use confidential information as a bargaining chip to extort money or win concessions. Such a scenario is not as far-fetched as it sounds. In 2003, employees of an Ohio company working in India threatened to release confidential data if their demands were not met.[82] In another similar case, a medical transcriptionist in Pakistan working indirectly for the University of California at San Francisco (UCSF) threatened the release of private data that had been obtained via a string of subcontracting arrangements.[83] She was employed as a subcontractor for a Florida company that was in turn a

---

[80] *See generally Social Security Numbers: Government Benefits from SSN Use*, *supra* note 20, at 18-19 (noting that government agencies not only share social security numbers with other government agencies, but also with contractors, credit bureaus, insurance companies, debt collection agencies, researchers, private investigators, and even marketing companies).

[81] Along these lines, a credit card call center employee reportedly misused customer accounts to accumulate $65,000 of fraudulent purchases. *Data Breaches Are Frequent, supra* note 34, at 21. Similarly, twenty-seven cases of identity theft were tied to a former FDIC intern who inappropriately accessed employee information. *Social Security Numbers: Government Benefits from SSN Use*, *supra* note 20, at 23.

[82] *Outsourcing Privacy: Countries Processing U.S. Social Security Numbers, Health Information, Tax Records Lack Fundamental Privacy Safeguards*, STAFF REPORT OF REP. EDWARD J. MARKEY, Sept. 2005, at 2, http://markey.house.gov/docs/privacy/iss_privacy_rep050914.pdf.

[83] *Id.*

subcontractor for a California company that was a contractor for UCSF.[84]

That sensitive data may be vulnerable when it is disbursed through multiple layers of geographically and culturally diverse intermediaries and affiliates is hardly surprising. Not only do numerous employees have access to the data, but varying levels of security provide an increased likelihood of a data breach. The GAO has reported that breaches at financial institutions are "typically due to lapses in data security by [a] third-party entity [such as a contractor or subcontractor] and not the financial institution itself."[85] For example, in *Pisciotta v. Old National Bancorp*,[86] the private data of tens of thousands of site users was exposed after a security breach at NCR, an independent organization that maintained Old National Bancorp's website. Similarly, in the 2006 case of *Forbes v. Wells Fargo Bank, N.A.*,[87] private data was compromised when computers belonging to Regulus were stolen.

Of course, the mere exposure of data or potential to penetrate a database does not necessarily lead to identity theft. Yet this hardly justifies an ostrich-like refusal to acknowledge the threat posed by the needless or careless exposure of data. To an identity thief, an organization that aggregates vast amounts of feebly-protected data in a central location is a Wal-Mart full of pre-packaged identity theft kits, a tempting proposition to be sure. Not surprisingly, organized criminal groups from around the world are increasingly turning to identity theft,[88] sometimes obtaining data by hacking

---

[84] David Lazarus, *Outsourced UCSF Notes Highlight Privacy Risk*, SAN FRANCISCO CHRONICLE, Mar. 28, 2004, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/03/28/MNGFS3080R264.DTL.

[85] *Data Breaches Are Frequent, supra* note 34, at 15 n.26.

[86] 499 F.3d 629, 632 (7th Cir. 2007).

[87] 420 F. Supp. 2d 1018, 1019 (D.C. Minn. 2006) (stating that Regulus was an independent service provider hired by a subsidiary of Wells Fargo to print account statements).

[88] Bob Sullivan, *Huge Identity Theft Ring Busted*, MSNBC, Nov. 25, 2002, http://www.msnbc.msn.com/id/3078518/ (describing a Nigerian crime ring that stole 30,000 identities and used the data to tap victims' bank accounts); *Identity Theft: The Organized Crime Factor*, IDENTITY THEFT KNOWLEDGE CENTER, Aug. 2003, http://identitytheft911.org/articles/article.ext?sp=90 ("[M]ore and

into corporate databases.[89] To cite just one example, the Department of Justice recently reported the indictment of eleven individuals from the United States, Estonia, Ukraine, Belarus, and China who allegedly conspired to hack into databases at TJX, BJ's, Barnes & Noble, Sports Authority, DSW, and others.[90] Allegedly, the conspirators sold some of the more than forty million credit and debit card numbers obtained to other criminals both in the United States and abroad.[91] Losses to banks, retailers, and consumers are estimated to be "at least tens of millions of dollars."[92]

The disconcerting vulnerability of databases has been repeatedly illustrated by data breaches, such as those in *Pisciotta* and *Forbes*, which have reached epic proportions over the last five years. The number of records compromised by data breaches reported in the United States has grown to over 229 million,[93] up dramatically from the 90 million reported less than two years previously.[94] While some of these records may duplicate information for a single individual, it is worthwhile to recall that the population of the United States is just over 300 million

---

more groups from overseas are making their way over here [to commit identity theft].").

[89] *See* Susan B. Shor, *International Identity Theft Ring Discovered*, TECH NEWS WORLD, Aug. 9, 2005, http://www.technewsworld.com/story/45337.html?welcome=1213457984 (describing a ring that used spyware to nab customer social security numbers and other data at fifty international banks); *see also* PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 19 (describing foreign computer hackers that penetrated corporate databases).

[90] *Eleven Indicted in Largest ID Theft Case Ever*, CBS NEWS, Aug. 5, 2008, http://www.cbsnews.com/stories/2008/08/05/tech/main4323211.shtml.

[91] *Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers*, DEPT. OF JUSTICE, Aug. 5, 2008, http://www.usdoj.gov/opa/pr/2008/August/08-ag-689.html.

[92] Brent Kendall, *Third Update: Eleven Charged With Massive Identity Theft*, CNN MONEY, Aug. 5, 2008, http://62.1.2.134/dj/news.asp?details=551805.

[93] *A Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited May 31, 2008).

[94] Kathryn E. Picanso, *Note: Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 369 n.103 (2006).

individuals,[95] and that an estimated 277 million individuals have social security numbers.[96] The President's Identity Theft Task Force reported that during a single year the records of 73 million people were lost or stolen.[97] Therefore, data breaches have likely touched a large majority of those who have records to compromise.

E. *Selected Data Breach Cases*

In January 2007, the TJX Companies announced one of the largest and most disturbing security breaches to date, which involved the theft of forty-six million credit card and debit card numbers including the personal information of at least 500,000 customers.[98] Two months later TJX realized that the true extent of the breach was almost 100 times greater and raised the number of those affected to 45.7 million.[99] TJX again increased the estimate in October 2007 to at least 94 million.[100] The theft began in the summer of 2005 in the parking lot of Marshalls, one of the retail stores owned by TJX. Hackers reportedly used a primitive "telescope-shaped antenna" with a laptop computer to access and intercept data transmitted via the store's wireless network.[101] The cost to TJX associated with the theft over the next several years

---

[95] *U.S. POPClock Projection*, US CENSUS BUREAU, http://www.census.gov/population/www/popclockus.html (last visited June 5, 2008).

[96] Barbara D. Bovbjerg, *Use of the Social Security Number Is Widespread*, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, 1 (May 9, 2000), *available at* http://www.gao.gov/archive/2000/he00111t.pdf.

[97] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 3.

[98] Dan Goodin, *Lax Security Led to TJX Breach*, THE REGISTER, May 4, 2007, http://www.theregister.co.uk/2007/05/04/txj_nonfeasance/print.html (last visited Dec. 1, 2007).

[99] Mark Jewell, *More Accounts Involved in TJX Breach,* MSNBC.COM, Oct. 24, 2007, http://www.msnbc.msn.com/id/21454847 (last visited Nov. 4, 2008).

[100] *Id. See also T.J. Maxx Owner: 46M Card Numbers Stolen*, CNNMONEY.COM, Mar. 29, 2007, http://money.cnn.com/2007/03/29/news/companies/tjx/index.htm (noting that "455,000 customers who returned merchandise without receipts had their personal data stolen, including driver's license numbers").

[101] Joseph Pereira, *How Credit Card Data Went Out the Wireless Door*, WSJ ONLINE, May 4, 2007, http://online.wsj.com/article/SB117824446226991797.html.

exclusive of insurance coverage, tax credits and possible litigation, has been estimated by Forrester Research to be over one billion dollars.[102]

In 2005, the FTC issued a complaint against BJ's Wholesale Club,[103] a membership club with eight million members.[104] When members made credit or debit card purchases, BJ's collected personal information from the magnetic stripe including card numbers, expiration dates and other information, to be used in obtaining payment authorization from the bank that issued the card.[105] In its complaint the FTC alleged that BJ's facilitated fraudulent purchases of over $13 million[106] by failing to adequately secure and protect stored information.[107] Specifically, while BJ's stored the information on its computer networks, it failed to encrypt the information, which allowed the information to be accessed anonymously. BJ's failed to employ readily available security means to limit such access or to detect unauthorized accesses, and stored the information up to thirty days after it was

---

[102] *See* Ross Kerber, *Analysts: TJX Case May Cost over $1b*, BOSTON.COM, Apr. 12, 2007, http://www.boston.com/business/personalfinance/articles/2007/04/12/analysts_tjx_case_may_cost_over_1b/?page=2. The U.S. Postal Inspection Service announced that Maksym Yastremskiy, a Ukrainian, was arrested in Turkey on suspicion of stealing and selling thousands if not millions of credit and debit card numbers stolen from TJX customers. Ross Kerber, *Suspect Named in TJX Credit Card Probe,* BOSTON.COM, Aug. 21, 2007, http://www.boston.com/business/globe/articles/2007/08/21/suspect_named_in_tjx_credit_card_probe/.

[103] Complaint, In re BJ's Wholesale Club, No. C-4148 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

[104] *BJ's Wholesale Club Settles FTC Charges*: *Agency Says Lax Security Compromised Thousands of Credit and Debit Cards*, FEDERAL TRADE COMMISSION, F.T.C. File No. 0423160, June 16, 2005, http://www.ftc.gov/opa/2005/06/bjswholesale.shtm.

[105] *Id.*

[106] *Id*.

[107] *Id.* Thieves were able to create counterfeit copies of member debit and credit cards that contained the same personal information BJ's had collected and stored. *Id*.

no longer necessary to keep it.[108] The FTC considered this an unfair practice likely to cause substantial consumer injury "that was not reasonably avoidable by consumers and not outweighed" by countervailing benefits to consumers or competition.[109] Subsequently, BJ's entered into a consent agreement with the FTC agreeing to establish and maintain a program that provided for administrative, technical and physical safeguards with audits by an independent third party to assure compliance.[110] These audits are to continue every other year for twenty years and must be submitted to the FTC.[111]

In 2005, the FTC filed a complaint against DSW Inc., a national chain of retail shoe stores, alleging that, as with BJ's, DSW failed to adequately protect personal information collected from debit and credit cards and stored on its computer networks.[112] As a result, third parties made fraudulent charges after they accessed the information contained in 1.4 million credit cards and 96,000 checking accounts.[113] DSW entered into a consent agreement with the FTC in which the terms were virtually identical to BJ's above, with the added requirement that DSW allow the FTC to monitor compliance.[114]

Retailers are only one of many access points to the raw materials needed for identity theft. Academic institutions, government bodies, and others have provided sobering examples of the vulnerability of personal data. In 2005, Ohio University

---

[108] Complaint, In re BJ's Wholesale Club, No. C-4148, 7 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

[109] *Id. See* 15 U.S.C. § 45(a) (2006) (prohibiting unfair or deceptive acts or practices in the marketplace).

[110] Decision and Order, In re BJ's Wholesale Club, No. C-4148, at 2 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

[111] *Id* at 3.

[112] Complaint, In re DSW, Inc., No. C-4157, at ¶ 7 (F.T.C. Mar. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf.

[113] *DSW Inc. Settles FTC Charges*, FEDERAL TRADE COMMISSION, Dec. 1, 2005, http://www.ftc.gov/opa/2005/12/dsw.shtm.

[114] *Id.*

(OU) suffered a series of security breaches when its Hudson Health Care Center was attacked by hackers who accessed the personal information—including social security numbers, identification numbers, addresses and medical records—of over 60,000 students.[115] The second breach involved 137,000 social security numbers and other data of over 300,000 alumni. The final breach targeted OU's Innovation Center, where hackers were able to access and compromise additional social security numbers and other personal information.[116]

In May 2006, the U.S. Veterans Affairs (VA) Department announced that a laptop belonging to one of its data analysts was stolen when his home had been burglarized.[117] At the time, the VA had no clear policy that indicated the procedure for protecting data when outside the VA's network. The laptop contained the names, social security numbers, dates of birth (including those of some of the veterans' spouses), and data related to disability ratings of approximately 26 million veterans.[118] Subsequently, on June 29, 2006 the laptop was found, and after a forensic analysis the VA indicated it found no evidence that the personal information contained in the data had been compromised.[119]

---

[115] Greg Sandoval, *University Server in Hackers' Hands for a Year*, CNETNEWS.COM, May 22, 2006, http://news.cnet.com/2102-7349_3-6074739.html.

[116] Martin H. Bosworth, *Ohio University: Data Breach Central?*, CONSUMERAFFAIRS.COM, May 15, 2006, http://www.consumeraffairs.com/news04/ 2006/05/ohio_u_data_theft.html.

[117] Greg Sandoval, *Veterans Data Swiped in Theft*, CNET NEWS, May 22, 2006, http://news.cnet.com/Veterans-data-swiped-in-theft/2100-1029_3-6075212.html.

[118] *Id. See also Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, DEPT. OF VETERANS AFFAIRS, OFFICE OF INSPECTOR GENERAL, Rep. No. 06-02238-163, July 11, 2006, at 4, *available at* http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf [hereinafter *Review of Issues*] (noting that the data was actually contained on an external hard drive that was stolen along with the laptop).

[119] *Review of Issues*, *supra* note 118, at 2. The VA suffered another smaller security breach in August 2006, when a computer containing data related to the medical records and other personal information of 18,000 veterans went missing from Unisys, a subcontractor providing software support for VA medical centers. Lisa Lerer, *Lost Laptops Law*, FORBES.COM, Sept. 27, 2006,

Many other large scale security breaches have occurred, including one involving AOL[120] and another involving LexisNexis.[121]

III. EXISTING LAW DOES NOT ADEQUATELY PROTECT CONSUMERS

In the wake of national media attention and a growing consumer voice, both federal and state legislatures have criminalized identity theft and provided stiff penalties.[122] A first-time conviction under the federal identity theft act, not in connection with violence or terrorism, carries a maximum prison term of fifteen years and can result in a fine and forfeiture of any personal property used to commit the offense.[123] Other federal statutes add an additional layer of deterrence by prohibiting crimes that may be committed concurrently with or as an adjunct to identity theft, such as credit card fraud,[124] computer fraud,[125] mail fraud,[126] wire fraud,[127] and financial institution fraud.[128] Violations of these statutes are felonies and provide for significant prison terms of up to twenty years along with forfeiture of property used to commit the offense.[129] Many state statutes provide for similarly stiff penalties.[130]

---

http://www.forbes.com/2006/09/27/lost-laptops-law-biz_cx_ll_0927laptops.html.

[120] Jim Hu, *AOL Security Breach Exposes Personal Info*, CNET NEWS, June 16, 2000, http://news.cnet.com/2102-1023_3-242034.html.

[121] Associated Press, *LexisNexis Theft Much Worse than Thought*, MSNBC, Apr. 12, 2005, http://www.msnbc.msn.com/id/7475594/ ("[I]ntruders may have accessed personal details of . . . 310,000 people.").

[122] For a list of state identity theft statutes, see *Identity Theft Statutes and Criminal Penalties*, NAT'L CONFERENCE OF STATE LEGIS., http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm (last visited June 4, 2008).

[123] 18 U.S.C. § 1028(b) (2006).

[124] *Id*. at § 1029.

[125] *Id*. at § 1030.

[126] *Id*. at § 1341.

[127] *Id*. at § 1343.

[128] *Id*. at § 1344.

[129] *See, e.g.*, 18 U.S.C. § 1029(c) (2006).

[130] *See, e.g.*, ALA. CODE § 13A-8-192 (2008); CAL. PENAL CODE 530.5 (West 2008); D.C. CODE § 22-3227.02 (2008); 720 ILL. COMP. STAT. ANN. § 5/16G-1 –

A. *The Difficulty in Deterring and Prosecuting the Identity Thief*

Despite substantial penalties and universal recognition of the problem, the crime of identity theft continues to claim millions of victims and bleed the economy of billions of dollars each year.[131] Why have identity thieves not been sufficiently deterred? The answer is in part that committing identity theft is very easy, while catching and prosecuting identity thieves is extremely difficult.[132] A Public Broadcasting Service television host reported that he was able to generate enough information to steal the identities of 300,000 people within one hour by combining new and old versions of CD-ROM databases sold by the government.[133] LifeLock, the company made famous by its one million dollar guarantee against identity theft and whose chief executive officer flaunts his real social security number in company commercials,[134] concedes that "you can't stop every form of identity theft."[135] Indeed, the CEO himself became a victim.[136] Because the "theft" of information, unlike that of physical possessions, does not deprive the owner of her property, the victim may not realize that her identity has been stolen until months or years after the fact.[137] Such a delay is more than enough time to place a large distance

---

5/16G-40 (West 2008); MASS. GEN. LAWS. ANN. 266 § 37E (West 2008); MINN. STAT. ANN. § 609.527 (West 2008); N.Y. PENAL LAW. § 190.77-190.84 (McKinney 2008).

[131] *See supra* Part II.A.

[132] *See generally* Levy & Stone, *supra* note 11 (describing identity theft as quick, easy, and low risk).

[133] *See* Robert X. Cringely, *How to Steal $65 Billion: Why Identity Theft is a Growth Industry*, PUBLIC BROADCASTING SERVICE, Sept. 11, 2003, http://www.pbs.org/cringely/pulpit/2003/pulpit_20030911_000785.html.

[134] *See* Lifelock Homepage, http://www.lifelock.com/ (last visited Nov. 4, 2008).

[135] Kim Zetter, *LifeLock Founder Resigns Amid Controversy*, WIRED, June 11, 2007, http://blog.wired.com/27bstroke6/2007/06/lifelock_founde_1.html.

[136] *Id.*

[137] Betsy Broder, Fed. Trade Comm'n, Prepared Statement of the FTC on Identity Theft to the Committee on Banking and Financial Services in the United States House of Representatives (Sept. 13, 2000), *available at* http://www.ftc.gov/os/2000/09/idthefttest.htm ("The FTC has received numerous reports from consumers who were not aware that they had been victimized . . . until four or more years after the first fraudulent transaction.").

between the thief and the victim, if they were ever in proximity at all. Estimates vary, but most agree that well over ninety percent of identity thieves are never brought to justice.[138] Even where the thief is identified, pursuing a thief in a distant or even overseas[139] forum might be cost ineffective and pose jurisdictional challenges.[140] Where a thief is both identified and caught locally, she may be impecunious. Even in the best of circumstances—where a thief is caught and returns the stolen money—the victim cannot be adequately compensated for her loss of reputation and effort spent dealing with the problem. In short, laws directed at the identity thief cannot by themselves provide an adequate remedy.

B. *Suing the Data Collector*

The high profile lawsuits pursued against Napster[141] and other file-sharing services in the early twenty-first century mainstreamed the idea of secondary liability in the minds of American consumers. These suits stood for the proposition that, if data was wrongfully transferred to a third party who could not herself be held accountable, the enabler of the transfer could be sued directly as a "secondary" wrongdoer. Thus, as newly enacted laws proved themselves powerless to sufficiently rein in identity theft—and as

---

[138] *See generally* Levy & Stone, *supra* note 11 (citing Avivah Litan, of the research firm Gartner Group, who speculates that fewer than 1 in 700 identity crimes leads to a conviction); Helen Giddings, *Staying Ahead of Identity Theft*, NAT'L NOTARY ASS'N, July 15, 2005, http://www.nationalnotary.org/news/index.cfm?Text=newsNotary&newsID=675 ("95 percent of identity thefts are never solved"); Ed Dadisho, *Identity Theft and the Police Response: The Problem*, THE POLICE CHIEF, Jan. 2005, at 25, 26, *available at* http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=493&issue_id=12005 ("Law offices reported that very few identity theft cases are solved."); John Leland, *Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, NY TIMES, July 11, 2006, at A1, *available at* http://www.nytimes.com/2006/07/11/us/11meth.html?pagewanted=print ("[M]ost [identity theft] crimes are never solved.").

[139] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 58 (noting that "a significant portion of the identity theft committed in the United States originates in other countries"); Krim, *supra* note 61 ("[A] thriving black market for the stolen data . . . exists online, run in large part from Eastern Europe.").

[140] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 59.

[141] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

the news media continued to report ever larger data security breaches—consumers naturally began to look to the enablers of identity theft for recourse. Lawsuits against data collectors could not be brought on a secondary liability theory per se because it would be difficult to allege that data collectors intentionally contributed to or financially benefited from the thefts, but the idea was essentially the same. As courts at all levels bought into the theory of secondary liability for copyright infringement, giants like Napster, Aimster, Grokster, and others were brought down in a firestorm of litigation as consumers watched with amazement.[142]

Secondary liability, of course, was nothing new, and the courts had merely extended to a new context a doctrine that was well established in nearly every area of the law.[143] Nevertheless, as newly enacted laws proved themselves powerless to sufficiently rein in identity theft and the news media continued to report on ever larger data security breaches, consumers naturally looked to what were seen as the enablers of identity theft for recourse. Lawsuits against the data collectors could not be brought on a secondary liability theory per se—it would be difficult to allege that data collectors intentionally contributed to or financially benefited from the thefts[144]—but the idea was essentially the same. If the problem could not be solved at its natural end point, perhaps it could be solved further upstream. Armed with this ideological perspective, consumers and their attorneys began to develop theories by which data collectors could be held liable when data breaches exposed sensitive information that could potentially be used by identity thieves. Three main theories were proposed:

---

[142] *E.g.*, *In re* Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[143] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984).

[144] Secondary copyright liability consists of vicarious liability and contributory liability. Vicarious liability may be found where the wrongdoer profits while failing to exercise a right to stop the wrongful activity. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005). Contributory liability occurs where a party is aware of a third party's wrongful conduct and materially contributes to it. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

breach of contract, negligence and breach of fiduciary duty. All would prove unavailing.

1. *Breach of Contract*

It has been suggested that breach of contract is the "best basis on which to bring a [loss from data breach] claim."[145] However, a breach of contract action is likely to leave the vast majority of people with little or no meaningful recourse. The FTC reports that only about one half of identity theft victims "know how the person who misused their personal information obtained it."[146] Even if the information was obtained as a result of a data breach at an organization with which the consumer had a contractual relationship, it would be difficult or impossible to discover (let alone prove to a legal certainty) which organization that was. Even if the organization is identifiable, many organizations that possess sensitive personal data do not have contractual relationships with consumers at all,[147] since they have obtained the information elsewhere.

Where a potential defendant can be identified and a contractual relationship exists, the contract is unlikely to provide a basis for a cause of action. Contracts between the individuals supplying the information and those collecting the information are frequently contracts of adhesion, drafted by the data collector. Any antecedent attempt to negotiate the liability of a medical office, university, or government entity for prospective damages associated with a contemplated future data breach is likely to be met with quizzical looks at best, and these entities have scant incentive to include such provisions on their own.

2. *Tort for Negligence*

A second possible manner of recovery is to bring an action in tort for negligence. Although some variation exists from state to

---

[145] Picanso, *supra* note 94, at 377.

[146] SYNOVATE, FEDERAL TRADE COMMISSION: IDENTITY THEFT SURVEY REPORT 9 (Sept. 2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf, at 9.

[147] Picanso, *supra* note 94, at 377.

state, a negligence action would generally require the plaintiff to establish: (1) existence of a legal duty; (2) breach of that duty; (3) causation of harm due to the breach; and (4) resulting damages.[148] In data breach cases, all four of these elements may be difficult or impossible to establish. Take the case of *Randolph v. ING Life Ins. & Annuity Co.*,[149] in which an ING employee laptop containing the private information of 13,000 people was stolen during a burglary.[150] The seven plaintiffs in the case alleged that they had or would soon have to purchase credit reports and monitoring of their credit for the indefinite future and that typical victims of identity theft spend hundreds of hours and hundreds of dollars rectifying their credit.[151] The plaintiffs did not, however, assert that they had already been the victims of identity theft. Under these facts, the court held that an increased risk of identity theft was not an "injury in fact" and that plaintiffs lacked standing.[152] Injury in fact is the "invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical."[153] Similarly, tort law allows recovery only if the plaintiff has suffered injury to a "legally protected interest."[154] Since the plaintiffs in *ING* did not suffer injury to a legally protected interest, they also would be unable to establish the damages element of a negligence action.[155]

---

[148] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635 (7th Cir. 2007); Kahle v. Litton Loan Servicing Co., 486 F.Supp.2d 705, 706 (S.D. Ohio 2007); Alcoa, Inc. v. Behringer, 235 S.W.3d 456, 459 (Tex. App. 2007).

[149] 486 F. Supp. 2d 1 (D.D.C. 2007).

[150] *Id*. at 1.

[151] *Id*. at 2.

[152] *Id*. at 5. Other courts have reached similar conclusions. In *Ponder v. Pfizer, Inc.*, a laptop of a Pfizer employee containing social security numbers of 17,000 employees was stolen. 522 F.Supp.2d 793 (M.D. La. 2007). The court held that there is no injury until "the compromised data are actually used by a third party to steal someone's identity." *Id.* at 4 n.5. *See* Key v. DSW Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006) (holding that plaintiff lacked standing).

[153] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (internal quotations omitted).

[154] Gibson v. Trant, 58 S.W.3d 103, 111 (Tenn. 2001).

[155] Although the two concepts are not identical, plaintiffs seeking to establish injury-in-fact for purposes of standing must make a showing similar to (but perhaps somewhat lower than) that required to establish the damages element of

Some courts have found an injury-in-fact sufficient for purposes of standing but not for purposes of establishing damages. In the Seventh Circuit case of *Pisciotta v. Old National Bancorp*,[156] a sophisticated and malicious hacker obtained access to the private information of tens of thousands of users of Old National Bancorp's website.[157] Like the plaintiffs in most data breach cases brought to date, the plaintiffs in *Pisciotta* did not allege that any members of their putative class had already been victims of identity theft. Rather than dismiss the case for lack of subject matter jurisdiction, the court held that the plaintiffs had alleged an injury in fact sufficient to confer standing[158] but ultimately concluded that plaintiffs had not suffered a compensable injury.[159] In reaching its decision, the court noted that the Indiana legislature had enacted a data breach statute specifically in response to the data breach at issue in the case. Although the statute was not retroactive and thus did not apply to the case at bar, the court found important the fact that the statute provided for no private right of action and "impose[d] no duty to compensate affected individuals."[160] Other courts have reached similar conclusions.[161]

---

a negligence action. *See* Kahle v. Litton Loan Servicing Co., 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007) (noting that the standard for establishing standing is not the standard for establishing damages in a tort action); Key v. DSW Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006) ("By dismissing all of Plaintiff's claims for lack of standing [because Plaintiff failed to allege that she suffered an injury-in-fact], the Court also finds that Plaintiff has not alleged cognizable damages sufficient to state a contract, negligence . . . or, breach of fiduciary duty claim.").

[156] 499 F.3d 629 (7th Cir. 2007).

[157] *Id.* at 631.

[158] *Id.* at 634.

[159] *Id.* at 640.

[160] *Id.* at 637.

[161] *See, e.g.*, Shafran v. Harley Davidson, Inc., 2008 U.S. Dist. LEXIS 22494, at *5 (S.D.N.Y. Mar. 24, 2008) (noting that all courts considering the issue of whether the time and money spent guarding against identity theft is a compensable injury have answered in the negative); Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483, at *4 & *6 (D. Minn. Feb. 7, 2006) (holding that where laptop containing private customer data was stolen from the home of one of defendant's employees, defendant was not liable, given that it complied with the relevant provisions of the Gramm-Leach-Bliley Act and had not breached any duty of care; furthermore, an increased risk of identity theft was not sufficient to constitute an injury under a negligence standard.); Kahle v.

Harm of the type sustained by victims of data breaches should be compensable, even where identity theft cannot be established. The Restatement (Second) of Torts states: "One whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made . . . in a reasonable effort to avert the harm threatened."[162] This rationale was applied in *Kuhn v. Capital One Financial Corporation*,[163] where eighteen fraudulent accounts were opened in Kuhn's name after her personal information was compromised.[164] Although she was not held responsible for any charges on those accounts, the court found a compensable injury in the "time spent . . . seeking to prevent or undo the harm,"[165] citing the provision contained in the Restatement.

The proposition that preventing future harm should be compensable finds analogous support in the contractual duty to mitigate. In general, damages in breach of contract cases are only recoverable to the extent that the non-breaching party could not have avoided them by taking reasonable measures.[166] This suggests that where a contractual relationship exists between an individual and a data collector and that data collector experiences a data breach that violates its contractual obligations with respect to the data, the individual would only be able to recover for damages that could not have been avoided by undertaking reasonable mitigation measures. If credit monitoring and other costs are not compensable, then this leaves the individual in a Catch-22. If she takes no preventative action and identity theft later occurs, then the data collector can argue that she should be unable to recover for those losses that she could have prevented by taking reasonable measures. If she takes preventative action, then she is precluded

---

Litton Loan Servicing Co., 486 F. Supp. 2d 705 (S.D. Ohio 2007) (finding that "credit monitoring costs are not sufficient injury where no fraud has occurred" in case where hard drives containing information on 229,501 former customers were stolen); Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005).

[162] RESTATEMENT (SECOND) OF TORTS § 919 (1979).

[163] 2006 WL 3007931 (Appeals Ct. of Mass. Oct. 23, 2006).

[164] *Id.* at *1.

[165] *Id.* at *3 (internal quotations omitted).

[166] RESTATEMENT (SECOND) OF CONTRACTS § 350 (1981).

from recovering the costs of that action from the data collector. In contrast, contract law generally allows for the recovery of incidental costs incurred by the non-breaching party to prevent anticipated losses: "Inasmuch as the law denies recovery for losses that can be avoided by reasonable effort and expense, justice requires that the risks incident to such effort should be carried by the party whose wrongful conduct makes them necessary."[167]

Causation may be equally difficult to establish. Hundreds of thousands of organizations—both public and private, domestic and foreign—may possess the private information of a given individual. Even if the individual has already experienced identity theft and is able to establish damages, she will face the nearly insurmountable challenge of proving that a given data breach was causally connected to the loss.[168] Even where only two organizations containing an individual's private data have experienced data breaches, it may be equally likely that the thief obtained the data from either source. Thus, the plaintiff would be unable to prove causation by even the minimal "preponderance of the evidence" standard.[169] In reality, creative thieves have innumerable options for obtaining private data, including phishing schemes, rifling through trash bins, examining public records, and simply buying information outright from a data broker for a nominal fee.[170] Therefore, even if a data breach victim could prove that her information was compromised by a particular defendant and later misused by a particular identity thief, she would have no

[167] Brandon & Tibbs v. George Kevorkian Accountancy Corp., 226 Cal.App.3d 442, 461 (Cal. Ct. App. 1990) (citing 5 ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 1044 (1964)).

[168] Picanso, *supra* note 94, at 380 ("Many security breaches and instances of identity theft are never solved, leaving injured parties unable to show with absolute certainty that a particular security breach caused their harm.").

[169] *See* Sanchez v. Monumental Life Ins. Co., 102 F.3d 398, 404 (9th Cir. 1996) (preponderance of the evidence standard requires party to prove that her claim is "more likely than not").

[170] Jonathan Krim, *Social Security Data Still Ripe for Picking*, SEATTLE TIMES, Apr. 17, 2005, at E1 (noting that social security numbers may be purchased online for as little as $35).

way of connecting the two events with any measurable certainty,[171] except in the unlikely event that the thief was caught and confessed.

3. *Tort for Breach of a Fiduciary Duty*

A third possible manner of recovery is the tort for breach of a fiduciary duty. Using the lack of standing and the traditional "economic loss" rule[172] theories for denying recovery advanced above, courts have not yet accepted breach of a fiduciary duty as a viable theory for recovery in data security breach cases.[173] Furthermore, courts have been reluctant to assign fiduciary status to individuals engaged in commercial transactions.[174]

Notwithstanding the current state of the law in this area, the fiduciary liability theory has been largely untested and should

---

[171] *See* Walters v. DHL Express, 2006 WL 1314132, at *5 (C.D. Ill. May 12, 2006) ("[D]amages would be based upon speculation as to . . . [whether the identity theft was] caused by Defendant's actions, rather than anyone else's . . . .").

[172] *See* Derek A. Bishop, *No Harm No Foul: Limits on Damages Awards for Individuals Subject to a Data Breach*, 4 SHIDLER J.L. COM. & TECH. 12 (2008) (noting that traditional tort law will not allow recovery for economic loss without evidence of physical harm and that contract law is better suited for such claims); *see also* Banknorth NA v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206 (M.D. Pa. 2006) (dismissing negligence claim of plaintiff credit card issuer against defendant retailer for the cost of reissuing credit cards after data breach of defendant, as the economic loss rule did not allow recovery absent physical harm).

[173] *See, e.g.*, Shafran v. Harley Davidson, Inc., 2008 U.S. Dist. LEXIS 22494, at *7 n.2 (S.D.N.Y. Mar. 24, 2008) (without actual injury, fiduciary duty claim must be dismissed); Key v. DSW Inc., 454 F.Supp.2d 684, 685 (S.D. Ohio 2006) ("By dismissing all of Plaintiff's claims for lack of standing, the Court also finds that Plaintiff has not alleged cognizable damages sufficient to state a . . . breach of fiduciary duty claim."); Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793 (M.D. La. 2007) (concluding that data exposure, without more, is not a compensable injury and granting a motion to dismiss all claims despite allegation of fiduciary relationship).

[174] *See* PulseCard, Inc. v. Discover Card Services, Inc., 917 F. Supp. 1488, 1493 (D. Kan. 1996) ("[F]iduciary obligations should be extended reluctantly to commercial or business transactions."); Terra Venture Inc. v. JDN Real Estate-Overland Park, L.P., 443 F.3d 1240, 1246 (10th Cir. 2006) ("We do not presume the existence of fiduciary duties and extend them to commercial transactions, where parties deal at arm's length for their mutual profit.").

therefore be considered further.[175] Most plaintiffs in data breach cases have not even alleged fiduciary duty.[176] Where fiduciary duty has been alleged, it has been pursued half-heartedly by plaintiffs and treated with little or no discussion by the courts.[177] To be viable, a plaintiff would have to establish that entrusting the data collector with personal information, especially one's social security number, springs into existence a quasi-fiduciary relationship that is more similar to an agency[178] than to an arm's-length relationship. As a fiduciary, it could be argued a data collector entrusted with personal identifiable information would assume the duty to act for the benefit of the consumer upon matters within the scope of the relationship.[179] Specifically, this duty would include loyalty, trust, and confidentiality—acting in the consumer's best interest to prevent unauthorized access to and use of the confidential information.[180] The duty of confidentiality is analogous to that arising from the attorney-client or physician-patient relationships. Those relationships certainly require the

---

[175] *See generally* Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1122 (2007) (advocating for the imposition of a fiduciary duty on data aggregators).

[176] *See, e.g.*, TRW Inc. v. Andrews, 534 U.S. 19 (2000); Randolph v. ING Life Insurance and Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007); Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 at 4 (D. Ariz. Sept. 6, 2005); Bell v. Axciom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); Spikings v. Cost Plus Inc., No. CV 06-8125-JFW (AJWx), 2007 U.S. Dist. LEXIS 44214 (C.D. Cal. May 25, 2007).

[177] *See*, *e.g.*, Guin v. Brazos Higher Education Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *2 (D. Minn. Feb. 7, 2006) (plaintiff voluntarily dismisses fiduciary duty claim); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020 n.2 (D. Minn. 2006) (plaintiff does not pursue fiduciary duty claim); Key v. DSW Inc., 454 F. Supp. 2d 684, 685 (S.D. Ohio 2006) ("By dismissing all of Plaintiff's claims for lack of standing, the Court also finds that Plaintiff has not alleged cognizable damages sufficient to state a . . . breach of fiduciary duty claim.").

[178] *See* RESTATEMENT (THIRD) OF AGENCY § 8.01 (2006) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship.").

[179] RESTATEMENT (SECOND) OF TORTS § 874 cmt. a (1979).

[180] *See id.* at § 874 ("One standing in a fiduciary relation with another is subject to liability to the other for harm resulting from a breach of duty imposed by the relation.").

physician and attorney to take whatever steps are necessary to protect the confidentiality (and unauthorized access and release) of client or patient information.[181] Similarly, data collectors should take whatever steps are necessary to safeguard the security of a consumer's personal information.

That a fiduciary duty exists (or should be held to exist) between a data collector and the individuals whose data is the subject of collection is a proposition that already finds support in current state and federal law. In a data breach case involving the failure to safeguard information of union members, the Michigan Court of Appeals proclaimed that "society has a right to expect that personal information divulged in confidence . . . will be guarded with the utmost care."[182] At the federal level, both the Gramm-Leach-Bliley Act (GLB)[183] and the Health Insurance Portability and Accountability Act (HIPAA)[184] include provisions designed to protect confidential information.[185] The provisions of GLB apply

---

[181] *See* MODEL RULES OF PROF. CONDUCT R. 1.6(a) (2007) ("A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure" is reasonably believed to be necessary to prevent death, substantial bodily harm, or crime, or in certain other limited circumstances.); AM. INST. OF CERTIFIED PUB. ACCOUNTANTS CODE OF PROF. CONDUCT R. 301 (1999) (requiring that a member in public practice cannot divulge confidential client information without the specific consent of the client). State rules also prohibit such disclosures. *See, e.g.*, N.Y. BD. OF REGENTS R. 29.1(b)(8) (2006), *available at* http://www.op.nysed.gov/part29.htm (Unprofessional conduct includes the "revealing of personally identifiable facts, data or information obtained in a professional capacity without the prior consent of the patient or client, except as authorized or required by law.").

[182] Bell v. Michigan Council 25, No. 246684, 2005 WL 356306, at *3 (Mich. Ct. App. Feb. 15, 2005) (limiting its holding to "where defendant knew confidential information was leaving its premises" and failed to implement any security procedures).

[183] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6801–6810).

[184] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of the U.S.C.).

[185] *See* 15 U.S.C. § 6801 (2006) ("It is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the

to financial institutions—including, but not limited to, banks, credit unions, mortgage companies, insurance companies, and brokerages—that offer financial goods and services.[186] GLB provides that a financial institution must obtain customers' consent before disclosing or sharing their personal identifiable information.[187] HIPAA applies to health care providers, clearinghouses, health plans including those offered by employers, and to those offering or providing services that include the electronic transmission of personal health information.[188] The regulations promulgated pursuant to HIPAA similarly require that the consent of the patient must be obtained before personal health information can be released or shared.[189]

As with the contract and negligence theories discussed above, the lack of actual damages could be an obstacle for the plaintiff's success in an action in tort for breach of a fiduciary duty against the data collector.[190] Courts have yet to award damages for time, money, and effort expended by data breach victims in attempting to prevent potential future economic losses including those that could result from identity theft,[191] deeming the claim for these

---

privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.").

[186] 15 U.S.C. § 6805(a)(1) – (7) (2006).

[187] 15 U.S.C. § 6802 (2006). GLB provides for an *opt-out* notice requirement which puts the onus on the customer to refuse to allow the financial institution to disclose or share personal information. *Id*. at § 6802(b).

[188] 42 U.S.C. § 1320d–1(a) (2008); *see also* 45 C.F.R. § 160.103 (2008).

[189] 45 C.F.R. §§ 164.506, 508 (2008).

[190] *See supra* Part III.B.2.

[191] *See* Walters v. DHL Express, No. 05-1255, 2006 WL 1314132, at *5 (C.D. Ill. May 12, 2006) (dismissing claim for damages for an increased risk of identity theft as speculative); Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *5 (D. Minn. Feb. 7, 2006) (rejecting claim that an increased risk of identity theft constituted damages, where a laptop containing sensitive information was stolen but there was no evidence of any identity theft); Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906, at *4 (D. Ariz. Sept. 6, 2005) (dismissing case where hard drives containing personal information were stolen from defendant's facility, reasoning that plaintiffs must, at a minimum, establish "1) significant exposure of sensitive personal information, 2) a significantly increased risk of identity fraud as a result of that exposure and 3) the necessity

damages to be speculative.[192] Given the plethora of data breaches that have occurred and are increasingly occurring,[193] legislation comparable to GLB and HIPAA is needed to strengthen security and protection of personal information in the possession of data brokers, with liability attaching for data breaches even where identity theft cannot be proven.

A prime example of the need for new and more stringent legislation is the case of *United States v. ChoicePoint*.[194] Since 1997, ChoicePoint has been selling an enormous variety of personal information including names, social security numbers, birth dates, bank and credit card account numbers and credit histories, police records, and claims histories.[195] Its customers include entities in both the public and private sectors. In 2005, ChoicePoint reported that it had inadvertently sold the personal information of 145,000 consumers to a group of identity thieves.[196] As a result, the Federal Trade Commission (FTC) filed a complaint[197] in which it alleged that ChoicePoint had violated

---

and effectiveness of credit monitoring in detecting, treating and/or preventing identity fraud.").

[192] *See, e.g.*, Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.D.C. 2007) (declining to award damages when theft of defendant's laptop computer exposed plaintiff's data, as any claim of damages was "mere speculation"); *see also* Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (holding that damages for time and money spent in obtaining credit monitoring, absent proof of actual unauthorized use, were speculative).

[193] Krebs, *supra* note 74.

[194] United States v. ChoicePoint, Inc., No. 1:06-cv-00198-JTC (N.D. Ga. Feb. 15, 2006).

[195] For more information about ChoicePoint and a description of the data they collect and provide, *see* ChoicePoint.com, *Overview*, http://www.choicepoint.com/about/overview.html (last visited July 7, 2008).

[196] *See* Matt Hines, *ChoicePoint Data Theft Widens to 145,000 People*, ZDNET NEWS, Feb. 18, 2005, http://news.zdnet.com/2100-1009_22-5582144.html. The number was later raised to 163,000. Jon Brodkin, *ChoicePoint Details Data Breach Lessons*, PC WORLD, Jun 11, 2007, http://www.pcworld.com/article/132795/choicepoint_details_data_breach_lessons.html.

[197] Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. ChoicePoint, No. 106-CV-0198 (Jan. 30, 2006), http://www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm.

various sections of the Fair Credit Reporting Act[198] and that these violations also constituted unfair or deceptive business practices under the FTC Act.[199] ChoicePoint entered into a settlement with the FTC, the terms of which included the payment of $10 million in civil penalties and $5 million in consumer redress.[200] ChoicePoint also agreed to comprehensive security audits every two years until the year 2026 and to conduct site visits of its subscribers to verify their authenticity.[201]

It is interesting to note Senator Patrick Leahy's (D. Vermont) pertinent comment regarding the ChoicePoint incident: "Their actions were an irresponsible violation of a fiduciary relationship they have with their customers."[202] While ChoicePoint might be reluctant to concede any legally binding fiduciary relationship, its mission statement provides a subtle acknowledgement of the security risks inherent in its business: "*We strive to create a safer and more secure society through the responsible use of information*."[203]

---

[198] *See, e.g.*, 15 U.S.C. §1681b (2008) (prohibiting a consumer reporting agency from providing consumer reports except for legitimate and permissible purposes); 15 U.S.C. § 1681c(a) (requiring a consumer reporting agency to employ reasonable efforts to verify the identity of its subscribers and to establish the uses for which the information sought is to be used).

[199] *See* 15 U.S.C. § 45(a) (2008).

[200] Stipulated Final Judgment and Order for Civil Penalties, In re ChoicePoint, No. 106-CV-0198, at 4 & 17 (Feb. 10, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf; Jaikumar Vijayan, *FTC Imposes $10M Fine Against ChoicePoint for Data Breach*, COMPUTERWORLD, Jan. 26, 2006, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,108069,00.html.

[201] Stipulated Final Judgment and Order for Civil Penalties, In re ChoicePoint, No. 106-CV-0198, at 6, 16-17 (Feb. 10, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

[202] Grant Gross, *Senators Rip into ChoicePoint, Bank of America on Data Losses,* COMPUTERWORLD, Mar. 11, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,100334,00.html?source=x73.

[203] ChoicePoint.com, *Vision and Mission*, http://www.choicepoint.com/about/overview/vision_mission.html (last visited July 7, 2008).

C. *Government Action Highlights Problems and Points Toward Solutions*

While the front line of data collecting entities has so far done relatively little to alter its data collection practices, there is reason to believe that meaningful change is just around the corner. The casual and unrestrained collection, use, transfer, sale, display, and disclosure of social security numbers has received increasingly vocal criticism and—due to its connection with identity theft—attracted attention at the highest levels of government. The Government Accountability Office has generated over twenty reports since 2002 directly addressing the use (and misuse) of social security numbers and generally recommending reform.[204] The FTC has testified before the House Committee on Ways and Means, urging "comprehensive reviews of both private and public sector usage of SSNs."[205] Consumers Union, the publisher of the widely-respected Consumer Reports magazine, has urged states to adopt its model legislation which would impose sensible restrictions on the use of social security numbers.[206] Most notably, in 2006 President Bush issued an executive order establishing a

---

[204] *E.g.*, U.S. GAO, Pub. No. GAO-06-495, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs* (May 17, 2006); U.S. GAO, Pub. No. GAO-06-238, *Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs* (Jan. 23, 2006); U.S. GAO, Pub. No. GAO-05-1016T, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain* (Sept. 15, 2005); U.S. GAO, Pub. No. GAO-04-1099T, *Social Security Numbers*: *Use Is Widespread and Protections Vary in Private and Public Sectors* (Sept. 28, 2004). A search of the GAO website for the term "social security numbers" revealed an impressive eighty-three reports since 1978, with sixty-three of these since 1995.

[205] Fed. Trade Comm'n, *Protecting the Privacy of the Social Security Number from Identity Theft*, Prepared Statement of the Federal Trade Commission, Subcommittee on Social Security of the House Ways and Means Committee, June 21, 2007, *available at* http://www.ftc.gov/os/testimony/P065409socsectest.pdf.

[206] ConsumersUnion.org, *Model State SSN Protection Law*, http://www.consumersunion.org/pub/core_financial_services/004800.html (last visited June 6, 2008).

task force to address the problem of identity theft.[207] Finally, both state legislatures and Congress have begun to answer these collective calls for reform by enacting legislation aimed at the core problems of indiscriminate data collection and, more commonly, social security number misuse.

1. *State Notice of Breach Statutes*

States have responded to the incidents at ChoicePoint, TJX, BJ's, DSW, and others by enacting statutes that require consumer notification in the case of a data breach. At least forty-four states have enacted some type of breach notification law to date,[208] imposing a number of breach-related costs on businesses. In addition to the direct costs of mailing letters and responding to consumer inquiries, businesses face an increased risk of litigation and the discomfort of public embarrassment.[209] At the same time, the hodgepodge of state law requirements is unnecessarily confusing and has led to calls for federal action.[210] Although there are bills pending in the U.S. Congress that would require notification upon breach,[211] none has yet passed.

2. *State Social Security Number Statutes*

Since 2001, states across the country have also been busily enacting legislation that restricts the ability of entities to publicly

---

[207] Exec. Order No. 13402, 71 Fed. Reg. 27,945 (May 10, 2006). The task force included the United States Attorney General (who was to serve as chair), the Chairman of the FTC (who would serve as co-chair), the Commissioner of Social Security, and the Secretaries of the Treasury, Commerce, Health and Human Services, Veteran's Affairs, and Homeland Security departments, among others.

[208] *See* Nat'l Conf. of State Legislatures, *State Security Breach Notification Laws*, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Aug. 1, 2008); *see also Notice of Security Breach State Laws*, CONSUMERS UNION, Aug. 21, 2007, http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf.

[209] *Cost of a Data Breach*, PONEMON INSTITUTE, Oct. 2006, at 2, http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf (last visited Aug. 1, 2008) .

[210] *See* Faulkner, *supra* note 175, at 1107.

[211] *E.g.*, Notification of Risk to Personal Data Act, S. 239, 110th Cong. (2007); Federal Agency Data Breach Protection Act, H.R. 2124, 110th Cong. (2007).

display and use the social security number. For example, California law now prohibits "a person or entity" from "[p]ublicly . . . display[ing] . . . an individual's social security number," "[p]rinting an individual's social security number on any card required for the individual to access products or services provided by the person or entity" or "[r]equir[ing] an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted."[212] Since January 1, 2008, New York has prohibited most private entities from making social security numbers available to the public, from printing them on any "card or tag required for the individual to access products, services or benefits," and from requiring individuals to transfer social security numbers unencrypted over the Internet.[213] More than twenty other states now have similar laws on the books,[214] and a few states have gone even further in protecting consumers. Minnesota and New Mexico, for example, require entities that do choose to use social security numbers to restrict access to employees who need such access to perform job duties.[215]

Unfortunately, legislation in almost all states is riddled with flaws and exceptions. Michigan, for example, allows the public display of up to four sequential digits of the social security number, but does not specify which four.[216] This leaves open the possibility that publicly available records could be combined to create complete social security numbers, a problem identified in a

---

[212] CAL. CIV. CODE § 1798.85(a) (West 2008). *Cf.* COLO. REV. STAT. § 6-1-715(1)(c) (West 2008); CONN. GEN. STAT. § 42-470(b)(3) (West 2008); GA. CODE ANN. § 10-1-393.8(a)(2) (West 2008); HAW. REV. STAT. § 487J-2(3) (2008); 815 ILL. COMP. STAT. 505/2RR(a)(3) (West 2008); MD. CODE ANN., COM. LAW § 14-3402(a)(3) (West 2008); MICH. COMP. LAWS § 445.83(1)(d) (West 2008); N.J. STAT. ANN. § 56:8-164(5) (West 2008); N.Y. GEN. BUS. LAW § 399-dd(2)(c) (McKinney 2008).

[213] N.Y. GEN. BUS. L . § 399-dd(2) (McKinney 2008).

[214] *See Notice of Security Breach State Laws*, CONSUMERSUNION.ORG, Aug. 21, 2007, http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf, at n.7.

[215] *See* MINN. STAT. ANN. § 325E.59(a)(7)(b) (West 2008). *Cf.* N.M. STAT. ANN. § 57-12B-3(D) (West 2008).

[216] MICH. COMP. LAWS § 445.83 (West 2008).

2006 General Accountability Office Report, which recommended federal legislation to standardize truncation practices.[217] Similarly, New Mexico's statute allows sufficient leeway for entities to make publicly available any eight of the nine digits in an individual's social security number.[218] Furthermore, government entities are granted exceptions under some state statutes,[219] and even if no statutory exception is available, a government entity may be able to take refuge under the doctrine of sovereign immunity.[220] In any event, state attorneys general may be reluctant to bring an action against an arm of the state for continuing longstanding data collection practices. Some states prohibit the use of the social security number as a primary identifier of an individual's account, but apparently allow its use as a secondary or higher-order identifier.[221] Most states exempt public records, severely impairing the statutes' prophylactic effects.[222]

Many of these state statutes are also riddled with exceptions for and limits on remedies against private entities. Businesses may continue to share social security numbers with affiliates and multiple levels of contractors, in some cases with explicit statutory

---

[217] U.S. GAO, Pub. No. GAO-06-495, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs* (May 17, 2006).

[218] N.M. STAT. ANN. § 57-12B-4(A)(1) (West 2008).

[219] *See, e.g.*, MINN. STAT. ANN. § 325E.59(a) & subdiv. 5 (West 2008) (excluding government entities other than state colleges and universities); OKLA. STAT. tit. 40, § 173.1(A)(2) (West 2008) (excluding the state and political subdivisions thereof); 74 PA. STAT. ANN. § 201(e)-(f) (West 2008); TEX. BUS. & COM. CODE ANN. § 35.58(b) (Vernon 2008).

[220] *See, e.g.*, McNichols v. Commonwealth, 804 A.2d 1264, 1267 (Pa. Commw. Ct. 2002) ("Wrongful discharge . . . is not one of the enumerated exceptions [to sovereign immunity].").

[221] *See, e.g.*, MINN. STAT. ANN. § 325E.59(a)(6) (West 2008).

[222] CAL. CIV. CODE § 1798.85(c) (West 2008); *cf.* COLO. REV. STAT. § 6-1-715(4) (West 2008) (exempting public records from the statute's purview); HAW. REV. STAT. § 487J-2(b)(11) (2008); 815 ILL. COMP. STAT. 505/2RR(d) (West 2008); MICH. COMP. LAWS § 445.83(g)(iv) (West 2008); MINN. STAT. ANN. § 325E.59 subdiv. 4 (West 2008); MO. REV. STAT. § 407.1355(4); N.M. STAT. ANN. § 57-12B-3(B)(3) (West 2008); VA. CODE ANN. § 59.1-443.2(D) (West 2008).

blessing.[223] In every state except Rhode Island and Maine, entities may use the social security number for "internal verification or administrative purposes,"[224] which would appear to condone the continued use of the number as a password. Penalties for violation of these statutes tend to be small.[225] Grandfather provisions allow entities engaged in use of social security numbers to continue that use even after the legislation becomes effective.[226] The right to sue is sometimes limited to state attorneys general or other public bodies, leaving consumers without direct recourse.[227]

---

[223] HAW. REV. STAT. § 487J-2(b)(8) (2008).

[224] CAL. CIV. CODE § 1798.85(b) (West 2008); CONN. GEN. STAT. § 42-470(d) (West 2008); GA. CODE ANN. § 10-1-393.8(b)(3) (West 2008); HAW. REV. STAT. § 487J-2(b)(9) (2008); 815 ILL. COMP. STAT. 505/2RR(c) (West 2008); KAN. STAT. ANN § 75-3520(b)(3)(B) (West 2008); MD. CODE ANN., COM. LAW § 14-3402(b)(3) (West 2008); MINN. STAT. ANN. § 325E.59 subdiv. 3 (West 2008); MO. REV. STAT. § 407.1355(3); N.J. STAT. ANN. § 56:8-164(b) (West 2008); N.M. STAT. ANN. § 57-12B-4(B)(2)(c) (West 2008); N.Y. GEN. BUS. LAW § 399-dd(3) (McKinney 2008); N.C. GEN. STAT. § 75-62(b)(2) (West 2008); OKLA. STAT. tit. 40, § 173.1(C) (West 2008); 74 PA. STAT. ANN. § 201(d) (West 2008).

[225] *See, e.g.*, CONN. GEN. STAT. § 42-470(e) (West 2008) (capping liability at $100 for first-time violators); ARK. CODE. ANN. § 4-86-107(f) (West 2008) (capping liability at $250 per violation); ARIZ. REV. STAT. § 44-1373(I) (2008) (capping liability at $500 dollars); 74 PA. STAT. ANN. § 201(g) (West 2008) (capping liability at $500 for first time violators); R.I. GEN. LAWS § 6-48-17 (2008) (imposing criminal penalties of up to $500); TEX. BUS. & COM. CODE ANN. 35.58(b) (Vernon 2008) ($500); KAN. STAT. ANN § 75-3520(c) (West 2008) (capping liability at $1000 per violation). In contrast, New York law provides for penalties of up to $100,000 for first time violations where multiple violations result from a single act or incident. N.Y. GEN. BUS. LAW § 399-dd(6) (McKinney 2008).

[226] *See, e.g.*, ARIZ. REV. STAT. § 44-1373(B) (2008); COLO. REV. STAT. § 6-1-715(2) (West 2008); 815 ILL. COMP. STAT. 505/2RR(b) (West 2008); MD. CODE ANN., COM. LAW § 14-3403 (West 2008); MICH. COMP. LAWS § 445.83(3)(b) (West 2008); N.M. STAT. ANN. § 57-12B-4(B) (West 2008); 74 PA. STAT. ANN. § 201(c) (West 2008).

[227] *See, e.g.*, ARIZ. REV. STAT. § 44-1373(H) (2008); ARK. CODE. ANN. § 4-86-107(f) (West 2008) (authorizing the attorney general to bring suit); N.Y. GEN. BUS. LAW § 399-dd(6) (McKinney 2008). One exception is Rhode Island, which allows consumer-plaintiffs to recover damages, attorney fees and costs. R.I. GEN. LAWS § 6-48-17(c) (2008).

On the other hand, Kansas, Rhode Island, Maine, and New Mexico have gone beyond the use and display restrictions characteristic of most state statutes and have directly attacked the foundational problem of indiscriminate social security number collection. Both Rhode Island and Maine have enacted concise statutes that prohibit conditioning the receipt of goods or services on the provision of a social security number.[228] The statutes in these states contain few exceptions and probably constitute the most consumer-favorable legislation to date.

The attempts in Kansas and New Mexico, while having positive attributes, suffer from significant shortcomings. Kansas limits the ability of private entities to ask an individual for her social security number "unless such number is necessary for [the entity's] normal course of business and there is a specific use for such number for which no other identifying number may be used."[229] However, as in most states, the provision does not apply with respect to "internal verification or administrative purposes,"[230] an exception that would seem to nearly swallow the rule. The Kansas legislation attempts to plug the hole created by the public record exemption by providing that documents available for public inspection may not contain both a social security number and other personal information such as name and address.[231] Still, court documents and records of deeds are exempted;[232] despite well-meaning intentions, the legislation essentially directs identity thieves to locations where social security numbers can still be

---

[228] R.I. GEN. LAWS § 6-48-17 (2008); 10 MAINE REV. STAT. § 1272-B (2008).

[229] KAN. STAT. ANN § 75-3520(b) (West 2008).

[230] KAN. STAT. ANN § 75-3520(b)(3)(B) (West 2008); *cf.* CONN. GEN. STAT. § 42-470(d) (West 2008); GA. CODE ANN. § 10-1-393.8(b)(3) (West 2008); HAW. REV. STAT. § 487J-2(b)(9) (2008); 815 ILL. COMP. STAT. 505/2RR(c) (West 2008); KAN. STAT. ANN § 75-3520(b)(3)(B) (West 2008); MD. CODE ANN., COM. LAW § 14-3402(b)(3) (West 2008); MINN. STAT. ANN. § 325E.59 subdiv. 3 (West 2008); MO. REV. STAT. § 407.1355(3) (West 2008); N.J. STAT. ANN. § 56:8-164(b) (West 2008); N.M. STAT. ANN. § 57-12B-4(B)(2)(c) (West 2008); N.Y. GEN. BUS. LAW § 399-dd(3) (McKinney 2008); N.C. GEN. STAT. § 75-62(b)(2) (West 2008); OKLA. STAT. tit. 40, § 173.1(C) (West 2008); 74 PA. STAT. ANN. § 201(d) (West 2008).

[231] KAN. STAT. ANN. § 75-3520(a)(1) (West 2008).

[232] KAN. STAT. ANN. § 75-3520(b)(2) (West 2008).

found.[233] Actions under the Kansas law may be brought by "aggrieved" individuals,[234] making it unclear whether proof of harm is required. As discussed above, proof of harm with respect to data exposure can be problematic.[235]

New Mexico similarly prohibits businesses from "requir[ing] a consumer's social security number as a condition for the consumer to lease or purchase products, goods or services from the business."[236] However, this broad protection is undermined by allowing the exception of consent.[237] This means that businesses may still require the completion of forms that request the social security number. Even though consumers are not obligated to provide it, only those who are savvy and bold enough to challenge the status quo by leaving the social security number field blank would benefit. Only New York—which, unlike New Mexico, does not prohibit the collection of social security numbers in the first instance—has recognized this type of problem and proactively addressed it. Entities in New York cannot bypass the statute's requirements by including waiver provisions in their contracts with customers; such purported waivers are statutorily determined to be against public policy and therefore void.[238]

Some exceptions to the prohibition on social security number use are clearly warranted. Entities deciding whether or not to extend credit, for example, must have a way of reliably locating an individual's credit history. Employers and others have legitimate needs to conduct background checks in order to ensure a safe work environment. With the few exceptions noted above, however, state legislation so far enacted contains exceptions so numerous and

---

[233] *See* Christopher Lee, *GAO: Social Security Numbers Vulnerable*, WASH. POST, Nov. 12, 2004, at A23 ("Identity thieves can snare Social Security numbers from a potpourri of public records, especially those maintained by state and local governments . . . .").

[234] KAN. STAT. ANN. § 75-3520(c) (West 2008); *cf.* N.Y. GEN. BUS. LAW § 399-dd(6) (McKinney 2008) (proof of damages not required).

[235] *See supra* Part II.B.

[236] N.M. STAT. ANN. § 57-12B-3(A) (West 2008).

[237] N.M. STAT. ANN. § 57-12B-3(C) (West 2008); *cf.* OKLA. STAT. tit. 40, § 173.1(C) (West 2008) (providing a written consent exception for employees with respect to their employers).

[238] N.Y. GEN. BUS. LAW § 399-dd(5) (McKinney 2008).

substantial as to eviscerate their *raison d'être*. In short, the statutes tend to be more form than substance. With alluring names like the "Social Security Number Privacy Act,"[239] they appear to be aimed at pacifying those concerned about identity theft, but the provisions themselves fail to reflect the fortitude needed to produce meaningful change.

State laws restricting social security number use exist in other contexts as well. New York, for example, prohibits educational institutions from using the social security number on student rosters and identification cards.[240] Arizona and Rhode Island similarly prohibit universities from assigning either faculty or student identification numbers that are identical to social security numbers.[241] Texas restricts the use of social security numbers provided to merchants in connection with merchandise returns, and requires that records containing the number collected for this purpose be destroyed within six months after collection.[242]

While these state laws shed light on the damaging misuse of social security numbers, they largely fail to address the core problem: the use of the social security number as a skeleton key by which the consumer—or an identity thief—can access multiple accounts. Most states that have enacted social security number use legislation prohibit the use of social security numbers to access websites, unless a password is also required to access the site.[243] Because these restrictions only apply to account access via the Internet, however, they leave open the possibility that an identity thief could use a social security number to access an account by telephone, fax, letter, in-person communication, or any other manner that does not involve the Internet. Moreover, an identity

---

[239] *See, e.g.*, Social Security Number Privacy Act, 2004 Mich. Pub. Acts 454 (effective Mar. 1, 2005); Social Security Privacy Act, Acts 2005 Md. Laws c. 521 (effective Jan. 1, 2006); The Consumer Empowerment and Identity Theft Prevention Act of 2006, 2006 R.I. Pub. Laws c. 226 (effective June 29, 2006).

[240] N.Y. EDUC. LAW § 2-b (McKinney 2008).

[241] ARIZ. REV. STAT. ANN. § 15-1823 (2008); R.I. GEN. LAWS § 16-38-5.1 (2008).

[242] TEX. BUS. & COM. CODE ANN. § 35.581 (Vernon 2008).

[243] *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-1373(A)(4) (2008); N.Y. GEN. BUS. LAW § 399-dd(2)(d) (McKinney 2008).

thief in possession of a social security number also would be halfway to unlocking accounts over the Internet, lacking only the password. Similarly, the use of truncated social security numbers as passwords is a specious tactic that suffers from a serious flaw. If entities provide account access based upon only the last four digits (or other variant) of a social security number, this does little to thwart criminal activity—the thief now needs only four digits to access the account instead of nine. A much better system would encourage the use of identifiers that are unique to a given organization, so that if the numerical key fell into the wrong hands, it would facilitate access to only one account rather than all accounts. Moreover, using a number other than the social security number would mean that it would be relatively easy to change that number if necessary, just as one can change locks when a physical key is lost or stolen.

3. *Federal Statutes*

Even if the aforementioned shortcomings of the state statutes were rectified, regulation at the state level has two main disadvantages. First, multiple inconsistent systems of compliance can be confusing and expensive. Because organizations normally maintain only one website that serves customers in multiple states, website interfaces must comply with all of the various state requirements. Similarly, since paper solicitations are often mailed across state lines, entities must either tailor multiple solicitations to individual states or develop a single solicitation that meets the requirements of all of the states.[244] Second, because widely stored information is only as secure as its most vulnerable point of access, social security number confidentiality is limited by the state with the weakest laws.

Acknowledging the nationwide scope of the problem, Congress has considered a number of major social security number protection bills.[245] Although none of these has passed, more

[244] Krebs, *supra* note 74 (quoting a spokesman of an organization that experienced a data breach: "More time was spent researching various state laws than trying to figure out how to remedy the problem.").

[245] *See, e.g.*, Safeguarding Social Security Numbers Act, S. 2915, 110th Cong. (2008); Social Security Number Misuse Prevention Act, S. 238, 110th Cong.

limited measures have succeeded.[246] In 1974, Congress enacted the Privacy Act, which prohibited "any Federal, State or local government agency from denying any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."[247] However, as with recent state legislation, the social security number provision was primarily symbolic; due to its substantial exceptions, it had little effect on the collection and use of social security numbers.[248] Another relatively narrow federal provision dictates that social security numbers obtained by government officials pursuant to laws enacted on or after October 1, 1990, must be maintained as confidential and not disclosed.[249] Prior to 1994, many states generated substantial revenue from selling social security numbers and other personal information that was required to be provided by driver's license applicants.[250] The Driver's Privacy Protection Act of 1994 ended this lucrative practice by restricting the sharing or sale of information collected by states when issuing driver's licenses.[251] Ten years later, the Intelligence Reform and Terrorism Prevention Act banned the display of social security numbers on

---

(2008); Social Security Number Fraud and Identity Theft Prevention Act, S. 699, 110th Cong. (2008); The Social Security Number Privacy and Identity Theft Prevention Act, H.R. 3046, 110th Cong. (2007); The Social Security Number Protection Act, H.R. 948, 110th Cong. (2007); Stop the Theft of Our Social Security Numbers Act, H.R. 2518, 109th Cong. (2005); Social Security Number Privacy and Identity Theft Prevention Act, S. 2801, 108th Cong. (2004); Social Security Number Protection Act, H.R. 4513, 107th Cong. (2002); Social Security Number Protection Act, S. 451, 107th Cong. (2001).

[246] For a comprehensive table of federal statutes and actions relating to the use of social security numbers, see CRS REPORT FOR CONGRESS, *supra* note 7, at 15-31.

[247] Privacy Act of 1974, Pub. L. No. 93-579, § 7(A) (1), 88 Stat 1896 (1974).

[248] *See* Privacy Protection Study Commission, *Personal Privacy in an Information Society*, at 612-13 (1977) ("In short, the Privacy Act and the Tax Reform Act essentially preserved the status quo with respect to the SSN: namely, widespread collection and use of the number.").

[249] 42 U.S.C. § 405(c)(2)(C)(viii)(I).

[250] Reno v. Condon, 528 U.S. 141, 143 (2000); *see also* Bloom, *supra* note 6, at 49 ("[S]tate and local governments have sought to reap economic benefit from their databases by selling them commercially.").

[251] Pub. L. No. 103-322, § 300001, 108 Stat. 1796, 2099 (1994) (codified as amended at 18 U.S.C. §§ 2721-2725 (1994)).

state driver's licenses and motor vehicle registrations.[252] Another act, the promisingly-titled "Social Security Number Confidentiality Act," has also been signed into law but contains only the most modest mandate that social security numbers not be visible on or through unopened mailings of government checks.[253] Additional protection at the federal level is provided in limited circumstances pursuant to the Family Educational Rights and Privacy Act,[254] the Fair Credit Reporting Act,[255] the Health Insurance Portability and Accountability Act of 1996,[256] the Gramm-Leach-Bliley Act,[257] the Freedom of Information Act,[258] and others.[259]

Fortunately, federal agencies are improving social security number practices even absent legislation. The Social Security Administration, for example, truncates social security numbers on the annual benefit statements sent to millions of Americans.[260] The Thrift Savings Plan, a retirement savings plan similar to 401(k) plans for federal government employees, replaced the social security number as an account identifier with an unrelated thirteen-digit identifier.[261] The departments of Defense and Veterans Affairs are eliminating social security numbers from employee

---

[252] Pub. L. No. 108-458, § 2714, 118 Stat. 3638, 3832 (2004) (codified at 42 U.S.C. § 405 (2004)).

[253] Pub. L. No. 106-433, 114 Stat. 1910 (2000) (codified at 31 U.S.C. § 3327 (2000)).

[254] Pub. L. No. 93-568, 88 Stat. 1858 (1974) (codified as amended at 20 U.S.C. § 1232g (1974)).

[255] Pub. L. No. 90-321, 84 Stat. 1128 (1968) (codified as amended at 15 U.S.C. § 1681 (1968)).

[256] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of the U.S.C. (1996)).

[257] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. §§ 6801-6810 (1999)).

[258] Pub. L. No. 89-554, 80 Stat. 383 (1966) (codified as amended at 5 U.S.C. § 552 (1966)).

[259] *See generally* PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at 31-32 (discussing GLB, FCRA, HIPAA, and others); CRS REPORT FOR CONGRESS, *supra* note 7, at 8 (discussing FERPA and FOIA).

[260] *How Is Social Security Protecting Social Security Numbers?*, SOCIAL SECURITY ONLINE, http://ssa-custhelp.ssa.gov/cgi-bin/ssa.cfg/php/enduser/std_adp.php?p_faqid=1122 (last visited June 11, 2008).

[261] *Frequently Asked Questions*, THRIFT SAVINGS PLAN, http://www.tsp.gov/faq/faqacctnum.html (last visited June 10, 2008).

identification cards and health insurance cards.[262] In the private sector, financial institutions are exploring alternatives to the use of the social security number.[263]

IV. PROPOSED STATUTES AND RECOMMENDATIONS

A. *Establish Laws that Internalize Current Externalities*

Although courts have held that plaintiffs in data breach cases have not suffered compensable loss, every year victims of identity theft collectively spend an astounding 300 million hours and $5 billion reestablishing their credit history.[264] Moreover, there are considerable consequences to consumers beyond mere time and money, including harassment from creditors, denial or loss of employment, denial of driver's licenses and the right to vote, loss of reputation, and even time spent in jail.[265] Victims of data breaches also lose peace of mind. Once private data is stolen there is no period of time after which a plaintiff can rest assured that the risk of identity theft has passed. As noted previously, social security numbers cannot easily be changed, and patient thieves may wait years before utilizing the information in the hope that

---

[262] Christopher Lee, *GAO: Social Security Numbers Vulnerable*, WASH. POST, Nov. 12, 2004, at A23.

[263] McCall, *supra* note 75.

[264] *Identity Theft Survey Report*, FEDERAL TRADE COMMISSION, Sept. 2003, at 6, http://www.ftc.gov/os/2003/09/synovatereport.pdf. Texas State Representative Helen Giddings, herself a victim of identity theft, claims to have spent over 1,000 hours and $4,000 addressing the problem. Giddings, *supra* note 138. The Privacy Rights Clearinghouse reports that, according to one survey, individual victims spent an average of 175 hours trying to resolve problems caused by identity theft, and that fewer than half were able to resolve their case within two years. *Nowhere to Turn: Victims Speak Out on Identity Theft*, May 2000, http://www.privacyrights.org/ar/idtheft2000.htm. The legislative history of the Federal Identity Theft & Assumption Deterrence Act included discussion of a couple that had spent over four years and $15,000 restoring their credit. Identity Theft and Assumption Deterrence Act of 1998, 144 Cong. Rec. 24.382 (1998) (Statement of Mr. Shadegg).

[265] *Prepared Statement of the FTC on Identity Theft*, Sept. 13, 2000, § II.A., http://www.ftc.gov/os/2000/09/idthefttest.htm.

consumers will let their guard down or cease credit monitoring.[266] These "emotional distress" losses are difficult to quantify but clearly exist.[267]

Such costs are externalities that are fueled by the collection and aggregation of data, in the sense that the data aggregator is engaged in an activity for which someone else bears the costs. Furthermore, the party bearing the risk of loss is separate and distinct from the party that is in a position to reduce the risk of loss.[268] As a consequence, the loss does not itself provide sufficient motivation to take preventative measures.[269] If the free market is unable to motivate the desired result of loss mitigation or prevention, then it is the role of the law to correct this market failure.[270]

A much better approach to reducing losses stemming from data breaches is to place the liability for such losses on the data collectors.[271] Such an allocation of liability would encourage data collectors to weigh the benefits of data collection against the costs flowing from potential breaches. Businesses and government

---

[266] *Cf.* Leibling, P.C. v. Mellon PSFS (NJ) Nat'l Assoc., 710 A.2d 1067 (N.J. Super. Ct. Law Div. 1998) (holding that where defendant cashed a check over an expired stop payment order nineteen months after issuance, plaintiff had no cause of action against the bank that paid the instrument). *See also Data Breaches Are Frequent, supra* note 34, at 29.

[267] In a letter from Attorney General Alberto Gonzalez to President Bush, Gonzalez acknowledged that identity theft "exacts a heavy . . . emotional toll from its victims" and "that its effects can range far beyond financial harm." PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27, at viii-ix.

[268] *See* Solove, *supra* note 23, at 1259 ("Exhortations to individuals to guard their data place the onus on the wrong parties.").

[269] *See generally* Levy & Stone, *supra* note 11 (noting that data security is lax because "the companies charged with safeguarding the information don't suffer the consequences when it's compromised").

[270] *See* RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 75 (Harvard University Press 1981) ("The basic function of law in an economic or wealth-maximization perspective is to alter incentives."); NICHOLAS MERCURO & STEVEN G. MEDEMA, ECONOMICS AND THE LAW 57 (Princeton University Press 1997) ("[L]egal decision making should promote efficiency.").

[271] *See* Tolbert v. Gerber Indus., Inc., 255 N.W.2d 362, 370 (Minn. 1977) (Kelly, J., dissenting) ("The loss in an accident situation should fall on the party who can, with the minimum cost, (1) take the precautions necessary to avoid the accident and (2) insure and spread the loss.").

entities would likely choose to forego the collection of information that is not truly needed for the operation of the business or whose value to the business is marginal.[272] Employers might delay the collection of social security numbers and other personal information from employment applicants until after a job offer is made or at least until after the applicant has progressed far enough in the process to warrant a background check. Instead of using a social security number, data collectors might choose to use a unique identification number whose theft would not enable access to a customer's other accounts. When data collectors decide that sensitive personal information is truly necessary, they would be motivated to weigh the costs of encryption and other safeguards against the potential losses from data breach. Under a liability regime, data collectors might restrict employee access to sensitive personal information or may adopt data purging policies under which data is erased after it becomes irrelevant.

Breach notification laws begin to internalize externalities by creating the specter of erosion of both an organization's bottom line and its reputation, thereby providing some incentive to improve data collection and use practices.[273] The Ponemon Institute estimates the average direct cost to a company as a result of a data breach, in states with notice-of-breach laws, is $54 per lost record, a figure that climbs to $182 per record when loss of goodwill and other costs are taken into account.[274] Even so, notification laws suffer from serious flaws. First, they are reactive rather than proactive, since the brunt of their force is aimed at mitigating problems after they occur. The circumstances surrounding data breaches aptly illustrate the maxim that an ounce of prevention is worth a pound of cure. Why subject data to

---

[272] *See* Krim, *supra* note 61, at D5 ("[I]ndustry players have not responded aggressively enough because they are insulated from the financial consequences of breaches.").

[273] *Data Breaches Are Frequent, supra* note 34, at 32 n.48.

[274] *Cost of a Data Breach*, PONEMON INSTITUTE, Oct. 2006, at 2, http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf; Forrester Research placed the cost even higher, at $90 to $305 per record. Sharon Gaudin, *Security Breaches Cost $90 to $305 per Lost Record*, INFORMATION WEEK, Apr. 11, 2007, http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222.

possible theft and misuse when such data could be collected later, purged earlier, secured better, or not collected at all?[275] Second, because the costs to a business imposed by notification laws are based on the occurrence of uncertain future events, these costs may tend to be undervalued by organizations that are more concerned with current profitability than with long term efficiency. Third, a proliferation of breach notices for breaches of varying risk levels could desensitize consumers and lead to unresponsiveness when a substantial threat exists. Finally, notice of breach statutes primarily leave to consumers the burden of dealing with the consequences of a breach in which they played no role.

These flaws in the current notification laws provide the motivation for enacting a federal law that allows affected individuals to recover specified statutory damages in the event of a data breach.[276] Such a law would avoid the difficult proof and damages problems that exist under current law and would partially compensate breach victims for their losses.[277] Statutory damages would also benefit data collectors. By placing a fixed dollar value on a record of data, data collectors could make rational and quantitatively based cost-benefit decisions regarding data collection and security practices. Clearly placing liability on data collectors is also likely to motivate prevention efforts that reduce losses.[278] The costs of these prevention efforts will be borne

[275] That information should only be collected for a "specific and legitimate purpose" is a "standard hallmark" of data privacy practice. *See* Ellen Nakashima, *European Lawmaker to Sue U.S. Over Data*, WASH. POST, July 1, 2008, at D3, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/06/30/AR2008063001895.html.

[276] In the rare case in which actual damages could be proven with certainty, the law should, and probably already does, allow for the awarding of these damages. The proposed statutory damages statute should not change this result.

[277] Congress has already endorsed statutory damages as a tool for deterring lax data security practices potentially connected to identity theft. *See* 15 U.S.C. § 1681n (a) (2006); 15 U.S.C. § 1681c (g) (2006) (providing statutory damages of $100 to $1000 plus attorneys fees and punitive damages for willful failure to comply with certain provisions of Title 15, including a provision prohibiting the display of more than five digits of a credit card number on receipts).

[278] *See* Picanso, *supra* note 94, at 373 (2006) ("Fears of litigation could actually play a stronger role in motivating businesses to dedicate more resources to information security than compliance with governmental regulations . . . .").

broadly by consumers, in contrast to the current system where the costs of lax information collection practices are borne by those whose private information has been compromised and especially by those who eventually become victims of identity theft. Finally, placing liability on data collectors allows for the free market to produce the most efficient data collection and security practices, a result unlikely to be achieved by statutorily enumerating specific prohibitions or requirements.

B. *Restrict Unnecessary Collection and Use of the Social Security Number*

The social security number has become so entangled with current business practices that it may not be easy to completely disentangle it. Imposing liability on data collectors for data breaches will help to facilitate such disentanglement in the least proscriptive means possible. At the same time, a few simple minima should be established that would substantially reduce the chances of certain types of identity theft.

First, and most importantly, a federal law should prohibit the use of the social security number as a password.[279] Such a prohibition would prevent the use by identity thieves of a single, unchangeable "skeleton key" to access a wide range of an individual's accounts.[280] For similar reasons, birthdays, mother's maiden names, and other non-changeable and widely-available data should be prohibited as passwords.[281] Exceptions could be made for limited activities that pose minimum risks to an account. For example, it is desirable that an individual who loses a credit card can cancel the card immediately rather than wait until she

---

[279] *See* Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277, 1279 (2003) ("[N]o one should be entitled to assume that I am you, simply because I know your social security number.").

[280] A skeleton key is a master key that will open a wide variety of locks. Service and security personnel sometimes carry skeleton keys in order to allow access to multiple rooms in a building without the need to carry around hundreds of different keys.

[281] *See* Solove, *supra* note 23, at 1260 ("SSNs, birth dates, and mother's maiden names would not expose people to identity theft if this data were not used by companies as a way to verify identity.").

locates her password at home. The use of a social security number as a password by an individual could be allowed for this limited purpose, as it entails a minimal risk of loss.

Second, the display of the social security number should be curtailed. The federal government should follow the lead of some states by prohibiting employers, educational institutions, and others from using the social security number as the primary means of identification. In order to keep social security numbers out of wallets, the display of social security numbers on most identification cards should be prohibited. By restricting the appearance of social security numbers on most documents sent through the mail, the ability of identity thieves to practice their trade by rifling through mailboxes or trash bins will be reduced. Of course, such measures will be largely in vain if social security numbers continue to appear in publicly available records. Therefore, social security numbers should not be collected for most public records; where social security numbers are required by law or by necessity, the records should be redacted before being made available to the public.

Third, a government body should undertake further study and make policy changes. Understanding the impact of social security number restrictions on business and government practices is no simple task, and it would be reckless to advocate sweeping new laws without understanding their impact. The FTC should therefore be authorized to study the problem and promulgate regulations to restrict the unnecessary collection, use, display, transfer, and sale of the social security number. The FTC also should be authorized to establish minimum data security and disposal procedures to be followed when private data must be collected or used. Furthermore, the FTC should be required to examine the effectiveness of the various state laws already passed in formulating its regulations. Any resulting federal laws or regulations should supersede state laws in order to impose the minimum possible impact on businesses and other organizations, which would be unnecessarily burdened by varying state requirements.

The overarching goal should be to reduce the dissemination and exposure of data that is linked to identity theft. Several general principles should be more fully developed by the FTC. First, the social security number should not be collected in all cases where another number would suffice. This would significantly mitigate the problem by reducing the number of points of data vulnerability. Second, in most cases, social security numbers should not be shared with or sold to third parties such as affiliates, contractors, or government entities. For example, employers could be required to establish and use secondary identification numbers in place of the social security number when providing information to contractors under outsourcing arrangements. These secondary identification numbers would be unique to the organization and the impact of their loss would therefore be limited. Third, appropriate security measures, such as encryption, should be mandated and should be flexible enough to accommodate varying levels of data sensitivity and other circumstances. Finally, regulations prescribing appropriate policies for data retention and disposal should be developed in order to encourage the timely and proper disposal of data once it is no longer needed. By restricting the use of social security numbers as passwords, limiting their public display, and promulgating flexible, nationwide regulations after careful study, the thoughtless and damaging overuse of social security numbers can be brought under control with minimal impact on business.

V. CONCLUSION

In 1935, proponents of the social security system justified its passage by arguing that, in light of the dramatic societal changes of the time, a person "might become a victim of circumstances far beyond his control . . . ."[282] In an ironic twist, and more than seventy years later, the social security number itself constitutes a key factor in the uncontrollable circumstances that are annually turning millions of consumers into identity theft victims.

---

[282] Frances Perkins, *Social Insurance for the U.S.* (National Radio Address), Feb. 25, 1935, *available at* http://www.ssa.gov/history/perkinsradio.html.

Certainly, identity theft is a problem of prodigious magnitude,[283] and this article makes no attempt to comprehensively address it. Instead, this article explains how current information collection practices, particularly with respect to the social security number, create an unnecessary risk of loss. Modest changes to information collection practices and related regulations and laws would help to reduce the incidence of certain types of identity theft. At worst, these small changes will create a more equitable system, aligning more closely the interests of those who collect and use social security numbers with those whom they identify, and reduce consumer perceptions of helplessness that result from the control of personal information by anonymous and widely-dispersed third parties. At best, these changes may have a significant impact on the prevalence of identity theft. Even if this latter goal is not achieved, the mere jurisprudential recognition of the value of social security number privacy will promote a culture where individuals will feel comfortable responsibly guarding their personal information. As with preventing terrorism, three hundred million cautious and aware individuals can do more to avoid identity theft than the best laws or law enforcement in the world.

It is not suggested that Americans need be distrustful of either their government or private businesses when those entities collect data. Instead, data collecting entities are doing what rational actors would do when faced with similar circumstances: they are collecting data that might possibly be useful because the cost of doing so is difficult to measure and is primarily borne by others. While data breach notification laws increase the expenses to data collecting entities associated with some data breaches and thereby bring these entities' interests into greater alignment with those of the individuals whose data is being collected, notification laws do not fully internalize externalities nor do they address the fundamental imbalance created when one entity holds valuable property of another without accepting accountability for the value of that property or for its loss or misuse. Fortunately, a number of relatively simple reforms can appropriately place accountability on data collecting entities and increase consumer confidence in data

[283] *See generally* PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 27.

collection and usage practices, all while thwarting the ever-present and opportunistic identity thief.