COMBATING IDENTITY THEFT: A COMPREHENSIVE ANALYSIS OF THE FEDERAL FRAMEWORK FOR IDENTITY THEFT REGULATIONS

By

KATE E. LUCENTE

A THESIS PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ARTS IN MASS COMMUNICATION

UNIVERSITY OF FLORIDA

2009

To my husband

ACKNOWLEDGMENTS

I thank my husband for his incredible support throughout this research process and during my entire course of studies at the University of Florida. I thank my mom and my dad for their constant encouragement. I thank the members of my supervisory committee for their invaluable feedback on this study. I am especially grateful to the chair of my supervisory committee for the attention and support he dedicated to supervising me through this research and to mentoring me all the way through my legal and graduate studies.

TABLE OF CONTENTS

page

Abstract of Thesis Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Master of Arts in Mass Communication

COMBATING IDENTITY THEFT: A COMPREHENSIVE ANALYSIS OF THE FEDERAL FRAMEWORK FOR IDENTITY THEFT REGULATIONS

By

Kate E. Lucente

May 2009

Chair: William Chamberlin
Major: Mass Communication

This study presents a comprehensive analysis of federal identity theft laws, rules and regulations. Identity theft is a growing problem in the United States today largely because information technology and electronic means of communication have led to the widespread availability and accessibility of personal information. The Information Age has significantly altered the way individuals, businesses and government bodies use information. Since information is now largely stored, created, sold, shared and accessed electronically, it is both easier to use and more valuable. However, it is also more susceptible to misuse by identity thieves.

Federal law does not adequately account for the privacy implications raised by the rapid progression of information technology and fundamental changes in the character of information. Identity theft crimes have risen dramatically over the past decade but the federal government's response to this growing threat has been mixed. Congress has passed three criminal identity theft laws since 1998 and also amended some information privacy laws that regulate the financial, credit and health care industries. However, these laws are limited in scope and largely inapplicable to the information sharing practices of numerous businesses that collect and share

personal information. There is no one federal law that governs the information practices of all public or private records holders or sets minimum standards for personal information privacy and protection.

In order to fully and coherently understand exactly how federal law targets identity theft and to identify weaknesses in the current federal approach, this study comprehensively analyzes the laws that make up the fragmented federal framework of identity theft protections. The study also examines the contours of identity theft by analyzing the empirical data that is currently available on the prevalence and characteristics of identity theft crimes. Ultimately, this study seeks to identify the current shortcomings of federal identity theft protections in order to offer potential legislative or regulatory solutions to the problem of identity theft.

Examination of prior research highlighted several specific problems associated with identity theft which hinder efforts to combat the crime. While there is a large body of research on identity theft, none of the research synthesizes and comprehensively analyzes all of the major issues surrounding the issue. To offer a coherent overview of the current federal framework for identity theft protection, this study analyzes all of the current federal laws relevant to identity theft protection. This study also identifies the weaknesses in current federal approach, by analyzing federal laws and enforcement measures in light of the major identity theft issues identified in prior research. Ultimately, this study presents some possible ways that the federal government may bolster current identity theft protections and develop effective solutions for a long-term approach to adequately and effectively combat identity theft.

CHAPTER 1
RESEARCH PROPOSAL

Introduction

According to the Federal Trade Commission (FTC), "identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes."[1] There are numerous reasons someone might fraudulently use the identity of another person.[2] For example, an undocumented immigrant to the United States might adopt another's identity in order to apply for a job or receive certain government benefits. Medical providers might use an individual's personal information to bill public or private insurance companies for services that were never rendered. On the other hand, an individual might use another's identity to obtain medical services.[3] Someone may use the identity of another to apply for a driver's license or even to rent a house. A criminal might use someone else's identity to avoid having criminal charges placed on his or her record or to avoid being arrested, based on an outstanding warrant, during a routine traffic stop.[4] In some instances, thieves actually create fictitious identities by piecing together

[1] FTC.gov, Identity Theft Site, About Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited March 20, 2009).

[2] *Id*. According to the FTC, an identity thief may use a stolen identity to commit any number of frauds, including credit card fraud, phone/utilities fraud, bank/finance fraud and document fraud. *Id*. Phone or utilities fraud includes, opening a new cell phone account in someone else's names. *Id*. Document fraud includes using someone else's identity to file a fraudulent tax return or access governments. *Id*.

[3] FED. BUREAU OF INVESTIGATION (FBI), FIN. CRIMES REP. TO THE PUB.: FISCAL YEAR 2006 (Oct. 1 2005 – Sept. 30, 2006), *available at* http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm (last visited March 10, 2009).

[4] *See* FTC.gov, About Identity Theft, *supra* note 1.

bits of personal information, often from more than one consumer, with invented information.[5] Most commonly, however, thieves use the personal information of their victims to obtain money, goods or services. This form of identity theft is often referred to as financial identity theft and sometimes simply as identity theft, while other fraudulent uses of an individual's personal identity, such as document fraud, are often classified under the broader term "identity fraud."[6]

Financial identity theft is the focus of this thesis. For the purposes of this thesis, "identity theft" and "financial identity theft" will be used synonymously to describe the theft of one individual's identity for financial purposes, such as accessing or applying for credit, loans or other accounts. "Synthetic identity theft" will be used to describe financial identity thefts that involve a combination of authentic and fictitious personal information pieced together to create an entirely new identity. Any other fraudulent uses of an individual's identity, for non-financial purposes, will be referred as "identity fraud."

---

[5] *See, e.g.*, Chris J. Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97, 101 (2007). In synthetic identity theft, for example:

> an impostor [may use] the victim's SSN with a fake name, thus creating a new, 'synthetic' identity . . . . A synthetic identity—sometimes supplemented with artfully created credit histories— can then be used to apply for credit. While it may sound improbable, this approach to opening new lines of credit is generally successful for two reasons. First, some lenders will give accounts to individuals with no credit history. A synthetic identity simply has a "thinner" credit file—a characteristic consistent with a legitimate new customer who is just entering the credit market. Second, the use of a real SSN may allow impostors to satisfy a lender's security measures; there is mounting evidence that credit issuers use the SSN for both identification and authentication, that is, to locate the applicant's credit file and to prove that the credit file belongs to the applicant. *Id.*

See also, FTC, 2006 IDENTITY THEFT SURVEY 24 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (last accessed March 10, 2009) (describing in brief synthetic identity theft and explaining that its survey does not include information on synthetic identity theft).

[6] *See, e.g.*, FTC.gov, About Identity Theft, *supra* note 1.

Identity thieves obtain the information necessary for their crimes through a variety of methods, from "dumpster diving" and purse snatching to phishing[7] and hacking.[8] There is no shortage of information in an age where computers and the Internet have become ubiquitous fixtures in American lives.[9] Information is stored, accessed and traded more readily than ever before, which increases the potential for misuse of personal information.[10]

According to the FTC, identity thefts have risen substantially since 2000.[11] The reasons for the increase in identity theft seem readily apparent at first glance: the advent of the Internet and the recent technology boom. However, the problem with this general assumption is that the

[7] "Phishing" is "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly." Merriam-Webster Dictionary and Thesaurus (online edition), *phishing*, http://merriam-webster.com/dictionary/phishing (last visited March 10, 2009).

[8] "Hacking" is to "gain access to a computer illegally." Merriam-Webster, Dictionary and Thesaurus (online edition), *hacking*, http://merriam-webster.com/dictionary/hacking (last visited March 10, 2009).

[9] More than 70% of adults use the Internet, and at least 72% of American Internet users use the Internet daily. Pew Internet & American Life Project, *Internet Usage Over Time* (through Dec. 31, 2008), http://www.pewinternet.org/trends/UsageOverTime.xls (last visited March 10, 2009). 91% of adults have sent e-mails, 72% have read the news online, and 52% use the Internet at work. *Id*. As of April 2008, 55 % of American adults subscribe to high-speed internet at home. Pew Internet & American Life Project, *Home Broadband Adoption* (2008), http://pewinternet.org/pdfs/PIP_Broadband_2008.pdf (last visited March 10, 2009).

[10] *See, e.g.*, Martin E. Halstuk & Bill F. Chamberlin, *The Freedom of Information Act 1966-2006: A Retrospective on the Rise of Privacy Protection over the Public Interest in Knowing What the Government's Up To*, 11 COMM. L. & POL'Y 511 (2006) (discussing federal legislator's attempts to respond to the "unprecedented invasions of privacy ranging from identity theft and illegal surveillance to the instant and mass dissemination of private—even intimate—personal information on the Internet"); *see also* Chris Barnstable-Brown, *Developments in Banking and Financial Law: 2006-2007: V. Data Security*, 26 Ann. Rev. Banking & Fin. L. 38, 38 (2007) ("with the rise of information technology and the spread of databases that record almost every detail of nearly every individual's personal information, almost no citizen or customer can go totally unnoticed."); Terrance J. Keenan, *The FACT Act of 2003: Securing Personal Information in an Age of Identity Theft*, 2 SHIDLER J.L. COM. & TECH. 5, para. 4 (2005) (reporting that surveys have shown that as of 2005 phishing attacks have reached more than 57 million adults, which is in part because "the speed of technological advancement and widespread use of information technology have provided identity thieves with new, more readily-available sources of personal information"); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1462 (2001) (discussing the recent shift towards an information-based society).

[11] *See* FBI, FINANCIAL CRIMES REPORT, *supra* note 3.

precise reasons for the rise in identity thefts are not entirely clear.[12] This uncertainty makes it difficult to pinpoint the specific reasons that identity theft has grown, which in turn makes it difficult for lawmakers to enact laws that effectively combat identity theft.

Another barrier to understanding identity theft is that most of the data available on the crime comes from the self-reporting of victims in response to surveys.[13] So, nobody knows with certainty how widespread identity theft is, how much it affects the economy, or how effective recent efforts to curb its threat have been.[14] This uncertainty hampers government efforts to combat identity theft.

Congress, for its part, has enacted, amended and proposed several laws over the past ten years that are aimed, at least partially, at mitigating the threat of identity theft.[15] While there is

[12] FTC, 2006 IDENTITY THEFT SURVEY 30 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (last visited March 10, 2009). The FTC reported that 59% of identity theft victims did not know how their information was obtained; 16% knew the thief personally; 7% reported the theft occurred as a result of a purchase or transaction; 5% had their wallet stolen; 5% reported that the information was stolen from a company that had their information; 2% reported that the information was garnered through the victim's mail; 1% cited hacking; 1% cited phishing; and 7% cited some other way. *Id*.

[13] Hoofnagle, *supra* note 5, at 99.

[14] *See, e.g.*, FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 30; *see also* Hoofnagle, *supra* note 5, at 99; THE WORLD PRIVACY FORUM, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU (2006), *available at* http://www.worldprivacy forum.org/pdf/wpf_medicalidtheft2006.pdf. (last visited March 10, 2009).

[15] *See* Chris Barnstable-Brown, *Developments in Banking and Financial Law: 2006-2007: V. Data Security*, 26 ANN. REV. BANKING & FIN. L. 38, 38 (2007) (discussing federal actions regarding information privacy from 2006-2007); Reesa Benkoff, *Developments in Banking and Financial Law: 2005: Combating Identity Theft*, 25 ANN. REV. BANKING & FIN. L. 127 (2006) (discussing federal identity theft initiatives from Dec. 2004-2005); Andrew Capalbo, *Developments in Banking and Financial Law: 2004: III. Consumer Credit: B. Consumer Privacy*, 24 ANN. REV. BANKING & FIN. L. 42 (2005) (discussing 2004 federal consumer privacy initiatives); Young Han, *Developments in Banking and Financial Law: 2003: VI. Developments in Consumer Credit*, 23 ANN. REV. BANKING & FIN. L. 72 (2004) (discussing 2003 identity theft initiatives involving the consumer credit system); David Koenigsberg, *Developments in Banking and Financial Law: 2005: XII. Security with Online Banking*, 25 ANN. REV. BANKING & FIN. L. 118, 119 (2006) (discussing federal actions regarding identity theft in 2005); J. Ryan McCarthy & Anita Pancholi, *Developments in Banking and Financial Law: 2003: Privacy*, 23 ANN. REV. BANKING & FIN. L. 123 (2004) (discussing federal legislative initiatives during 2003 that implicated individual privacy).

no shortage of literature on identity theft, none of the literature located comprehensively examines the federal framework for identity theft protection. Rather, most of the identity theft literature focuses on a particular aspect of the problem, in order to advocate a particular solution. For example, author and privacy expert Daniel K. Solove has advocated for increased regulation of the information sharing practices of both public and private entities.[16]

The goal of this thesis is to examine the problem of identity theft and illuminate some potential solutions. To that end, this study will attempt to: (1) examine the data on the prevalence of identity theft in the United States, as well as its causes and effects; (2) analyze the federal government's current approach to combating identity theft, including existing federal regulations, proposed legislation, and the FTC's regulatory policies and practices with respect to information sharing; (3) identify the deficiencies in the current system of identity theft regulations; and (4) evaluate relevant proposals and solutions to the problem of identity theft.

Review of the Literature

Reports on the growing threat of identity theft in the United States have sparked widespread public concern. Amidst this growing concern, there has also been much debate over the realities of the identity theft problem. Unfortunately, the available empirical data on identity theft offers little in the way of conclusive explanations.[17] While it is generally accepted that

[16] *See, e.g.*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

[17] *See, e.g.*, J. Howard Beales, III & Timothy J. Muris, *Symposium: Surveillance: Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 125 (2008) (explaining that the decrease in the number of identity thefts reported by one survey group. Javelin Strategy and Research, may not be statistically significant).

identity theft financially harms consumers, creditors and retailers, as well as the economy as a whole, the true extent of the crime remains unclear.[18]

Similarly, there is no real consensus on either the root causes of identity theft, or exactly why such thefts have risen markedly over the past decade. Surrounded by all these uncertainties, Congress, scholars and professionals continue to debate how to effectively and efficiently deal with the problem of identity theft. In other words, how should the federal government regulate the collection, sharing, use and accessibility of personal information, with respect to both government and private record holders?

Identity Theft: Prevalence and Cost

The data available on the rates of identity theft is confusing and somewhat contradictory. Identity theft is purportedly one of the fastest growing crimes in the United States, and according to the FBI, it is the fastest growing white-collar crime in the United States.[19] Further, reported identity thefts are by far the most common consumer complaint the FTC receives.[20] In 2003, the FTC reported that identity thefts had grown markedly since 2000. However, based upon the available reports, it is unclear whether the number of identity thefts is still increasing.[21]

---

[18] *See, e.g.*, GRAEME R. NEWMAN & MEGAN MCNALLY, REPORT PREPARED FOR THE U.S. DEPT. OF JUSTICE, IDENTITY THEFT LITERATURE REVIEW ix-x (2005), *available at* http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf (discussing in general terms the harm identity theft causes but stating that the extent of the harm is unknown) (last visited March 10, 2009).

[19] *See* FBI, FINANCIAL CRIMES REPORT, *supra* note 3.

[20] FTC, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA JANUARY– DECEMBER 2007 7 (Feb. 2008), *available at* http://www.ftc.gov/sentinel/ reports/sentinel-annual-reports/sentinel-cy2007.pdf. In 2007, identity theft accounted for 32% of all consumer complaints received by the FTC. *Id*. The second most common consumer complaints reported to the FTC were those regarding shop-at-home or catalog sales, which accounted for 8% of all complaints. *Id*. Identity theft complaints also accounted for the majority of FTC consumer complaints filed in 2005 and 2006: during both years 37% of complaints regarded identity theft. *Id*.

[21] Martin H. Bosworth, *FTC Findings Undercut Industry Claims that Identity Theft Is Declining*, CONSUMERAFFAIRS.COM, Feb. 9, 2007, http://www.consumeraffairs.com/ news04/2007/02/ ftc_top10_folo.html

In a 2006 survey report, the FTC reported that 8.3 million Americans (3.7%) had been identity theft victims in 2005.[22] The FTC conducted a similar survey in 2003, which found that nearly 10 million Americans (4.6%) had been victims of identity theft in the previous year.[23] Comparing the 2003 and 2006 survey results seems to suggest that identity thefts are decreasing somewhat but the FTC attributes the variance to a change in its survey methodology and asserts that the "apparent decrease" does not indicate a "real decrease" in identity thefts.[24]

On the other hand, Javelin Strategy and Research (Javelin) reported that identity thefts had significantly decreased every year from 2003 to 2007.[25] Javelin's conclusions are based upon a comparison of the data from the 2003 FTC survey report and Javelin's own Identity Fraud Survey Reports for 2004 to 2006.[26] According to Javelin, identity thefts dropped from 10.1

(reporting that the newest data on consumer complaints from the FTC and the a survey from the National Crime Prevention Council refute financial industry claims that identity thefts are declining) (last visited March 10, 2009).

[22] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 24.

[23] FTC, 2003 IDENTITY THEFT SURVEY REPORT 7 (2007), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited March 10, 2009).

[24] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 8. "The difference between the [2003 and 2006 survey] rates is not statistically significant." *Id*. "Given the sample sizes and the variances within the samples, one cannot conclude that the apparent difference between the two figures is the result of a real decrease in ID [sic] theft rather than a result of random variation." *Id*.

[25] JAVELIN STRATEGY AND RESEARCH (JAVELIN), 2008 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2008), *available at* http://www.javelinstrategy.com/research/2 (last visited March 10, 2009); JAVELIN, 2007 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2007), *available at* http://www.javelinstrategy.com/research/2 (last visited March 10, 2009); JAVELIN, 2006 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2006), *available at* http://www.javelinstrategy.com/research/2 (last visited March 10, 2009); JAVELIN, 2005 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2005), *available at* http://www.javelinstrategy.com/research/2 (last visited March 10, 2009). Note, the "Full Version" of these reports may be purchased for $3,000 and downloaded online.

[26] Javelin's 2005, 2006 and 2009 Identity Fraud Survey Reports were co-released with the Council on Better Business Bureaus (BBB Council). *See* Press Release, Better Business Bureau, New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control than They Think (Jan. 31, 2006), *available at* http://www.bbb.org/alerts/ article.asp?ID=651 (last visited March 10, 2009); Press Release, Better Business Bureau, New Research Shows That Identity Theft Is More Prevalent Offline with Paper than Online (Jan. 26, 2005),

million in 2003,[27] to 9.3 million in 2004,[28] 8.9 million in 2005,[29] 8.4 million in 2006,[30] and 8.1 million in 2007.[31] However, Javelin's most recent report found that identity thefts rose in 2008 to nearly 10 million.[32]

The studies conducted by both Javelin and the FTC are the most comprehensive empirical studies available on identity theft in the United States.[33] Unfortunately, the two organizations have seemingly drawn different conclusions on the growth of identity theft in the United States. Further, neither of these surveys tracks synthetic identity theft,[34] which occurs when thieves combine a consumer's personal information with other fabricated information in order to create

---

available at http://www.bbb.org/ALERTS/article.asp?ID=565 (last visited March 10, 2009). However, none of Javelin's other reports appear to have been co-released with the BBB Council.

[27] JAVELIN STRATEGY AND RESEARCH, 2005 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2005), *available at* http://www.javelin strategy.com/research/2 (last visited March 10, 2009). Javelin's 2003 figures were based upon Javelin's own analysis of the raw data from the 2003 FTC survey report. *Id*. Javelin's 2005 survey report disclosed the results of a survey that was administered in 2004. *Id*. Thus, the results and findings presented in Javelin's 2005 Identity Fraud Survey Report relate to identity thefts that occurred in 2003 and 2004. *Id*.

[28] *Id*.

[29] JAVELIN STRATEGY AND RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2006), *available at* http://www.javelinstrategy.com/research/2 (last visited March 10, 2009).

[30] JAVELIN STRATEGY AND RESEARCH, 2007 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2007), *available at* http://www.javelinstrategy.com/research/2.

[31] JAVELIN STRATEGY AND RESEARCH, 2008 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2008), *available at* http://www.javelinstrategy.com/ research/2(last visited March 10, 2009).

[32] JAVELIN STRATEGY AND RESEARCH, 2009 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2009), *available at* http://www.javelinstrategy.com/ research/2 (last visited March 10, 2009).

[33] *See* Beales & Muris, *supra* note 17, at 124-25 (crediting the FTC's 2003 identity theft survey as "the first systematic analysis of the nature and extent of identity theft" and citing Javelin's survey methodology as an attempt to replicate the FTC surveys in order to identify identity theft trends).

[34] *See* FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 4, 11 (explaining that surveys based on consumer reporting likely do not accurately reflect synthetic identity theft since consumers do not always detect this type of fraud); JAVELIN, 2009 IDENTITY FRAUD SURVEY, *supra* note 32, at 15 ("Because this report's underlying survey was based on interviews with individuals who were the victims of fraud . . . it will not include other categories of crime such as synthetic identity fraud, which is based upon a wholly fictitious identity.").

an entirely new identity. This is problematic because synthetic identity theft is widely considered to be a growing form of identity theft.[35]

According to financial industry experts, synthetic identity theft is inherently hard to track,[36] due in large part to the fact that many victims of synthetic identity theft may never discover the misuse of their personal information.[37] Synthetic identity thieves do not take over any one individual's entire identity. Rather, they combine bits of personal information from multiple consumers with phony information to manufacture a new identity. For example, a synthetic identity thief may apply for a credit card using a stolen Social Security number (SSN) and a fictitious name. While there is no existing credit profile for the fictitious identity, this doesn't necessarily stop the thief from obtaining credit, using it and never repaying it, since some creditors routinely give credit to consumers with no history.[38]

Since synthetic identity theft is so difficult to track, many believe that it is significantly underreported.[39] According to multiple sources, synthetic identity thefts are very rarely

---

[35] *See* Hoofnagle, *supra* note 5, at 101-02 ("According to Mike Cook of ID Analytics, a company that specializes in the reduction of fraud risk to businesses, synthetic identity theft 'is a larger problem than [common new account fraud] and is growing at a faster rate." (alteration in original)), quoting Mike Cook, *The Lowdown on Fraud Rings*, 10 COLLECTIONS & CREDIT RISK 20, 24 (2005)). Further, even though "there are no reliable figures documenting losses from synthetic identity theft, some experts estimate that 'synthetic schemes constitute at least 20% of credit charge-offs and 80% of losses from credit-card fraud." Hoofnagel, *supra*, at 102, quoting Christopher Conkey, *The Borrower Who Never Was; Synthetic-Identity Fraud Hits Credit Bureaus, Banks; A Night at the Ritz-Carlton*, WALL ST. JOURN, Oct. 29, 2007, at B1.

[36] *See, e.g.*, Reesa Benkoff, *Developments in Banking and Financial Law: 2005: Combating Identity Theft*, 25 ANN. REV. OF BANKING & FIN. L. 127, 132 (2006) (reporting that, although many synthetic identity thefts are undetected, many financial institutions attempt to track synthetic identity thefts as part of their fraud detection and prevention programs).

[37] *See, e.g.*, FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 4.

[38] *See* Hoofnagle, *supra* note 5, at 101.

[39] *See* JULIA S. CHENEY, PAYMENT CARDS CENTER, IDENTITY THEFT: A PERNICIOUS AND COSTLY FRAUD (2003), *available at* http://www.philadelphiafed.org/payment-cards-center/publications/discussion-

reported.[40] Further, according to experts, financial institutions don't necessarily detect the accounts opened by these synthetic identity thieves as fraudulent, even if balances accumulate that are never paid. Ultimately, financial institutions often write off unpaid balances as losses, without first conducting a fraud investigation.[41] Since synthetic identity thefts are believed to be significantly underreported, it is also argued that the current identity theft data appreciably understates the extent of identity theft as a whole.[42]

In a 2007 article published in the Harvard Journal of Law and Technology, Chris J. Hoofnagle wrote that the "contours of the identity theft problem" are "known unknowns."[43] While acknowledging that the synthetic identity thefts hinders attempts to accurately track identity theft, [44] Hoofnagle went on to attribute this lack of understanding primarily to the data collection methods used in identity theft surveys.[45] As a solution, Hoofnagle suggests that the

---

papers/2003/IdentityTheft_122003.pdf (last visited March 20, 2009) (discussing the underreported nature of synthetic identity fraud).

[40] *See* FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 4; JAVELIN, 2006 IDENTITY FRAUD SURVEY, *supra* note 29, at 15; Hoofnagle, *supra* note 5, at 101; CHENEY, *supra* note 39.

[41] CHENEY, *supra* note 39.

[42] *See* Benkoff, *supra* note 36, at 132 (explaining the synthetic identity theft "often goes undetected" by financial institutions).

[43] *See* Hoofnagle, *supra* note 5, at 98.

[44] As Hoofnagle explains, many victims of synthetic identity theft never discover that their personal information was stolen, which is problematic given that most of the data on identity theft is based on the reports of victims themselves. *Id*. at 104. Additionally, since most victims don't realize their personal information has been hijacked, they never report it to law enforcement or to credit agencies. *Id*. at 105. When credit agencies are unaware of the fraudulence of the account, unpaid accounts are usually charged off as credit losses well before the synthetic fraud is detected. *Id*. However, according to Hoofnagle, initial studies on synthetic identity theft have indicated it is growing problem. *Id*.

[45] *Id*. According to Hoofnagle:

> what we do know [about identity theft] has been learned through telephone and Internet surveys; however, few in-depth studies have been done . . . [the existing] surveys cannot completely document the contours of the crime. More fundamentally, however, we are asking the wrong people about the crime. The surveys seek

federal government impose mandatory reporting requirements on financial institutions, arguing that they are in a much better position than victims to uncover synthetic identity theft and to report accurate identity theft information, especially with regard to costs.[46]

Some industry reports indicate that the overall amount of identity theft fraud may be decreasing slightly.[47] According to reports by Javelin, the overall amount of money fraudulently obtained by identity thieves went from $55.7 billion in 2005, to $49.3 billion in 2006 and $45.3 billion in 2007.[48] The FTC's 2006 study, which compared the 2003 and 2006 survey data, shows an even larger decline, from $47.6 billion in 2003 to $15.6 billion in 2006.[49] Unfortunately, the FTC goes on to state that the results from its two surveys are not comparable because of changes in its survey methodology.[50] Thus, the data on the annual cost of identity theft fraud seems inconclusive. However, consumer groups and government agencies seem to agree that the crime costs financial institutions billions of dollars every year.[51]

> to obtain information about identity theft from its victims—individuals who have the most limited view of the problem and often do not know [how] or by whom their personal data [was] stolen . . . . *Id*.

[46] *Id*. at 100-01.

[47] Beales & Muris , *supra* note 17, at 125 (discussing Javelin's surveys, which attempt to expand on those of the FTC). Beales & Muris explained:

> trends, however, are difficult to discern. Because sample sizes are relatively small (just over four thousand in the original FTC survey, and around five thousand in subsequent surveys), and the incidence of identity theft relatively low (4.6 percent in the past year in the FTC survey), finding statistically significant differences in incidence or cost is difficult. *Id*.

[48] JAVELIN, 2008 IDENTITY FRAUD SURVEY, *supra* note 31, at 15; s*ee also* Jonathon Stempel, *US Identity Fraud $45.3 billion in 2007, but Declining*, REUTERS, Feb. 11, 2008, available at http://www.reuters.com/article/rbssFinancialServicesAndReal EstateNews/idUSN1161861220080211 (last visited March 10, 2009).

[49] *See* FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 9.

[50] *Id*.

[51] *See* FBI, FINANCIAL CRIMES REPORT, *supra* note 3. According to the FBI, the uncertainty is largely because businesses do not report financial losses from identity theft. *Id*.

On the other side of the identity theft financial analysis are consumers. According to Javelin, identity theft victims incurred out-of-pocket expenses averaging $422 in 2005, $675 in 2004 and $555 in 2003.[52] The results of the 2003 and 2006 FTC surveys indicated that the average out-of-pocket expenses to consumers dropped from $500 in 2003 to $371 in 2006. Further, according to the majority of sources, including the FTC, most individual identity theft victims do not pay any out-of-pocket expenses.[53] Although the direct cost to consumers is much lower than that of financial institutions, many victims still face considerable hardships.[54]

Additional hardships may include taking the time and effort spent repairing their credit, reporting the fraud to creditors and law enforcement, dealing with debt collectors, and placing fraud alerts or credit freezes on your credit history. Further, many victims must take time off from work in order to deal with the problem.[55] According to the Javelin reports, in 2006 victims spent on average 25 hours resolving the identity theft.[56] The FTC estimated that during the same

[52] JAVELIN, 2006 IDENTITY FRAUD SURVEY, *supra* note 29, at 15; JAVELIN, 2005 IDENTITY FRAUD SURVEY, *supra* note 27. Only the figures for 2003-2005 are reported because the corresponding figures for 2006-2007 were not reported in the Consumer Versions of Javelin's 2007-2008 Identify Fraud Survey Reports.

[53] *See e.g.*, FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12, at 9 ("The majority of victims (59%) incurred no out-of-pocket expenses."); BBB, Press Release, *New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think* (Jan. 31, 2006), *available at* http://www.bbbonline.org/IDtheft/safetyQuiz.asp (last visited March 10, 2009).

[54] *See, e.g.* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 45-48 (2005) (discussing the negative implications of personal information fraud); Harry Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2 (2004).

[55] *See e.g.*, FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12; JAVELIN, 2007 IDENTITY FRAUD SURVEY, *supra* note 30.

[56] JAVELIN, 2007 IDENTITY FRAUD SURVEY, *supra* note 30.

time period, 60% of victims spent more than 10 hours resolving problems stemming from identity theft, and a full 31% of victims actually spent 40 hours or more resolving the theft.[57]

Root Causes of Identity Theft

Just as the true extent of identity theft in the United States is rather uncertain, so are the root causes of the crime. It is unclear from recent studies how thieves most commonly gain access to stolen personal information:[58] do they use more traditional methods—e.g., dumpster diving, purse snatching and stealing mail—or more sophisticated electronic methods[59]—e.g., hacking,[60] phishing[61] and pharming.[62] Some scholars point to the proliferation of information technologies and the rise of electronic transactions as a contributing factor.[63]

---

[57] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12.

[58] *See, e.g.*, FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 12.

[59] *See, e.g.*, David Koenigsberg, *Developments in Banking and Financial Law: 2005: XII. Security with Online Banking*, 25 ANN. REV. OF BANKING AND FIN. L. 118, 119 (2006) ("Despite [an] alarming rise in online [identity] theft, criminals are still more likely to access account information through non-electronic means, such as stealing mail or wallets."). While identity thieves more often use non-electronic means of stealing personal information, successful online thefts result in more loss. *Id*. The average loss per individual from phishing is $2,320. *Id*.

[60] "Hacking" is to remotely "gain access to a computer illegally." Merriam-Webster Dictionary and Thesaurus (online edition), *hacking*, http://merriam-webster.com/ dictionary/hacking.

[61] "Phishing" is "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly." Merriam-Webster Dictionary and Thesaurus (online edition), *phishing*, http://merriam-webster.com/ dictionary/phishing.

[62] In "pharming" schemes, attackers exploit vulnerabilities in the software of Domain Name Servers, allowing them to "acquire the domain name for a site, and to redirect that web site's [sic] traffic to another web site [sic], typically run by the attacker." PHISHING AND COUNTERMEASURES 123 (Markus Jakobsson & Steven Myers eds., 2006).

[63] *See, e.g.*, Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 VAL. U.L. REV. 1061 (2007); Andrea M. Matwyshyn, Symposium: Toward a General Theory of Law and Technology: Commerce, Development, Identity, 8 MINN. J.L. SCI. & TECH. 515 (2007); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2007); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002); Solove, *Privacy and Power*, *supra* note 16, at 1394; Harry Valetk, Mastering *the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2 (2004).

For example, according to Peter Swire, a law professor at Ohio State University and former Chief Counselor for Privacy to the Clinton administration, the shift from paper to electronic forms of payment has left financial transactions, and likewise personal information, more susceptible to identity theft.[64] A record, Swire points out, is created for virtually every payment made electronically, and those records are then stored, at which point they can be compiled to create detailed consumer purchasing histories for marketing purposes, or perhaps sold to any bidder willing to pay for it.[65]

Similarly, Daniel K. Solove, a well-known privacy expert and author of the textbook *Information Privacy Law*, has written extensively on the negative implications of information technology.[66] Information technology, according to Solove, has made it easy to create and keep detailed records of consumer transactions, and has also made access to and aggregation of public records easier.[67] This relative ease with which public information can be accessed and transactional records can be created and stored has in turn led to the proliferation of database companies, which amass and sell detailed personal profiles of the majority of people in the United States. Solove said the practice of amassing such data appears to have made identity theft easier because all the information one needs to steal the identities of millions of consumers is available from a single source.[68]

---

[64] Peter P. Swire, Financial Privacy and the Theory of High Tech Government Surveillance, 77 WASH. U.L.Q. 461, 464-66 (1999).

[65] *See id*. at 465.

[66] *See, e.g.*, Solove, *Privacy and Power*, *supra* note 16, at 1393.

[67] *Id*. at 1462.

[68] *Id*. at 1407-08.

Solove proposes more regulation on personal information sharing with respect to both government records and private records.[69] Solove is not alone in this. Other authors also have advocated limiting access to public records information, as well as court records, in order to decrease the potential for identity theft.[70]

On the other hand, Lynn LoPucki, a law professor at the University of California, Los Angeles, has argued that the problem of financial identity theft is essentially caused by the failure of public and private entities to properly identify individuals.[71] LoPucki argues that limiting information sharing will do little to curb the threat of identity theft.[72] In fact, LoPucki challenges the assumption that restricting the flow of personal information will effectively prevent identity theft, by cutting off thieves' access to personal information.[73] The better solution, argues LoPucki, is to develop a more secure system for identification, a system that does not rely so heavily on the use of name, address, SSN and date of birth to identify individuals.[74] Public and private record holders frequently use SSNs to authenticate individuals' identity and to link individuals with their particular records, which means SSNs are stored along

---

[69] *Id*. at 1457-63.

[70] *See, e.g.*, Melissa F. Brown, *Family Court Records: A Treasure Trove for Identity Thieves*, 55 S. CAR. L. REV. 777 (2004) (arguing that online access to court records increases the chances for inadvertent disclosure of sensitive personal information). But c.f., some authors have criticized increased regulation of public records disclosure in response to identity theft and information privacy concerns. *See* Brian N. Larson and Genelle I. Belmas, *Second Class for the Second Time: How the Commercial Speech Doctrine Stigmatizes Commercial Use of Aggregated Public Records*, 58 S. CAROLINA L. REV. 935 (2007) (arguing that the First Amendment protects commercial access to aggregated public records).

[71] Lynn M. LoPucki, *Symposium: Enforcing Privacy Rights: Remedying Privacy Wrongs—Did Privacy Cause Identity Theft?* 54 HAST. L.J. 1277 (2003). S*ee also* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 94-95 (2001).

[72] *Id*. at 1278.

[73] *Id*.

[74] *Id*. at 1287-91.

with other personally identifying information in numerous and varied locations.[75] In light of this, LoPucki seems to see restricting the sharing such information as futile.[76]

An entire industry has sprung up around amassing the personal information from multiple sources and organizing it into detailed individual profiles.[77] Often the work of amassing, compiling and selling personal consumer information is completed by database companies such as ChoicePoint.[78] The industry's practice of gathering and selling massive amounts of personal information has been widely criticized. [79] In addition to advocating regulations to limit the way database companies may share information,[80] some scholars advocate breach notification laws.[81]

---

[75] *See, e.g,* Hoofnagle, *supra* note 5, at 101 (discussing credit issuers use of SSNs as personal identifiers and identity authenticators); s*ee also* GOV'T ACCOUNTABILITY OFFICE, GAO-07-752, FEDERAL ACTIONS COULD FURTHER DECREASE AVAILABILITY IN PUBLIC RECORDS, THOUGH OTHER VULNERABILITIES REMAIN (2007) (discussing the vulnerability of SSNs in public records).

[76] LoPucki, *supra* note 71, at 1287-91.

[77] *See, e.g.* ROBERT O'HARROW, JR., NO PLACE TO HIDE 41-50 (2004); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE *20 (2004).*

[78] *See, e.g.* DANIEL J. SOLOVE, MARC ROTENBURG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 696 (2006).

[79] *See, e.g.* O'HARROW, JR., *supra* note 77, at 41-50 (2004); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?,* 44 FED. COMM. L.J. 195 (1992); Daniel J. Solove and Chris J. Hoofnagle, *A Model Regime of Privacy Protection,* 2006 UNIV. ILL. L. REV. 357 (2006); Peter P. Swire, *Financial Privacy, supra* note 64; Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution,* 86 MINN. L. REV. 1137 (2002); Solove, *Privacy and Power, supra* note 16, at 1394.

[80] *See, e.g.,* A. Michael Froomkin, *Creating a Viral Federal Privacy Standard*, 47 B.C.L. REV. 55, 76 (2007) ("Meaningful privacy rules restricting the use of indexing information, and the information indexed with it, will have to be set nationally."); s*ee also* Susan W. Brenner and Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 2006; Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140 (2006); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 563 DUKE L.J. 967, 970-71 (2003).

[81] *See, e.g.,* Michael E. Jones, *Privacy on the Internet and in Organizational Database: Data Breaches: Recent Developments in the Public and Private Sectors*, 3 INFO. SOC'Y J.L. & PUB. POL'Y 555 (2007-2008). Further, since 2005 at least 32 states have passed breach notification statutes. Chris Barnstable-Brown, *Developments in Banking and Financial Law*, 26 ANN. REV. BANKING AND FIN. LAW 38, 41-42 (2007).

According to some privacy advocates, individuals' have the right to know when their personal information has been compromised, putting them at risk for identity theft.[82]

However, the true impact of data breaches on identity theft is largely unknown. While most privacy experts and industry officials agree that data breaches often involve the personal information of millions of people,[83] there is no conclusive evidence that these breaches have significantly contributed to the number of identity thefts.[84] For this reason, several authors caution against imposing strict breach notification requirements on businesses. These arguments often characterize notification requirements as poorly focused or misplaced efforts that do little to mitigate the threat of identity theft and ultimately impede commercial growth.[85]

While data breaches plague both private and public records, much of the debate surrounding the harm caused by such breaches has focused on private entities. However, there have also been numerous data security breaches in multiple agencies throughout the federal

---

[82] *See, e.g.*, James P. Nehf, *Recognizing the Societal Value in Informational Privacy*, 78 WASH. L. REV. 1, 81 (2003) (discussing the benefits of system-wide oversight of information sharing and security breaches); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1653 (1999) (suggesting that unsecure information processing threatens democratic principles); Brendan S. Amant, Note, *The Misplaced Role of Identity Theft in Triggering Public Notice*, 44 HARV. J. ON LEGIS. 505 (2007) (arguing that people have a right to notice arising out of personal autonomy).

[83] *See* PRIVACY RIGHTS CLEARINGHOUSE, CHRONOLOGY OF DATA BREACHES, (2005-2008), http://www.privacyrights.org/ar/ChronDataBreaches.htm (listing more than 250 data breaches that have been made public, resulting in the compromise of more than 245 million records containing sensitive personal information).

[84] *See* FRED H. CATE, THE CENTER FOR INFORMATION POLICY LEADERSHIP 2, *Information Security Breaches and the Threat to Consumers*, at 8 (2005), http://www.hunton.com/ files/tbl_s47Details/FileUpload265 /1280/Information_ Security_Breaches.pdf ("Research indicates that only a small percentage of breaches result in any harmful use of data."); *but cf.* Arshad Mohammed, *Record Fine for Data Breach*, WASH. POST, Jan. 27, 2006, at D1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/ 01/26/AR2006012600917.html (reporting that the FTC blamed a 2005 ChoicePoint data breach for at least 800 identity thefts).

[85] *See, e.g.*, FRED H. CATE, PRIVACY IN PERSPECTIVE (2005); Eric Goldman, *The Privacy Hoax*, FORBES Oct. 14, 2002, available at http://www.ericgoldman.org/Articles/ privacyhoax.htm; Thomas M. Lenard & Paul H. Rubin, *An Economic Analysis of Notification Requirements for Data Security Breaches* 8, PROGRESS ON POINT, July 2005.

government.[86] According to the Government Accountability Office (GAO), in 2006 federal agencies reported 5,146 incidences involving information security breaches.[87] Since 1997, the GAO has categorized information security at federal agencies as a "high-risk" problem.[88] According to the GAO, significant weaknesses persist with respect to the federal government's information security practices.[89] While the literature offers no clear explanation of the effects of information security breaches on the problems of identity theft, it is clear that weaknesses in information security continue plague both public and private record holders.

Legal Framework and Theory

Much of the debate regarding identity theft has focused on criticism of the current, fragmented legal framework of personal privacy protections.[90] As the Government Accountability Office has stated, "no single federal law governs all uses of personally identifiable information."[91] Rather, Congress has passed laws that deal with particular sectors of the economy or particular industries but none that apply universally. In an attempt to strengthen personal privacy protection, Congress has criminalized identity theft. However, addressing identity theft purely in the context of criminal law, by punishing the fraud, seems inadequate. There aren't enough law enforcement resources to investigate the estimated 8-10 million identity

[86] GOV'T ACCOUNTABILITY OFFICE (GAO), PROTECTING PERSONALLY IDENTIFIABLE INFORMATION, GAO-08-343 (2008), *available at* http://www.gao.gov/new.items/d08343.pdf (last visited March 10, 2009).

[87] *Id*.

[88] *Id*.

[89] *Id*.

[90] *See, e.g.*, Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999) (arguing that the current to privacy protection in the United States "has led to incoherence and significant gaps in the protection of citizens' privacy").

[91] GOV'T ACCOUNTABILITY OFFICE, GAO-08-343, *supra* note 86.

thefts each year, let alone prosecute these crimes. In recognition of the current regulatory inadequacies, Congress, professionals and scholars continue to attempt to identify the best framework for regulation.[92]

Authors proposing a framework or legal theory for identity theft regulations often consider the theft as part of the larger issue of personal information privacy.[93] The right to personal information privacy is sometimes considered a component of the right to personal privacy. In the United States, the modern concept of the individual right to personal privacy is largely attributed to Samuel D. Warren and Louis S. Brandeis. In their famous article *The Right to Privacy*, Warren and Brandeis articulated the now widely-accepted notion that every individual

[92] *See e.g.*, Francis J. Facciolo, *Unauthorized Payment Transactions: Who Should Bear the Losses*, 83 CHI.-KENT L. REV. 605 (2008) (discussing how to best allocate the costs of identity theft between financial institution and consumer victims); Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27 (2007) (discussing the different legal theories potentially available for consumer action against private record holders for information security breaches—e.g., tort action, statutory right of action, state common law); Christine Easter, *Auditing for Privacy*, 1 J.L. & POL'Y FOR INFO. SOC. 879 (2006) (recommending federal auditing mandates for all private companies that maintain personal information); Dennis Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1 (2006) (recommending adoption of certain uniform minimum standards for information privacy protection); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140 (2006) (arguing for an enforcement of information security and data protection via tort law); Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345 (2005) (discussing the inadequate remedies consumers have in contract law against distributers of malicious software); Paul M. Schwartz, *Symposium: Enforcing Privacy Rights: Remedying Privacy Wrongs: New Models*, 54 HASTINGS L.J. 1183 (2003) (arguing for the creation of federal privacy agency for centralized regulation over all private businesses); David Lish, Comment, *Would the Real David Lish Please Stand Up: A Proposed Solution to Identity Theft*, 38 Ariz. L.J. 319 (2006) (proposing that consumers should be given both more control to correct erroneous information and more responsibility for securing their own information); Catherine Pastrikos, Comment, *Identity Theft Statutes: Which Will Protect Americans the Most?*, 67 ALB. L. REV. 1137 (2004) (analyzing the different kinds of identity theft statutes at both the state and federal level).

[93] *See, e.g.*, Martin E. Halstuk, *Shielding Private Lives From Prying Eyes: The Escalating Conflict Between Constitutional Privacy and the Accountability Principle of Democracy* 1 COMMLAW CONSPECTUS 71, 73-74 (2003); Stan Karas, *Loving Big Brother*, 15 ALB. L.J. SCI. & TECH. 607, 611-612 (2005); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 563 DUKE L.J. 967, 970-71 (2003); J. Stephen Zielezienski and Catherine I. Paolino, *Insurance Privacy After Gramm-Leach-Bliley-Old Concerns, New Protections, Future Challenges*, 8 CONN. INS. L.J. 315, 316 (2001-2002).

is entitled, as a basic human dignity, to a private life free from public intrusion.[94] In a sense, this notion approaches personal privacy as a property right; an individual, as the owner of his or her private life, has the right to control who is granted access.[95]

Similarly, some scholars articulate the right to personal information privacy as a right to control one's own personal life. For example, Paul M. Schwartz, coauthor of the textbook *Information Privacy Law*, has argued that the mass collection of consumer data threatens individual autonomy.[96] The more information known about a consumer, Schwartz argues, the easier it is to control that consumer's behavior and strip away that consumer's free choice.[97] Implicit in these arguments for control over one's personal information, seems to be the assumption that individuals do in fact "own" their personal information even where that information is held by others.

On the other hand, Stan Karas, a lawyer and privacy scholar, has criticized the theory of personal information as a property interest as misguided and ultimately weak.[98] Karas has proposed that individuals have a privacy right in their personal consumer information, which arises out of their constitutional right to be free from unwarranted intrusions into their personal

---

[94] *See, e.g.* Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*,36 U. BALT. L. REV. 1, 13-18 (2006) (discussing the historical underpinnings of *The Right to Privacy*); *see also* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (defining the right to privacy in the context of four distinct privacy torts).

[95] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) (discussing personal information as a "commodity").

[96] *See id*; *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995)..

[97] Schwartz, *Privacy and Democracy in Cyberspace*, *supra* note 96, at 1676.

[98] Stan Karas, *Privacy, Identity, Database*, 52 AM. U.L. REV. 393, 402-403 (2002).

or private life.[99] However, Karas frames the right, not in terms of control over personal information, but instead as control over self-expression of one's social identity—how we choose to present ourselves to the world.[100] Karas uses the database industry to illustrate his point.[101] The purpose of that industry, according to Karas, is to amass vast amounts of consumer information—e.g., shopping habits, eating habits, finances, music preference—in order to create and sell detailed dossiers on the lives of millions of individual consumers.[102] The accumulation of such consumer information, Karas argues, provides marketers and other third parties with a spy hole into consumers' personal life, through which can they track consumers' daily activities, preventing consumers from personally defining how they present themselves to the world.[103]

Other authors have approached the issue of personal information in the context of fair information practices. In the 1960s, the Department of Health, Education and Welfare issued the now-famous HEW Report, commenting on personal privacy in government records.[104] Amidst the proliferation of computerized record keeping in the 1960s, the Secretary of Health, Education and Welfare commissioned the report to study the resulting threats such record keeping posed to personal privacy. The HEW Report's recommendations and findings proved to be very

[99] *Id*. at 397-98.

[100] *Id*. at 428-429.

[101] *Id*. at 399-412.

[102] *Id*.

[103] *Id*. at 428-29.

[104] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

influential in setting privacy standards for the federal government.[105] In fact, the report was a motivating factor behind passage of the 1974 Privacy Act, which regulates the federal government's information sharing practices.[106]

The HEW Report recommended certain "fair information practices" for the government as a record keeper, including the obligations to: 1) refrain from maintaining secret databases; 2) grant individuals access to their own records; 3) allow individuals to control the different uses of their information; 4) permit individuals to correct mistakes regarding their personal information; and 5) implement information security measures.[107] Some privacy advocates have advocated the adoption of similar fair information practices in the context of private companies.

In 2006 Daniel J. Solove and Chris J. Hoofnagle, proposed a framework for privacy regulation grounded on fair information practices.[108] In order to supplement current privacy regulations,[109] the authors propose adopting a universally applicable regulatory framework based on notions of fairness with respect to information practices.[110] Under the framework, all entities that buy, maintain or sell personal information would be required to: (1) register with the FTC,

---

[105] *See* SOLOVE, ROTENBURG & SCHWARTZ, *supra* note 78, at 696.

[106] *See* GOV'T ACCOUNTABILITY OFFICE, GAO-08-343, *supra* note 86.

[107] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

[108] Daniel J. Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357 (2006).

[109] *See, e.g.*, GOV'T ACCOUNTABILITY OFFICE, GAO-08-343, *supra* note 86. Some federal statutes provide privacy protections for information used for specific purposes or maintained by specific types of entities. *Id*. For example, the Fair Credit Reporting Act applies to companies that prepare or provide information on consumer creditworthiness. *Id*. *See also, e.g.*, Tamela J. White & Charlotte A. Hoffman, *The Privacy Standards under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 W. VA L. REV. 709 (2004) (discussing the HIPAA privacy rules promulgated by the FTC).

[110] Solove & Hoofnagle, *A Model Regime of Privacy Protection*, *supra* note 108, at 368-71.

disclosing their information sharing practices; and (2) seek consent from individuals prior to selling their personal information, absent some statutory exemption. Rather than requiring companies to individually contact consumers for permission, the authors propose that the FTC establish a centralized mechanism, such as the federal Do Not Call Registry, that allows consumers to easily opt out of certain information sharing.[111] According to Solove and Hoofnagle, setting a general threshold for sound information practices, when coupled with creating a centralized federal oversight mechanism, offers a relatively simple and effective way to address identity theft.

Other scholars have criticized the application of the principles of fair information practices in the context of information sharing. In a 2008, J. Howard Beales, former director of the FTC's Consumer Protection Bureau, and Timothy J. Muris, former FTC chairman, argued that fair information practices are a faulty basis for privacy regulation.[112] The authors recognized the appeal of fair information principles such as notice and choice, conceding that it is difficult to convincingly argue against giving consumers rights to be informed of and control how their personal information is collected and used.[113] However, Beales and Muris believe this approach is impractical because it imposes high transaction costs on information sharing, while providing only marginal benefits to consumers.[114] Instead of fair information practices, the authors argue

[111] *Id*.

[112] Beales & Muris, *supra* note 17, at 109.

[113] *Id*. at 114.

[114] *Id*. In other words, the authors believe that this approach is impractical for two main reasons: (1) it ignores the economic aspects of the issue—both the benefits of information sharing and the costs of providing notice; and (2) it assumes that most consumers would actually use the notice to make an informed decision about the sharing of their personal information. *Id*.

that privacy regulations should focus—not on information sharing itself—but on the negative consequences that occur from the misuse of information, e.g., identity theft. According to the authors, actual harm is what consumers most want to avoid.[115]

Judge Richard Posner also has criticized current public policy on information privacy. Posner has asserted that focusing on information sharing as an issue of personal privacy flatly ignores the economic aspects of data collection. In particular, Posner argues that technological advances have made data collection an economically efficient tool for businesses, which is an important benefit that should not be ignored.[116] Further, Posner believes that most of the data collected by companies is "trivial" and poses no threat to individuals' personal privacy.[117] Thus, according to Posner, a cost-benefit analysis favors less regulation of information sharing.[118]

Other scholars have recognized the need to weigh the often competing interests of consumers and businesses. In order to strike the best balance between consumer protection and economic prosperity, David A. Friedman proposes that the federal government move from its current, one-size-fits-all approach, and adopt one that is more targeted.[119] Freidman sees the current regulatory scheme as taking one of two general approaches to identity theft regulation: (1) focusing on criminal enforcement of the actual theft or fraud; or (2) crafting protections from the perspective of all consumers as a whole. These approaches fail, according to Freidman,

---

[115] *Id*.

[116] *See* RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 46 (7th ed. 2007).

[117] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 406-08 (1978).

[118] *See* POSNER, ECONOMIC ANALYSIS OF LAW, *supra* note 116; RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1981); Richard A. Posner, *The Right of Privacy*, *supra* note 117.

[119] David A. Freidman, *Reinventing Consumer Protection*, 57 DEPAUL L. REV. 45, 48 (2007).

because of the high cost of enforcement and oversight, the limited availability of resources, and the government's inability to anticipate and proactively handle the innovations of fraudsters.[120] Friedman posits that lawmakers should adopt more targeted solutions by identifying particular subsets of consumers—i.e., those that are the most vulnerable to identity theft and its consequences—and providing them with "heightened protection."[121]

According to Freidman, this approach combines the important elements of the first two approaches—consumer engagement and government enforcement—in a much more targeted way, enabling lawmakers to design contoured solutions.[122] By focusing more protection on vulnerable consumer groups,[123] Friedman argues that law makers can make better use of limited resources and decrease enforcement costs, as well as reduce the prevalence of identity theft by making it both more difficult and more risky for criminals to prey on the most vulnerable of consumers.[124]

Summary of Identity Theft Issues

As identified in the literature review, various factors contribute to the problem of identity theft. The data available on identity theft are fairly inconclusive, which hinders understanding of even the basic causes of and solutions to identity theft. Additionally, personally identifiable information, and in particular SSNs, are frequently used by both public and private record

[120] *Id*.

[121] *Id*.

[122] *Id*.

[123] Vulnerable groups, according to the author, may include certain ethnic or minority groups, low-income communities, or the elderly population. *See id*. at 56.

[124] *Id*. at 48-56.

holders to identify a person's records and to authenticate a person's identity. Thus, there are myriad sources of an individual's personal information that are almost entirely outside of that individual's control. Further, public and private records holders sometimes fail to adequately protect the personal information in their possession, as evidenced by the numerous reported data breaches. The fragmented federal framework of privacy protections also contributes to the problem of identity theft by providing inconsistent protections and remedies to individuals and making it difficult to address identity theft and its solutions in broad terms.

The issue of identity theft is complex, which has prompted numerous varied proposals for combating the crime. Some authors urge regulations that give individuals more control over their personal information and more control over how others use such information. Others have pushed for stiffer regulation of the information sharing practices of the entities that collect and store individuals' personal information. Sometimes such proposals advocate the adoption of a standard set of information practices broadly applicable to all entities that possess personal information. Further, some authors have argued for penalizing or imposing affirmative duties upon entities when the personal information in their possession is compromised.

On the legislative side of the identity theft debate, Congress has debated or considered numerous bills over the past decade that are aimed at mitigating the threat of identity theft. However, few such bills have passed. Just as there is a lack of agreement amongst scholars and industry experts regarding how to address identity theft, members of Congress seem unable to agree on the appropriate legislative solution. Currently, individuals must make do with the current, piecemeal system of privacy protections in the United States.

Essentially, personal information is protected only to the extent that the entity in possession of that information is regulated by one of the individual privacy laws that make up the

current fragmented system of privacy protection in the United States. Individuals do have some personal remedies at law in the event that they have already been the victim of identity theft. However, individuals have little control over their personal information that is in the possession of numerous public and private entities. This leaves individuals with limited means of preventing the theft of their personal information. This lack of personal control, coupled with the lack of accountability on the part of many record holders, is especially troubling given that the sources of personal information—such as name, SSN and date of birth—are so numerous.

An examination of prior research on identity theft highlighted several problems : (1) an inadequate understanding of the contours of identity theft, (2) the widespread use and availability of SSNs and other personally identifiable information in public and private records, (3) vulnerabilities in information security, (4) a lack of individual control over personal information, and (5) fragmented federal privacy protections that have led to both inconsistent protection for individuals and inconsistent accountability of record holders.

However, just as the system of federal privacy protection is fragmented, to some extent so is the literature on identity theft research. None of the sources located and reviewed during the course of this research provided a comprehensive analysis of identity theft. Most of the literature analyzed in this thesis focused on one particular aspect of identity theft, in order to advocate a particular solution to the problem. No literature was found that attempted to synthesize and comprehensively analyze all of the major issues surrounding identity theft. To fill the gap in the existing identity theft literature, this thesis comprehensively analyzed the federal laws relating to identity theft.

Research Questions

In this thesis, federal privacy laws and regulations that are aimed at protecting against identity are analyzed. All of the materials collected will be analyzed in order to answer the following four questions:

RQ1: What are the federal laws that address identity theft and how are they enforced?

RQ2: To what extent do these laws address the identity theft problems identified in the literature review?[125]

RQ3: What identity theft legislation might Congress adopt in the near future?[126]

RQ4: What kinds of laws may address the problems identified in the literature review?

Methodology

This study used legal research and analysis to examine the system of federal regulations that target identity theft. First, a preliminary analysis of identity theft was conducted, which looked at the available data on identity theft crimes and also identified the primary laws that target identity theft. The results of the preliminary analysis were then used to set the parameters for this thesis and to develop the proposed research questions for this study.

Next, the information garnered from the preliminary analysis was used to design a comprehensive legal search for primary and secondary sources relevant to the research questions of this study. On an on-going basis, the sources located during the search were evaluated and analyzed. This on-going process continued until the search results become merely repetitious of previous searches or the new sources located contribute nothing further to the study.

[125] *See supra* p. 30 last paragraph.

[126] In answering this question, particular attention will be given to any legislation that is currently pending before Congress, as well as any legislation that passed one house of Congress but not the other during the 2007-2008, 110th Congress.

The basic structure and focus of this study of identity theft protections was designed after a review of the laws, rules and regulations identified in the preliminary analysis. Based upon the results of the preliminary analysis, the parameters of the study were limited to the universe of federal regulations, excluding state laws and policies from the analysis. The issue of identity theft is closely intertwined with other federal regulatory issues, especially the regulatory frameworks of the financial industry and the credit system. Since many of these federal regulations preempt state law, federal laws operate as the primary mechanism for such regulation and apply to businesses and industries throughout the United States. Thus, a broad analysis of identity theft issues and policies should begin at the federal level. Future studies, building upon the results of this study, could conduct state-by-state analyses of identity theft regulation.

This study analyzed federal laws that apply to private entities as well as federal laws that apply to the federal government itself. Primarily, this study was concerned with laws that regulate private and government record keepers. Thus, the legal analysis is focused on information privacy laws and industry-specific regulations. However, a brief analysis of federal criminal identity theft laws was also conducted. While there are numerous federal laws that could be categorized as information privacy laws, only those laws which relate to the federal government's efforts to combat identity theft were analyzed.

The information privacy laws examined in this study were those listed by the President's Identity Theft Taskforce and the FTC as protecting against identity theft. All of these laws, which apply to private entities or individuals, were analyzed. This thesis also examined the Privacy Act and the E-Government Act, which have been identified by the Government Accountability Office as the two primary information privacy and security laws that apply to the

federal government's record-keeping practices. Additionally, recent and currently pending federal legislative proposals targeting identity theft were also analyzed.

The enforcement of federal identity theft protections is largely the responsibility of administrative agencies within the federal government. The FTC is essentially the flagship federal agency for consumer protection, including protection from identity theft, and has enforcement authority under several information privacy laws. This study extensively examined the efforts of the FTC efforts to enforce the identity theft laws and regulations under their control. In addition to the FTC, other federal agencies such law enforcement agencies and financial-industry regulatory bodies enforce identity theft protections.[127] The enforcement actions of other federal regulatory and law enforcement agencies were also examined and summarized, though not to the same extent as the FTC enforcement actions.

The legal research and analysis of this study emphasized federal statutory and agency laws and materials. However, secondary sources were also used to provide background on identity theft. Additionally, secondary sources were consulted for the review of the literature regarding the proper regulation of identity theft and protection of information privacy.

The bulk of the secondary source materials came from law reviews, academic journals, survey reports and other data compilations. Survey reports and data published by FTC and other government agencies, as well as reports published by private industry groups, were consulted. Additionally, books, treatises, and articles written by legal scholars, privacy experts and industry analysts provided some background for this study.

[127] The federal financial regulatory agencies include the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, Securities and Exchange Commission

Most of the legal research was conducted using electronic sources and databases, including LexisNexis, Westlaw, THOMAS (the Library of Congress' site for legislative materials), and the University of Florida Library catalog and available databases. Primary and secondary sources were located using keywords and Boolean searches. Searches included the following terms or variations of such terms: "identity theft," "identity fraud," "information privacy," "data privacy," "phishing," "vishing," "pharming," "hacking," "information sharing," "information security," information protection," "information practices," "breach notification," "data broker," "database companies," "data mining," "database marketing," and "cyber crime."

CHAPTER 2
BACKGROUND ON IDENTITY THEFT

Identity Theft: Misuse of Personal Information

"Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information."[1] The Federal Trade Commission (FTC), one of the federal agencies tasked with mitigating identity theft, classifies identity theft as a financial crime where a thief uses another individual's identity to open a new account or credit card or to gain access to an existing credit account.[2] Identity theft is just one type of identity fraud—there are numerous other reasons a criminal may fraudulently assume another's identity, such as immigration fraud or evasion of arrest.[3]

Identity thieves obtain personal information on individuals through various methods, which include going through trash, stealing wallets and purses, taking someone's mail, spying on people who are shopping or talking on the phone, phishing,[4] and obtaining personally identifiable information from private and public record holders.[5] However, which method is

[1] FTC.gov, Identity Theft Site, About Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited March 10, 2009).

[2]FTC, 2006 IDENTITY THEFT SURVEY 24 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinal ReportIDTheft2006.pdf (last visited March 10, 2009).

[3] For example, during a routine traffic stop, an identity thief may another person's identity to avoid being arrested where the thief knows that there is an outstanding arrest warrant in the thief's name. In some instance, an identity thief may have obtained a driver's license or identity card in the victim's name. In others, a thief may claim to have lost his or her license and provide the stopping officer with personal information to show identity. *See id* (discussing the different types of identity theft).

[4] *Id*.

[5] Press Release, Fed. Bureau of Investigation (FBI), Protecting Your Identity (Aug. 21, 2006), *available at* http://www.fbi.gov/page2/dec06/scams 122906.htm (last visited March 10, 2009).

most common is unclear because more than half of identity theft victims report that they do not know how their information was stolen, which is a significant obstacle to effectively preventing identity theft.[6]

In the FTC's 2006 Identity Theft Survey[7] the agency found that only 43% of identity theft victims knew how their information was stolen; 16% personally knew the thief;[8] 7% cited wallet or purse theft; 2% cited mail theft; 5% reported the information was obtained from a private company; 1% cited hacking; and 1% cited phishing.[9] This data seems to suggest that either more technologically advanced means of theft, such as hacking, are not easily detectable by consumers or that these methods are simply used less often. It also appears to indicate that either data breaches are unlikely to result in identity theft or that this cause of identity theft is underreported because consumers are unaware that their information has been compromised by a breach. The problem is that these distinctly different possibilities warrant markedly different legislative solutions.

---

[6] 56 % of identity theft victims reported that they did not know how their information was taken. FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 2.

[7] Another group that has conducted several identity theft studies is Javelin Strategy and Research . Javelin reported that identity thieves increasingly use the telephone to obtain personal information, most often through "vishing," the telecommunications equivalent of "phishing." Press Release, Javelin Strategy and Research , New Research Confirms Identity Fraud Is On Decline (Feb. 11, 2008), *available at* http://www.javelin strategy.com /2008/02/11/new-research-confirms-identity-fraud-is-on-decline/ (last visited March 10, 2009). "Vishing" is a term that describes situations where an identity thief calls a consumer, often using untraceable VoIP technology, and fraudulently solicits information from that consumer. *Id*. The thief may falsely claim to be from a non-profit organization or a customer service representative of a financial institution. *But c.f.* Chris J. Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97, 119-20 (2007) (stating that Javelin's studies and conclusion have been criticized as biased).

[8] This is not surprising. Logically, it seems that where a thief steals the identity of a victim the thief knows, the victim is more likely to discover how their stolen information because of the proximity of thief to the victim. On the other hand, where a victim's personal information is stolen as a result of a data breach and the breach is not reported, the victim is much less likely to discover how their information was stolen by the thief.

[9] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 2.

For example, if data breaches are very unlikely to lead to identity theft, then laws mandating consumer notification of breaches would not be very effective solutions to the problem. On the other hand, if consumers are unaware of how their personal information was stolen because they were never notified that it had been compromised, breach notification statutes may very well mitigate some of the resulting harm from identity theft. This lack of adequate knowledge of the most common methods of identity theft significantly impedes Congress' ability to effectively mitigate the impact of this crime and enact legislation that is specifically targeted towards the real causes of identity theft.

Another problem with the available data on identity theft is that it is based on the self reporting of victims in response to surveys. The FTC conducted its two identity theft surveys using Random-Digit-Dialing methodology to obtain a random sample of adults, ages eighteen and older.[10] The individuals sampled were asked to report whether they had been a victim of identity theft.[11] Individuals who identified themselves as victims were then asked to identify the details of the identity theft, including the amount of the theft, economic loss to the victim, time spent by the victim attempting to rectify the harm, and whether or not the victim reported the theft to the police.[12] It seems that this survey method in itself raises reliability issues because the FTC has no real way of effectively checking the accuracy of the data. Also, the FTC report did

[10] *See, e.g.*, FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 2.

[11] *Id*.

[12] *Id*.

not compare its data to the number of identity thefts reported to either law enforcement or credit companies.[13]

Additionally, uncertainty exists regarding even the actual prevalence of identity theft. In its first identity theft report, the FTC reported that in 2003 more than 10 million identity thefts occurred in the United States.[14] In its most recent report the FTC reported that an estimated 8.3 million Americans were victims of identity theft in 2006.[15] The 2006 report seemingly shows a sharp decline in identity thefts from 2003 to 2006. However, the FTC attributed the decrease to a change in its survey methodology, and stated that "the difference between the rates is not statistically significant."[16]

According to studies conducted by the private industry group Javelin Strategy and Research (Javelin), the incidence and cost of identity theft conclusively decreased every year from 2003-2007.[17] However, in its most recent identity theft report, Javelin reported that actual identity thefts had increased from 8.1 million in 2007 to nearly 10 million in 2008.[18] Javelin's

---

[13] *Id*.

[14] FTC, 2003 IDENTITY THEFT SURVEY 4, *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited March 10, 2009).

[15] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 2, at 4. Also, according to the 2003 FTC identity theft study, an estimated 10 million Americans discovered that they were victims of identity theft in 2003. *Id*.

[16] *Id*. at 8.

[17] JAVELIN STRATEGY AND RESEARCH (JAVELIN), 2009 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2009), *available at* http://www.javelinstrategy.com/ research/2 (last visited March 10, 2009). The "Consumer Version" of this report is available free of charge and the "Full Version" may be purchased online for $3,000. Javelin reported that identity theft incidents dropped from 10.1 million in 2003 to 9.3 million in 2005 and 8.4 million in 2007. Furthermore, the company reported that the dollar amount of this fraud has dropped in recent years as well, going from $55.7 billion in 2005 to $49.3 billion in 2006 and $45 billion in 2007. *Id*. The most recent Javelin Survey Report is a comparison of the data obtained from annual surveys conducted from 2003 to 2008. *Id*.

[18] Javelin, 2009 Identity Fraud Survey Report, *supra* note 17.

surveys, which are sponsored by major financial corporations including Visa Inc. and Wells Fargo and Company, have been criticized as being flawed and biased.[19]

Javelin has conducted annual identity theft survey since 2004. In the company's most recent 2009 Identity Theft Survey Report, Javelin downplays the role of data breaches and other cyber sources and suggests that most identity thieves obtain personal information not from private companies but directly from individual victims:[20]

> Despite the hefty blame—largely perpetuated by the media—placed on the Internet and cyber-crime, online identity theft methods (phishing, hacking and malware) only accounted for 11% of fraud cases in 2008. The truth is, most known cases of fraud occur through traditional methods, when a criminal has direct, physical access to the victim's information. These instances include stolen and lost wallets, checkbooks, or credit cards, or even through the simple act of a criminal surreptitiously eavesdropping into your conversation as you make a purchase [emphasis added].

However, Javelin's claims about the methods of identity thieves are misleading. The numbers presented by Javelin are only representative of the small number of identity thefts where the victim actually knows how the thief accessed their information.[21] Only 35% of the identity theft victims surveyed by Javelin reported knowing how their information was obtained by the identity thief.[22] However, without making that clear, Javelin disingenuously reported that

---

[19] *See* Chris J. Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97, 119-20 (2007) (discussing the misleading and often questionable survey methods employed by industry-sponsored polls, conducted by companies such as Javelin Research). "Javelin Research releases many such surveys, such as industry-sponsored polls, which assert that identity theft is declining. *Id* Yet Javelin's polls do not reflect synthetic identity theft." *Id*. at 119. Synthetic identity theft typically occurs when an identity thief uses someone's social security number with a fake name; thereby, creating a "new" identity. *Id*. at 101.

[20] Javelin, 2009 Identity Fraud Survey Report, *supra* note 17, at 7.

[21] *Id*.

[22] *Id*.

"most cases of fraud occur through traditional methods, when a thief has direct physical access to the victim's information."[23]

The company then goes on to warn consumers to beware of their own friends and family, implying that they are more likely to be victimized by a friend, family member or acquaintance than by a thief who steals personal information from a private company that maintains it:[24]

"Friendly theft," reported by 13% of victims, occurs when friends, family or in-home employees take your private data and use it without your permission for their personal gain. While it is hard to believe that those who are close to us would engage in such an act, it is these individuals that have the closest access to sensitive documents that may contain your financial account numbers, Social Security numbers, and any other valuable personal identifying information needed to commit fraud. They also know your habits so it is easier for them to avoid detection for longer periods of time.[25]

This survey essentially reports that the vast majority of identity thefts occur through no fault of financial institutions. However the survey fails to make clear that its findings are not representative of all identity thefts. The truth is that the circumstances surrounding those identity thefts in which victims knows how their information was stolen are quite possibly very different from those in which victims have no idea how a thief obtained their personal information.

---

[23] *Id*.

[24] The FTC has characterized this conclusion as misleading. *See Hoofnagle*, *supra* note 19, at 121, *citing* email from Claudia Bourne Farrell, Office of Public Affairs, FTC, to Robin Sidel, Correspondent, Wall St. J. (Oct. 20, 2005) (recognizing that Javelin's conclusions cannot be generalized to the entire population of identity theft victims because the results were based on answers from only the small subset of identity theft victims who actually knew how their information was stolen).

[25] Javelin, 2009 Identity Fraud Survey Report, *supra* note 17, at 7.

For instance, identity theft victims who have also recently had their purse stolen have every reason to conclude that the identity thief used the contents of the stolen purse to perpetuate the identity theft. On the other hand, identity theft victims whose information has been compromised in a data breach may not even be aware of such breach and are unlikely to report that they know how their information was obtained by the thief. Javelin's method of presenting generalized conclusions about the most common sources of identity theft based on the answers of only a small subset of victims calls into question the reliability of the survey as a whole.

Additionally, the results of both the Javelin and the FTC surveys regarding the cost, source and prevalence of identity thefts are based on information provided by consumers in response to survey questions. The accuracy of the information provided by consumers has not been independently verified. A further shortcoming of both the FTC surveys and the Javelin surveys is that neither accurately tracks incidences of synthetic identity theft.[26] Due to its nature, synthetic identity theft is not always detectable by victims, so even less is known about its prevalence.[27]

Synthetic identity thieves create fictitious identities by piecing together the personal information of one or more individuals with fabricated information.[28] While the majority of identity thefts have usually involved a thief assuming an existing individual's identity, some evidence suggests that synthetic identity theft is growing, likely because bits and pieces of

[26] *Id*. at 4; FTC, 2006 Identity Theft Survey, *supra* note 2, at 4. *See also Hoofnagle*, *supra* note 19, at 119-20 (2007).

[27] *See Hoofnagle*, *supra* note 19, at 119-20.

[28] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 2, at 4.

different identities are more easily obtained and assembled. [29] Conceivably, this may be attributable in part to data breaches, which often involve a wide array of personal information on multiple individuals. [30] However, without more data on synthetic identity theft it is difficult to draw conclusions regarding its causes.

A little more information on identity theft can be garnered from the federal government's identity theft prosecutions. In the past, identity thefts were most often prosecuted under federal mail and wire fraud statutes.[31] Now, according to the Center for Identity Management and Information Protection (CIMIP),[32] these statutes are the least often used, and identity thieves are more often charged under one of the newer federal identity fraud or computer-related fraud statutes.[33]

---

[29] FRED H. CATE, PRIVACY IN PERSPECTIVE (2005).

[30] *See* S. Rep. 110-70, 110th Congress (2007) (listing 500 security breaches of personally identifiable information reported by public and private entities from 2005 through 2007); *see also* Privacy Right Clearinghouse Web site, *Chronology of Data Breaches—2005-2008*, http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008 (last visited March 10, 2009) (reporting more that 1,000 data breaches between 2005-2008).

[31] CENTER FOR IDENTITY MANAGEMENT AND INFORMATION PROTECTION (CIMIP), IDENTITY FRAUD TRENDS AND PATTERNS: BUILDING A DATA-BASED FOUNDATION FOR PROACTIVE ENFORCEMENT 21 (Oct. 2007), *available at* http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf (last visited March 10, 2009).

[32] The Center for Identity Theft Management and Protection, a research collaborative housed at Utica College, was founded by a federal grant in June 2006. CIMIP Web site, About CIMIP, http://www.utica.edu/academic/institutes/cimip/about/index.cfm (last visited March 10, 2009). CIMIP's mission is to mitigate the impact of identity theft on national security through its collaborative research on identity management, information sharing and data protection. *Id*. The organization is essentially a cooperative of academic institutions, federal agencies—including the FBI, Secret Service, Department of Homeland Security, United States Postal Service and United States Marshal Service—and some private organizations, including LexisNexis, IBM and TransUnion. *Id*.

[33] CIMIP, *supra* note 31, at 20-22. Of the identity theft cases studies, approximately 25.5 % of federal identity theft charges levied against the accused thieve were brought pursuant to Section 1028 of Title 18, which was amended by the Identity Theft Assumption and Deterrence Act to specifically prohibit identity theft. *Id*. 30.9 % of these cases were brought under Section 1029 of Title 18, which criminalizes fraud in connection with the unauthorized access to computers and other electronic sources. *Id*. In contrast only, 10.7% were brought under federal mail and wire fraud statutes. *Id*.

In its 2007 study, the CIMIP reported that identity thieves convicted under federal law are predominantly male: 67.4%.[34] The CIMIP also concluded that most convicted identity thieves used the stolen identity to obtain and use credit,[35] which is a finding echoed by the FTC Identity Theft Surveys.[36] In 34.1% of federal identity theft cases examined by the CIMIP, thieves obtained the stolen information through their place of employment;[37] in 43.8% of these cases, the place of employment was a retail store.[38] In addition, CIMIP also reported that "in approximately half of the cases, the Internet and/or other technological devices were used in the commission of the crime."[39] This data seems to undermine Javelin's conclusions that technological means, such as hacking, play only a small roll in identity theft. However, while the CIMIP results are useful, they can't be generalized to all identity thefts because the only of identity theft crimes studied were those that were ultimately prosecuted by the federal government.

Identity theft, generally speaking, results from inadequate control over personal information, whether the breakdown occurs on the part of private companies, government entities, or individuals. This lack of control is in many ways a byproduct of the changing nature of information in today's society. The importance of information, as well as the way it is stored,

---

[34] *Id*. at 32.

[35] *Id*. at 38. Other forms of identity theft include medical fraud, immigration fraud, document fraud or phone and utilities fraud. FTC.gov, About Identity Theft, *supra* note 1.

[36] FTC, 2006 IDENTITY THEFT SURVEY, *supra* note 2, at 30.

[37] CIMIP, *supra* note 31, at 42.

[38] *Id*.

[39] *Id*. "Technological devices" include computers used to scan or produce documents, computer printers, copiers, typewriters, digital cameras, cell phones, telephone, access device reader, credit card encoder, fax machine, and laminating machines. *Id*. at 48.

created, sold, lost and used as a commodity has changed significantly since the advent of the Internet and the proliferation of personal computers.

Changing Character of Information in the Information Age

Currently, in what is often termed the "Information Age," society revolves around the creation, distribution, processing, storing, and accessing of information. Generally, the term "Information Age" describes "both the notion of industries primarily producing, processing, and distributing information, as well as the idea that every industry is using available information and information technology to reorganize and make themselves more productive."[40] The Information Age has revolutionized the way most companies conduct their affairs. Even companies that are not specifically engaged in "producing, processing, and distributing information" rely on information technology and services in order to operate more efficiently and effectively.[41] For example, most new business records are created and stored electronically, enabling easy retrieval and accumulation of information.[42]

Furthermore, with the advent of online financial tools such as e-trading, electronic banking and online shopping,[43] a growing percentage of economic transactions in the United States are

[40] U.S. Census Bureau Web site, Service Annual Survey Industry 51 Summary, http://www.census.gov/svsd/www/services/sas/sas_summary/51summary.htm#sectordescription (last visited March 10, 2009).

[41] *Id*.

[42] Peter P. Swire, Financial Privacy and the Theory of High Tech Government Surveillance, 77 WASH. U.L.Q. 461, 464-66 (1999).

[43] E-commerce transactions are transactions for the purchase of goods and services conducted online. U.S. Census Bureau Web site, Service Sector Statistics Definitions, http://www.census.gov/mrts/www/summary.html#defin (last visited March 10, 2009).

conducted electronically, increasing demand for technological means of conducting business.[44] The rising demand for information technologies is illustrated by recent economic reports from the U.S. Census Bureau.

According to the Census Bureau, U.S. businesses have increased spending on "e-business infrastructure"—information and communication technology equipment and computer software—since 2003 when the Census Bureau began tracking this information.[45] In its most recent 2009 report, the Census Bureau reported that U.S. businesses spent a total of $264.2 billion on e-business infrastructure in 2007, a 4.4% increase over 2006.[46] E-business infrastructure spending also increased annually from 2005, 2006 and 2007 by 2%, 3.3% and 6.8%, respectively.[47] Collectively, the companies that supply this e-business infrastructure, referred to as information-and-communications-technology-producing industries (ICT industries), consist of a cross-section of different service and goods-producing industries.[48]

---

[44] *See* U.S. CENSUS BUREAU (CENSUS BUREAU), 2007 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY app. A (Feb. 2009), *available* at http://www.census.gov/csd/ict/ (last visited March 10, 2009).

[45] *See* CENSUS BUREAU, 2007 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY, *supra* note 44 ; CENSUS BUREAU, 2006 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY (March 2008); CENSUS BUREAU, 2005 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY (April 2007); CENSUS BUREAU, 2004 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY (March 2006); CENSUS BUREAU, 2003 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY (June 2005).

[46] CENSUS BUREAU, 2007 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY, *supra* note 44.

[47] *See* sources cited *supra* note 45.

[48] This consists of industries from cross-sectors of the economy: 1) those that produce computer and electronic products (part of durable-goods manufacturing sector of the economy); 2) publishing industries, including traditional and software publishers (part of the information services sector); 3) information and data processing services (part of the information services sector); and 4) businesses that perform computer systems designs and related services (part of the professional, scientific, and technical services). CENSUS BUREAU, 2007 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY, *supra* note 44.

Additionally, in its most recent economic report the Bureau of Economic Analysis reported ICT industries experienced double-digit growth in 2007, the fourth consecutive year the industry has seen such growth.[49] The BEA's December 2008 report found that in 2007 ICT industries overall grew by 13%.[50] Businesses in the information services sector[51] derive profits by from transforming information into a product or commodity,[52] accomplishing this by producing or distributing information, providing the means to distribute or transmit information, or processing information or data.[53]

[49] *See* Press Release, Bureau of Economic Analysis (BEA), Financial and Insurance Industries Led Slowdown in 2007 (Dec. 15, 2008), *available at* http://www.bea.gov/newsreleases/industry/gdpindustry/2008/pdf/gdpind07_rev.pdf (last visited March 10, 2009) ("Information-communication-technology-producing (ICT) industries' value added remained strong in 2007, increasing 13.0 percent."); *see also* Press Release, BEA, Private Services-Producing Sector Continued to Lead Growth in 2006 (Jan. 29, 2009), *available at* http://www.bea.gov/newsreleases/industry/gdpindustry/2008/gdpind06_rev.htm (last visited March 10, 2009) ("[ICT] growth continued to exceed 11.0 percent for the third consecutive year in 2006.").

[50] Press Release, BEA, Financial and Insurance Industries Led Slowdown in 2007, *supra* note 49.

[51] "The main components of this sector are the publishing industries, including software publishing, and both traditional publishing and publishing exclusively on the Internet; the motion picture and sound recording industries; the broadcasting industries, including traditional broadcasting and those broadcasting exclusively over the Internet; the telecommunications industries; Web search portals, data processing industries, and the information services industries." U.S. Census Bureau Web site, 2007 NAICS Definitions: Sector 51 Information, *at* http://www.census.gov/naics/2007/def/NDEF51.HTM#N51 (last visited March 10, 2009).

[52] Information products include, among other things, movies, blogs, newspapers, computer software, email accounts, phonebooks and databases. These products may have any of a number of expressive purposes – e.g., educational, literary, marketing, entertainment, efficiency, analytical, or creative – and may be intended, by information service companies, for distribution on a mass scale or to a more limited or particular audience. *Id*.

[53] *Id*. According to the Census Bureau:

> the Information sector groups three types of establishments: (1) those engaged in producing and distributing information and cultural products; (2) those that provide the means to transmit or distribute these products as well as data or communications; and (3) those that process data. Cultural products are those that directly express attitudes, opinions, ideas, values, and artistic creativity; provide entertainment; or offer information and analysis concerning the past and present. Included in this definition are popular, mass-produced products as well as cultural products that normally have a more limited audience, such as poetry books, literary magazines, or classical records. *Id*.

The primary information service industries include publishing companies, software companies, broadcasters, telecommunications companies, internet service providers, data processing companies and internet search engines.[54] While many of these information services industries have existed since long before the Information Age, some are newly emerging as growing industries, and none have remained unaffected by the shifting nature of information and the growing importance of information technology and the Internet.

One of the growing industries of the information sector is the database industry, which collectively amasses, sorts, and sells databases that contain vast amounts of personal information on the majority of adults in the United States. [55] According the BEA's most recent economic report, the data processing services industry grew by 26% in 2007.[56] This industry includes direct marketing companies, data brokers and data mining companies. Recent technological advances have greatly enabled the growth of the database industry by simplifying the collection, analysis and distribution methods of massive amounts of information. Information held by these

[54] *Id*.

[55] *See, e.g.*,DANIEL J. SOLOVE, MARC ROTENBURG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 629 (2006). Equifax spin-off ChoicePoint has bought more than fifty other database companies since its inception. *Id*. In 2006, the company now had more than 17 billion online records on about 220 million adults. *Id*. at 149. Additionally, database company Axciom amasses information on nearly ever adult in the country, including name, age, address, phone number, marital status and family status, income, home value, car value, occupation, unlisted phone numbers, religions, ethnicities, Web orders, and vacations ROBERT O'HARROW, JR., NO PLACE TO HIDE 41-50 (2004). The company sells marketing profiles, credit records, data for background checks, and information to government agencies. *Id*. Other large database companies include LexisNexis, Catalina Marketing Company, Aristotle, Inc. and Donnelly Marketing Information Services. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 20 (2004).

[56] Press Release, Bureau of Economic Analysis, U.S. Dep't of Commerce, 2005 Growth Led by Services Producing Industries (Dec. 11, 2006).

companies is compiled and sold to, among others, marketers, employers and law enforcement organizations.[57]

Public agencies increasingly rely on the database industry to investigate crimes.[58] Reciprocally, database companies rely on the information released by public agencies to complete their files.[59] Thus, the personal information on individuals that was previously housed by public agencies in multiple separate physical locations is now being housed electronically on information systems that are often remotely accessible.

Information is both easily accessible and more mobile than ever before.[60] Wireless internet and laptop computers give people access to the Internet from virtually anywhere. Furthermore, mobile phones are no longer simply what the name implies. These "phones" do much more than enable mobile calling. Rather, cell phones are now mobile "all-in-one" devices with Internet browsers and the capability to store, create, manipulate and give access to information, which can then be electronically transmitted from one phone to a phone, computer or email address.[61] Information technology—such as "mobile phones" and the Internet—have enabled individuals to conduct much of their business via telecommunications, reducing the need

[57] SOLOVE, ROTENBURG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 55.

[58] GOV'T ACCOUNTABILITY OFFICE, DESPITE REPORTED PROGRESS, FEDERAL AGENCIES NEED TO ADDRESS PERSISTENT WEAKNESSES, GAO-07-837 (2007), *available at* http://www.gao.gov/new.items/d07837.pdf (last visited March 10, 2009).

[59] *Id*.

[60] 62% of all Americans are part of a wireless, mobile population that participates in digital activities away from home or work. Pew Internet & American Life Project, Mobile Access to Data and Information (2008), http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Mobile.Data.Access.pdf.pdf (last visited March 10, 2009).

[61] These "phones" store information (calendars, documents, address and phone book, photos, music, etc.), receive and send email and instant messages, and access the Internet. Mobile phones are personal computers, video players, wireless Web browsers, GPS navigators, cameras and music players.

for in-person business transactions. The ability to remotely conduct business makes identity theft easier and likely more attractive since it is more difficult (and more risky) to impersonate someone in person than over the phone or Internet.[62] Overall, the relative ease with which personal information is amassed, distributed, stored and accessed has had some impact on the potential for the misuse of personal information. New information protection laws should be able to adapt to ongoing technological changes in order to be truly effective.

Some federal information privacy laws give consumers certain rights, which are often remedial in nature and intended to help mitigate the harmful effects of identity theft.

Additionally, the federal government attempts to protect consumers from identity theft through a combination of criminal laws and information privacy regulations. Some federal laws seek to punish and deter identity theft by criminalizing the actual theft of another's identity. Other federal regulations attempt to prevent criminals from obtaining the personal information necessary to perpetrate the crime by imposing information security regulations on record keepers.

[62] *See* Lynn M. LoPucki, Symposium: Enforcing Privacy Rights: Remedying Privacy Wrongs—Did Privacy Cause Identity Theft?. 54 HAST. L.J. 1277, 1278 (2003).

CHAPTER 3
CURRENT FEDERAL FRAMEWORK FOR IDENTITY THEFT PROTECTION

In the United States, there are essentially two kinds of federal identity theft protections: criminal laws and information privacy laws. Information privacy laws target various entities across numerous industries, including financial institutions, health care providers and credit reporting agencies. These laws are generally directed towards the entities that maintain personal consumer information. The federal government's criminal identity theft laws attempt to deter the actual crime of identity theft by imposing stiff criminal penalties on identity thieves.

Criminal Identity Theft Laws

In 1998, Congress passed the Identity Theft Assumption and Deterrence Act—the first federal law that specifically criminalized identity theft—making it a crime to unlawfully use another individual's identity in furtherance of a crime.[1] Pursuant to the 1998 law, it is a felony under federal law to "knowingly transfer[], posses[], or use[], without lawful authority, a means of identification of another person . . . in connection with any unlawful activity that constitutes a violation of Federal law or a felony under any applicable State or local law."[2] Since passing the 1998 identity theft law, Congress has passed two new identity theft laws that strengthen the penalties for identity theft and increase the scope of identity theft prosecutions.

The Identity Theft Penalty Enhancement Act, which was passed in 2004, increased penalties for identity theft crimes in certain circumstances by creating a class of identity theft crimes labeled "aggravated identity theft."[3] The bill was passed soon after the Federal Trade

[1] Pub. Law No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028 (2006)).

[2] 18 U.S.C. § 1028(a)(7).

[3] Pub. Law No. 108-275, 118 Stat. 831 (2004) (codified as amended at 18 U.S.C. § 1028A (2006)).

Commission (FTC) released it first identity theft survey in 2003. According to legislative history of the act, Congress was alarmed by the increasing prevalence of identity thefts, troubled by the convicted thieves' relatively brief prison sentences, and concerned that identity fraud may facilitate terrorism:

> Despite all the attention [given] to this type of crime since September 11, 2001 the incidence of this crime is increasing. . . Identity theft and identity fraud is a threat to personal security as well as national security. Under current law, many perpetrators of identity theft receive little or no prison time. That has become a tacit encouragement to those arrested to continue to pursue such crimes.[4]

The Identity Theft Penalty Enhancement Act was Congress' attempt "to reduce the incidence of identity theft and fraud and . . . [provide] stronger penalties for those who [commit identity theft] in furtherance of other more serious crimes."[5] In addition to the base sentence imposed under federal sentencing guidelines, a mandatory two year prison term is added for identity theft convictions committed in connection with more egregious felonies such as those involving public money, bank fraud or immigration fraud.[6] A mandatory five-year additional prison sentence is added to identity theft crimes committed in connection with federal crimes classified as terrorism offenses.[7] The increased sentences for aggravated identity theft are not only mandatory but they may not to be served concurrently with another sentence.[8] Further,

[4] H. Rep. 108-528, 108th Cong. (2004).

[5] *Id*.

[6] 18 U.S.C. § 1028A.

[7] *Id*.

[8] *Id*.

courts are prohibited from imposing probation in lieu of prison time for people convicted of aggravated identity theft.[9]

Most recently, Congress enacted the Identity Theft Enforcement and Restitution Act of 2008.[10] The Act was signed into law by President George W. Bush on September 26, 2008.[11] With respect to identity theft convictions, the law provides for criminal restitution orders to compensate the victims for the time lost and money spent remedying the effects of the identity theft.[12] The law also amends federal law to allow for the federal prosecution of criminals for stealing personal information from a computer, even where the victim's computer and the thief are located in the same state. Previously, the law only allowed prosecution of such crimes involving "interstate or foreign communication," and excluded instances where the thief was located in the same state as the victim whose computer the thief accessed.[13]

Congress has certainly taken steps to strengthen criminal laws against identity theft. However, criminal laws only go so far in combating identity theft. Aside from the potential deterrent effects of these criminal laws, they do little to actually prevent identity theft from occurring or to curb the ultimate harm caused by the crime.

---

[9] *Id*.

[10] Pub. L. No. 110-326, 122 Stat. 3560, tit. II, §§ 201-09 (2008) (codified in scattered sections of 18 U.S.C. (2006)).

[11] *Id*.

[12] *Id*. § 202.

[13] *Id*. § 203.

Information Privacy Laws

Private Sector Regulations

In the United States, there is no single comprehensive information privacy law. Rather, there are "a number of federal laws, regulations, and guidelines [that] protect consumer information," according the President's Identity Theft Taskforce (ID Theft Taskforce or Taskforce).[14] The ID Theft Taskforce was established in May 2006 by George W. Bush[15] and directed "to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution."[16] In a 2008 report, the Taskforce listed seven federal laws and regulations that make up the primary federal framework of information privacy protection, with respect to the private sector.[17] These laws apply to various entities, including consumer credit reporting agencies, financial institutions, health care providers, educational institutions and state departments of motor vehicles, as well as individuals.

Fair Credit Reporting Act: Privacy of credit information

Since identity theft almost always affects the credit history of victims, credit industry regulations are particularly pertinent to the examination of federal identity theft regulations. The Fair Credit Reporting Act (FCRA) is the primary federal law regulating the system of credit

[14] PRESIDENT'S IDENTITY THEFT TASKFORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, vol. II, pt. A, at 1 (April 2007).

[15] Exec. Order No. 13402, 71 Fed. Reg. 27945 (May 10, 2006).

[16] IDTheft.gov, President's Identity Theft Taskforce, *About the Taskforce*, http://www.idtheft.gov/about.html (last visited March 10, 2009).

[17] PRESIDENT'S IDENTITY THEFT TASKFORCE, COMBATING IDENTITY THEFT, *supra* note 14, at 1-11.

reporting in the United States,[18] and it applies to "consumer reporting agencies"[19] that provide consumer credit reports.[20] The FCRA was enacted in 1970 "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[21] The Act is intended mainly to control the reporting, not the collection, of consumer information.[22]

In 2003, Congress amended the FCRA to increase consumer privacy protections for credit report information. The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) was Congress' attempt to address the growing threat of identity theft and its impact on consumer credit.[23] This Act strengthened identity theft laws by imposing additional duties and restrictions

[18] Pub. L. No. 91-508, tit. VI (1970), 82 Stat. 146 (1970) (codified as amended at 15 U.S.C. § 1681-1681x (2006)). In addition to the FCRA, the FTC lists three other federal laws that implicate information privacy and the credit industry. FTC Identity Theft Site, Federal Laws: Privacy & Information Security, http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/federal-privacy.html (last visited March 20, 2009).

[19] 15 U.S.C. § 1681a. Consumer reporting agency "means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." *Id*. § 1681a(f). The three main consumer reporting agencies in the United States are Equifax, Experian and TransUnion. *See* Press Release, FTC, Nation's Big Three Consumer Reporting Agencies Agree To Pay $2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act (Jan. 13, 2000), *available at* http://www.ftc.gov/opa/2000/01/busysignal.shtm (last visited March 10, 2009). In 2000, all three agencies were charged with violating the Fair Credit Reporting Act. *Id*.

[20] Consumer report "means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness [*sic*], credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for" an authorized purpose. *Id*. § 1681a(d).

[21] In 1970, Congress passed the FCRA, which was one among many consumer protection laws passed in response to the consumer movement. Barbara Crutchfield George, Patricia Lynch & Susan F. Marsnik, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735 (2001).

[22] DANIEL J. SOLOVE, MARC ROTENBURG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 696, 708 (2006).

[23] The FACT Act is "[an act to] amend the Fair Credit Reporting Act, to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer

on private businesses, giving federal agencies increased authority to promulgate new information privacy rules applicable to the credit-industry and its patrons.[24] The FACT Act also gave consumers increased rights and remedies—such as the right to receive free annual credit reports—to enable consumers to better protect their credit histories and information.[25]

Consumer rights. The FACT Act gives consumers certain rights intended to help them prevent and detect credit fraud and identity theft. In order to prevent identity theft, consumers may request that consumer reporting agencies only reveal the last four digits of the consumer's Social Security number (SSN) in any disclosure of the consumer's credit report.[26] Also, consumers are entitled to one free credit report annually from each of the three major reporting agencies.[27]

Additionally, the FACT Act gives consumers certain rights intended to mitigate any harm resulting from identity theft. First, consumers may place fraud alerts on their credit reports by notifying one credit reporting agency; that agency must then notify the other agencies.[28] Second, if a consumer requests a fraud alert, consumer reporting agencies must also notify everyone that

---

access to, credit information, and for other purposes." Fair Credit Reporting Act (FACT Act) Pub. Law. 108-159, 117 Stat. 1952 (2003) (codified as amended at 15 U.S.C. §§ 1681-1681x (2006)).

[24] § 115.

[25] *Id*.

[26] *Id*.

[27] *Id*. § 211. The FACT Act also mandated the creation of a central source where consumers may request their credit reports from each credit reporting agency, and these agencies must also provide consumers with one free credit report per year, upon request. *Id*; *see also* Press Release, FTC, FTC Issues Final Rule on Free Annual Credit Reports (June 4, 2004), *available at* http://www.ftc.gov/opa/2004/06/freeannual.shtm (last visited March 10, 2009).

[28] FACT Act § 111.

requests that consumer's credit report that the consumer may be the victim of fraud.[29] Third, consumers may require that creditors disclose to them or to law enforcement officials the transactions and fraudulent credit applications of the identity thief.[30] Fourth, consumer reporting agencies must block any information in a consumer's file that is the result of a properly reported identity theft and notify the creditor that reported the disputed information to the agency.[31] Fifth, if a consumer properly notifies a creditor that specific debts are the fraudulent, that creditor may not report any of the disputed information to consumer reporting agencies unless it is subsequently determined that the disputed transactions are not fraudulent.[32]

Duties and restrictions on businesses. The FACT Act also imposes additional restrictions and duties on credit reporting agencies and other private entities. Each time a credit reporting agency discloses a consumer's credit report, that agency must also provide the consumer with a summary of rights under the FCRA.[33] Consumer reporting agencies are also required to promptly and fully investigate any disputed credit report information and notify the consumer of the investigation results within thirty days.[34] Creditors are also prohibited from selling, transferring or placing in collections any debts that have been properly reported as

[29] *Id*. The same right applies to members of the military who are going on active duty. *Id*.

[30] *Id*. § 103 (2003). In order to obtain this information from creditors, consumers must make a written request, prove their identity to the creditor, and provide a copy of the identity theft police report. *Id*.

[31] *Id*. § 152.

[32] *Id*. § 154.

[33] *Id*. § 629.

[34] *Id*. § 313.

fraudulent.[35] Further, all creditors are required to notify a consumer after reporting negative information on that consumer's account to a credit reporting agency.[36] Additionally, in order to safeguard consumers' credit and debit cards, all businesses are prohibited from printing more than the last five digits of a credit or debit card number and its expiration date on receipts.[37]

In addition to the regulations directly imposed by the FACT Act, Congress also gave the FTC and other federal agencies the power to promulgate additional rules to prevent identity theft.[38] These new regulations require financial institutions and creditors to establish "reasonable policies and procedures" in order to identify potential risks to customers or to the "safety and soundness of the institution or customers."[39]

Red Flags Rule. Pursuant to the FACT Act, the FTC, in conjunction with the federal financial regulatory agencies, promulgated the Identity Theft Red Flags and Address Discrepancies Rule (Red Flags Rule).[40] The rule requires that all financial institutions and creditors develop specific plans for mitigating identity and implement "a written program that

[35] *Id*. § 154.

[36] *Id*. § 217. After the initial notification, creditors are not required to notify the customer before reporting additional negative information regarding the same transaction or account. *Id*.

[37] *Id*. § 113.

[38] *Id*. § 114.

[39] *Id*. *See also* Press Release, FTC, Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy (July 18, 2006), *available at* http://www.ftc.gov/opa/2006/07/idtheftredflagjoint.shtm (last visited March 10, 2009).

[40] Red Flags Rule, 12 C.F.R. § 681 (FTC) (2009); 12 C.F.R. § 41 (Office of the Comptroller of Currency) (2009); 12 C.F.R. § 222 (Fed. Reserve System) (2009); 12 C.F.R. §§ 334, 364 (Fed. Deposit Insurance Corp.) (2009); 12 C.F.R. § 571 (Dep't of the Treasury) (2009); 12 C.F.R. § 717 (Nat. Credit Union Admin.) (2009).

identifies and detects the relevant warning signs—or red flags—of identity theft."[41] According to the FTC, such red flags may include "unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents."[42] In addition, the rule requires credit card issuers to take certain steps to fully verify a customer's information after receiving a request for a change of address or replacement credit card.[43]

Disposal Rule. In addition to implementing new rules that apply to financial institutions and creditors, the FACT Act required the FTC and the federal financial regulatory agencies[44] "in coordination with one another, to adopt consistent and comparable rules regarding the proper disposal of consumer report information and records." The resulting joint rule, known as the Disposal Rule, applies to all entities[45] and individuals[46] that use consumer credit reports for any

[41] FTC, Business Alert, New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft (June 2008), *available at* http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm (last visited March 10, 2009). Further, these identity theft plans must be managed and overseen by a high-level official or employee. *Id*.

[42] *Id*.

[43] *See* 12 C.F.R. § 681; FACT Act § 114. *See also* Press Release, FTC, Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy (July 18, 2006), *available at* http://www.ftc.gov/opa/2006/07/idtheftredflagjoint. Shtm (last visited March 10, 2009).

[44] The FACT Act applies to the federal financial regulatory agencies, including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, Securities and Exchange Commission. 117 Stat. 1952, § 114.

[45] Essentially, all entities are subject to this rule if they use consumer reports for any business purpose. *See* FTC, Business Alert, Disposing of Consumer Report Information? New Rule Tells How, *available at* http://www.ftc. gov/bcp/edu/pubs/business/alerts/alt152.shtm (last visited March 10, 2009). For example, consumer reporting agencies, financial institutions, lenders, government agencies, auto dealers, debt collectors and businesses that use credit reports to make employment decisions are subject to this rule. *Id*.

[46] Landlords, employers, attorneys, private investigators and individuals that obtain credit reports on prospective nannies, contractors, or other in-home employees. *See* FTC, FTC Business Alert, Disposing of Consumer Report Information, *supra* note 46.

business purpose.[47] The purpose of the new rule is "to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information."[48]

The rule does not mandate any specific form of disposal. Rather, it requires that individuals or entities that use consumer credit reports take "reasonable measures" to safely dispose of both the reports and any personally identifiable information obtained from the reports.[49] The FTC offers examples of "reasonable measures" for disposal, which include shredding and burning paper records and erasing or destroying electronic media.[50]

The FCRA is the only comprehensive system of credit industry regulations in the United States, intended to prevent, detect and mitigate identity theft. In fact, the FCRA actually preempts most state laws that regulate those business transactions covered by the act.[51] While the Act specifically states that it does not preempt state laws that attempt to prevent or mitigate identity theft, it then goes on to list numerous exceptions to this rule.[52]

---

[47] FTC Disposal Rule, 16 C.F.R. § 682 (2009). "Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." *Id*. § 682.3(a).

[48] *Id*. § 682.

[49] *Id*. The FTC lists as SSN, driver's license number, phone number and physical address as examples of personally identifiable information. *Id*. However, the Disposal Rule does not contain a specific definition or exhaustive list of personally identifiable information because, as the FTC put it, "depending upon the circumstances, data elements that are not inherently identifying can, in combination, identify particular individuals." *Id*.

[50] *Id*. § 682.3(b).

[51] 15 U.S.C. § 1681t (2006).

[52] *Id*. § 1681t(a).

Under the FCRA, states may not enact more stringent laws regulating the practice of prescreening consumers in order to make (unsolicited) "firm offers of credit or insurance."[53] States are also prevented from imposing any additional requirements on credit reporting agencies in connection with dispute investigations,[54] or on other businesses regarding the reporting of information to credit reporting agencies.[55] Further, states may not give identity theft victims a right of access to additional information regarding fraudulent transactions,[56] or regulate the sharing of consumer reports among affiliated businesses.[57] States are also barred from imposing additional requirements on creditors who intend to report negative consumer credit information on a consumer,[58] or further limit the information disclosed in consumer credit report.[59] Essentially, the FCRA significantly limits states' ability to enact more stringent requirements on credit reporting agencies and creditors in order to mitigate the threat of identity theft.

While the FCRA is not the only law that regulates the consumer credit system in the United States, it is the primary law that regulates this industry. Other consumer protection laws that apply to the credit industry include the Fair Debt Collection Practices Act of 1966,[60] the Fair

[53] *Id*. §1681t(b)(1)(A). Credit reporting agencies may provide reports to requestors who intend to use them to make an unsolicited "firm offer of credit or insurance" to a consumer. *Id*. § 1681b. Consumer may opt-out of prescreened credit offers. *Id*.

[54] *Id*. § 1681t(b).

[55] *Id*.

[56] *Id*.

[57] *Id*.

[58] *Id*.

[59] *Id*.

[60] 15 U.S.C. §§ 1692-1692p (2006). The Fair Debt Collection Practices Act does not directly address identity theft—it protects consumers from being coerced to pay debts fraudulently accumulated in that consumers name. *Id*.

Credit Billing Act of 1974,[61] and the Electronic Fund Transfer Act of 1978.[62] However, he FCRA, as amended by the FACT Act, is perhaps the most comprehensive federal law on identity theft. Congress passed the FACT Act in direct response to the growing threat of identity theft. As such, it represents one of the few successful congressional attempts to examine and pass a comprehensive set of identity theft protections.

Overall, the federal identity theft protections that apply to the credit industry take a varied approach to identity theft. The FCRA gives consumers specific rights with respect to the credit accounts and financial transactions in their names and also limits consumer liability for fraudulent transactions. It imposes certain requirements on credit reporting agencies, financial institutions and creditors, including rules mandating the protection and proper disposal of consumer credit information. Additionally, the FCRA limits how credit reporting agencies may share consumer credit reports.

It was enacted to "eliminate abusive debt collection practices by debt collectors." *Id*. Essentially, the Act prohibits debt collector from attempting to collect unpaid debts using abusive or coercive measures such as threatening violence or reputational harm, using profane language or making harassing phone calls. *Id*. Consumers may also stop debt collectors from contacting them by writing a letter requesting a collector make no more contact with the consumer. *Id*.

[61] Pub. L. No. 93-495, 88 Stat. 1500 (codified as amended in scattered section of 15 U.S.C. (2006)). The Fair Credit Billing Act was enacted "to protect the consumer against inaccurate and unfair credit billing and credit card practices." *Id*. The Act applies to creditors "who regularly extend, or arrange for the extension of credit . . . for which the payment of a finance charge is or may be required." *Id*. Essentially, the Act sets procedures through which credit card holders may challenge disputed charges on their bills and limits consumers' liability for any fraudulent charges. *Id*.

[62] Pub. L. No. 90-321, 82 Stat. 164 (1978) (codified as amended in scattered sections of 15 U.S.C. (2006)). The Electronic Fund Transfer Act was enacted to "[establish]" the rights, liabilities, and responsibilities of participants in electronic fund transfer systems." *Id*. Its primary purpose was to give consumers certain rights when making electronic fund transfers, which include debit card transactions. *Id*. The Act requires merchants to disclose certain information regarding fees, liability, and limits to consumers and also limits consumer liability for fraudulent electronic fund transfers. *Id*.

Title V of the Gramm-Leach-Bliley Act: Privacy of financial information

In 1999, Congress passed legislation that limited the information sharing practices of financial institutions. The Gramm-Leach-Bliley Act (GLB Act) of 1999 was primarily enacted to deregulate the financial industry and "to enhance competition in the financial services industry."[63] The GLB Act repealed the more restrictive Glass-Steagall Act,[64] which was passed soon after the Great Depression and heavily restricted affiliation among financial institutions.[65] Only part of the GLB Act was intended to protect personally identifiable information held by financial institutions.

Under the new regime, financial institutions have greater freedom to share customer information. In light of the privacy implications raised by the deregulation, Title V of the GLB Act also imposed certain privacy standards with respect to consumer financial information.[66] In Subtitle A, Congress imposed information privacy obligations on financial institutions.[67] The FTC and the other federal financial regulatory agencies were directed to promulgate and enforce rules as "necessary to carry out the purposes of [Subtitle A]" of the GLB Act.[68] Subtitle B of Title V specifically prohibited "pretexting"—the practice of using false pretenses to obtain

[63] Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[64] Pub. L. No. 44, ch. 89, 48 Stat. 162 (1933), 12 U.S.C. §§ 78, 377 (repealed 1999).

[65] SOLOVE, ROTENBURG & SCHWARTZ, *supra* note 22, at 714.

[66] Pub. L. No. 106-102, tit. V, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801-6809, 6821-6827).

[67] *Id*. §§ 501-10.

[68] *Id*. §§ 504-05.

customer information from financial institutions—and established criminal penalties for violations of the pretexting ban. [69]

Title V, Subtitle A of the GLB Act attempted to protect consumer privacy in financial information in two ways. First, it required the FTC and federal banking regulatory authorities to implement measures to "protect the security and confidentiality of [their] customers' nonpublic personal information."[70] Second, the Act limited financial institutions' ability to share "nonpublic personal information" with third parties. The resulting agency rules lay out the specific requirements of financial institutions with respect to safeguarding and sharing personal information.

Information sharing rules. Pursuant to the GLB Act, the FTC and the federal bank regulatory agencies issued a joint rule, known as the Financial Privacy Rule.[71] The rule requires that financial institutions provide customers with a privacy notice annually, which details the companies' information sharing practices.[72] This rule distinguishes between three types of information sharing: 1) affiliate sharing;[73] 2) third-party sharing for marketing purposes;[74] and 3)

[69] *Id*. §§ 521-27. "Pretexters" use false pretenses, to solicit personal information from individuals or businesses, which they then sell to other people. *See id*. § 6821(a).

[70] *Id*. § 501(a).

[71] 16 C.F.R. § 313 (2009).

[72] 16 C.F.R. § 313 (2009).

[73] Under GLB financial institutions may share information freely with their affiliates, whether such affiliates are financial or non-financial institution. 16 C.F.R. § 313 (2009). "An affiliation exists when one company 'controls', is controlled by, or is under common control with another company." *Id*. (citation omitted).

[74] Third-party sharing for marketing purposes is sharing with any non-affiliated third party, except when that party is performing a valid business service for the financial institution that necessitates access to personally identifiable financial information. 16 C.F.R. § 313 (2009). Non-affiliated third parties are not permitted to sell any of this information. *Id*.

third-party sharing for business purposes.[75] Financial institutions must inform customers how their personal information is shared in all of these instances, but must only allow customers to opt out of third-party sharing for marketing purposes.[76] Additionally, certain personally identifiable information, including account numbers and credit card numbers, may never be shared, except with credit reporting agencies.[77] Essentially, the Financial Privacy Rule limits the sharing of personal information by financial institutions only to the extent that consumers take affirmative steps to "opt out" of having their own information shared with third parties.[78]

Information security rules. Pursuant to Title V of the GLB Act, the FTC, the federal banking regulatory agencies, and the SEC each promulgated information security and protection rules. These rules are substantively similar to each other since each was promulgated pursuant to the same provisions of the GLB Act.[79] The FTC's information protection rule, the Safeguards Rule, took effect in 2003. It mandates that financial institutions "develop, implement and maintain a comprehensive information security program" that takes into account their own size, structure and particular characteristics.[80]

---

[75] Third-party sharing for valid business purposes includes, *inter alia*, bill processing, statement printing and customer services. 16 C.F.R. § 313 (2009).

[76] 16 C.F.R. § 313 (2009).

[77] 16 C.F.R. § 313 (2009).

[78] 16 C.F.R. § 314 (2009).

[79] *See* Interagency Guidelines Establishing Information Security Standards (Security Guidelines), 12 C.F.R. § 30 (Dep't of the Treasury, Office of the Comptroller of Currency), §§ 208, 225 (Fed. Reserve Sys.), § 364 (Fed. Depository Insurance Corp.), §§ 568, 570 (Dep't of the Treasury, Office of Thrift Supervision) (2009); SEC Regulation S-P, 17 C.F.R. § 248 (2009); Safeguards Rule (FTC), 16 C.F.R. § 314 (2009).

[80] 16 C.F.R. § 314.3(a) (2009).

The FTC's Safeguard Rule applies to all financial institutions that are not within the specific regulatory authority of the federal financial regulatory agencies.[81] The financial institutions within the FTC's regulatory arm include companies that are "significantly engaged" in financial activities, including "non-bank mortgage lenders, loan brokers . . . financial or investment advisers, real estate settlement services, and debt collectors."[82] Recently, the FTC has charged several companies for violating the Safeguards Rule, as well as the Financial Privacy Rule. [83]

USA PATRIOT Act and the Customer Identification Program: Identity verification

Another, perhaps unlikely, source of consumer information protection, according to the ID Theft Taskforce, is the USA PATRIOT Act of 2001.[84] Section 326 of the Act amended the Bank Secrecy Act to require financial institutions to take certain steps to verify the identity of new accountholders.[85] The Secretary of the Treasury, in conjunction with federal bank regulatory agencies, was directed to implement rules "setting forth the minimum standards for financial institutions . . . regarding the identity of [customers] in connection with the opening of an

[81] The FTC's authority under the GLB Act does not extend to banks, credit unions, securities brokers or other financial institutions that are under the specific authority of the Department of the Treasury, Office of the Comptroller of Currency; Federal Reserve System; Federal Deposit Insurance Corporation; Department of the Treasury; or National Credit Union Administration. Gramm-Leach-Bliley Act, Pub. Law No. 106-102, § 505, 113 Stat. 1338, (1999) (codified at 15 U.S.C. § 6805 (2006)).

[82] PRESIDENT'S IDENTITY THEFT TASKFORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, vol. II supp. at 3, *available at* http://www.idtheft.gov/reports/VolumeII.pdf (2007) (last visited March 10, 2009).

[83] FTC.gov, Privacy Initiatives, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited March 10, 2009).

[84] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[85] USA PATRIOT Act § 326.

account."[86] While the rules were actually enacted to combat terrorist financing and money laundering, they may deter identity thieves who would attempt to use a consumer's identity to open a fraudulent bank account.[87]

The resulting rules apply to all "financial institutions," defined broadly under the Bank Secrecy Act to include "commercial banks . . . foreign banks in the United States, thrifts, credit unions, private banks, trust companies, investment companies, brokers and dealers in securities, futures commission merchants, insurance companies, travel agents, pawnbrokers, dealers in precious metals, check-cashers, casinos, and telegraph companies, among many others."[88]

Under the rules, a financial institution must implement a documented Customer Identification Program (CIP) that details its "risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable." Essentially, this means that each financial institution decides what types of identity verification documentation to accept and how to verify the information a customer provides. The rule does not specifically mandate how institutions must verify customer's identity but it does specify certain minimum standards.

Prior to opening a new customer account, financial institutions must obtain a customer's name, date of birth, taxpayer identification number, and a residential or business address.[89] Then, the financial institution must verify the customer's identity information by either requesting documentary evidence from the customer—e.g., an unexpired driver's license—or by

[86] *Id*.

[87] *Id*.

[88] Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 31 C.F.R. § 103 (2009).

comparing the identity information provided with information from another source, such as a credit report or public database.[90] Financial institutions are also required to maintain a record of all of the customer identity information obtained, document the procedures taken to verify the information, and check customer names against terrorist watch lists.[91]

While the CIP rules require financial institutions to take certain minimum steps to verify customer identity, the mandatory record keeping requirements of the CIP may raise some privacy implications because they require financial institutions to collect, document and maintain specific personal information. Additionally, the role of CIP in combating identity theft is speculative. Individuals may never find out that an identity thief tried to use their information to open an account at one financial institution. Further, financial institutions are not required to report each instance where they are unable to verify a customer's identity; they must simply refuse to open such accounts.[92] Potentially, this means that an identity thief could simply continue attempting to fraudulently use the stolen information by applying to open a new account at a different institution.

Health Insurance Portability and Accountability Act: Health information privacy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted primarily to improve the continuity of health insurance coverage and to promote lower health

---

[89] For individuals who do not have a physical address, financial institutions must obtain the address of the individual's next of kin or another personal contact. *Id*.

[90] *Id*.

[91] *Id*.

[92] *Id*.

care costs by streamlining the procedures for transmitting health care information.[93] In order to improve efficiency, Congress instituted a uniform billing code and provided for the development of an electronic system for processing health care information.[94] HIPAA as originally enacted did not regulate health care privacy, but the new electronic billing provisions raised privacy concerns among members of Congress because they enabled easy of sharing health care information.[95] Congress was unable to reach agreement on the privacy provisions, so it left the specifics to the Department of Health and Human Services (HHS).[96] Congress also gave the HHS the authority to establish rules for the protection of electronically stored health care information.[97]

The HIPAA information security rules went into effect in 2003, and impose "a series of administrative, technical, and physical security procedures" upon covered entities in order to ensure the confidentiality of electronically-maintained protected health information."[98] The HIPAA privacy rules went into effect in 2001.[99] Prior to HIPAA, medical information was often shared without patients' consent.[100] In promulgating the privacy rules, the HHS cited numerous

[93] Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[94] *Id*.

[95] *See* Tamela J. White & Charlotte A. Hoffman, *The Privacy Standards under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 W. VA L. REV. 709 (2004); DANIEL J. SOLOVE, MARC ROTENBURG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 696, 380 (2006).

[96] Pub. L. No. 104-191, § 262(a), 110 Stat. 2024 (1996) (codified at 42 USCS § 1320d-2 (2000)).

[97] *Id*.

[98] *Id*.

[99] Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160 (2009).

[100] *Id*.

health information security breaches, some accidental and others deliberate.[101] While there is no provision in the HIPAA privacy rules that refers specifically to identity theft, it is clear that this crime was one of the HHS's major concerns; health records contain detailed personal information about individuals, far beyond just medical history.[102]

HIPAA applies to health care plans,[103] health care clearinghouses,[104] and health care providers who transmit health care data electronically,[105] referred to collectively as "covered entities."[106] The privacy rules restrict the transmission of "individually identifiable health information" (IIHI),[107] including name, date of birth, SSN, dates of medical procedures, and identifying physical characteristics.[108] Basically, IIHI means personal health care information

---

[101] *Id*.

[102] *Id*.

[103] "*Health plan* means an individual or group plan that provides, or pays the cost of, medical care." § 160.103 (citations omitted).

[104] "*Health care clearinghouse* means a public or private entity, including a billing service, repricing [sic] company, community health management information system or community health information system . . . that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format . . . into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format . . . for the receiving entity." *Id*.

[105] "*Health care provider* means . . . a provider of medical or health services . . . and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. *Id*. (citations omitted).

[106] *Id*. § 160.102.

[107] *Id*.

[108] "*Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and: 1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." *Id*.

that, if released, would identify the person to whom it refers. Covered entities may only disclose IIHI under certain circumstances to authorized individuals.[109]

The HIPAA privacy rules essentially establish a minimum threshold for privacy protection, requiring covered entities to implement policies and procedures that protect privacy at least to the extent required by HIPAA. Covered entities also must hire a Chief Privacy Officer tasked with enforcing the privacy rules within the organization.[110] Furthermore, HIPAA does not exempt state laws which impose additional, more stringent requirements, on the sharing of individually identifiable health information.[111] Thus, many states have enacted health care privacy laws that go beyond that of HIPAA.[112]

Congress passed HIPAA to address both the transferability of health insurance and the need for efficiency in processing patient information for billing purposes. In doing so, it recognized that easier electronic sharing of patient information had serious privacy implications, creating the need for additional protections for personally identifiable health care information.

Driver's Privacy Protection Act: Privacy of driver's license information

In 1994, Congress enacted the Driver's Privacy Protection Act, limiting the ability of any state department of motor vehicles (DMV) to disclose the personal information contained in

---

[109] HIPAA Privacy Rule, 45 C.F.R. §§ 164.500-534 (2009) "A covered entity may not use or disclose protected health information, except as permitted or required" under these rules. *Id*. § 164.502 (2009). Individually identifiable health information may be disclosed to the individual to whom it pertains, to a third party with the consent of the individual, or to a third party for reasons involving treatment, payment, or health care operations. *Id*.

[110] *Id*.

[111] HIPAA, Pub. L. No. 104-191, § 1178, 110 Stat. 2024 (1996) (codified at 42 USCS § 1320d-7 (2000)).

[112] *See generally* Elec. Privacy Info. Ctr., Medical Privacy, http://epic.org/privacy/medical/#stateLaw (last visited March 10, 2009).

individuals' motor vehicle records.[113] Essentially, DMVs may only disclose personal information to entities that are specifically permitted by the Act to receive driving-record information.[114] Under the law, authorized recipients include law enforcement and other government agencies, courts, insurers, licensed private investigators and employers.[115] If the requestor is not specifically authorized under the Driver's Privacy Protection Act, then it may only be disclosed with the express, written consent of the individual to whom the personal information pertains.[116]

Family Educational Rights and Privacy Act: Privacy in education records

Congress passed the Family Educational Rights and Privacy Act in 1974 to limit the disclosure of personal information contained in student records.[117] The Act applies to all institutions and schools that receive federal funding.[118] Essentially, the Act gives parents of children under eighteen the right to control how their children's student information is disclosed.[119] Upon turning eighteen, these rights are transferred to the student. Without written consent, schools generally may not share the information contained in student records with other parties. This prohibition on disclosure is subject to some limited exceptions. For example, schools may disclose such information in response to court subpoenas. They may also disclose

[113] 18 U.S.C. §§ 2721-25 (2006).

[114] 18 U.S.C. § 2721.

[115] *Id*.

[116] *Id*.

[117] 20 U.S.C. 1232g (2009).

[118] 20 U.S.C. 1232g (2009).

[119] *Id*.

such information to third parties who are conducting research on behalf of the school.[120] However, once a child turns eighteen, schools may not disclose such information to a child's parents without the consent of the student/child to whom the information pertains.[121] Parents do not maintain the rights to access to their child's student information once the child turns eighteen.[122]

Federal Trade Commission Act: Federal ban on unfair and deceptive trade practices

The FTC has broad consumer protection powers that give the agency the authority to bring actions against to enforce the federal ban on unfair business practices. Section 5 of the Federal Trade Commission Act (FTC Act) directs the FTC to "prevent persons, partnerships, or corporations" from engaging in "unfair and deceptive acts or practices in or affecting commerce."[123] Unfair and deceptive practices are those which "cause or are likely to cause reasonably foreseeable injury within the United States."[124]

The FTC has the power to deem practices "unfair" where they "cause[] or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[125]

---

[120] *Id*.

[121] *Id*.

[122] *Id*.

[123] 15 U.S.C. § 45(a) (2006). The FTC's enforcement power does not apply to banks, savings and loans, federal credit unions or other entities that are specifically subject the regulatory authority of a different federal agency. *Id*.

[124] *Id*.

[125] *Id*. If the FTC believes that an entity is engaging in unfair practices, it may initiate enforcement proceedings by notifying the entity of the charges and scheduling a hearing. At the hearing, the respondent may request leave to present evidence to defend its practices. *Id*. After the hearing, if the FTC finds the acts in question are "unfair," the agency will issue an order requiring the respondent to "cease and desist" from engaging in such acts. Such orders

After conducting an adjudicatory hearing regarding the practices in question, the Commission may issue a cease-and-desist order, which becomes final after sixty days if not appealed.[126] Violations of final cease and desist orders are subject to civil penalties of up to $11,000 per violation.[127]

After issuing a final order, the FTC may file suit against a respondent in federal district court seeking a permanent injunction, consumer redress, and other equitable relief. The FTC may also file a civil action for penalties against a respondent who violates a final order. Further, the FTC may enforce final cease and desist orders against non-respondents as well, seeking civil penalties where the agency can show that the non-respondent "had actual knowledge that such Act or practice was unfair and deceptive and is unlawful."[128] According to the FTC's Office of the General Counsel, actual knowledge is usual shown by proving that the FTC provided the non-respondent violator with a copy of the final order prohibiting the acts in question.[129]

Essentially, the FTC has the authority to bring civil actions and enforcement proceedings against a wide variety of businesses and individuals for unfairly or deceptively collecting, maintaining and sharing personal information, among other things. The FTC has used this authority to bring actions "involving the use or protection of consumers' personal

---

become final after 60 days, unless stayed by the FTC or a federal court. *Id*. The respondent may appeal the FTC order to a federal appeals court. *Id*.

[126] *Id*. § 45(b).

[127] *Id*. § 45(l).

[128] *Id*. § 45(m).

[129] *See* FTC, Office of the Inspector General, A Brief Overview of the FTC's Investigative and Law Enforcement Authority (July 2008), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm.

information."[130] For example, the FTC brought an action against Microsoft Corporation for failing to honor its privacy policy representations.[131] The agency also brought an enforcement action against Gateway Learning Corporation, seller of the "Hooked on Phonics" learn-to-read products, for disclosing consumer information to third-party marketers despite express assurances that the information would be kept private.[132] Additionally, the FTC has used its Section 5 power to bring actions against companies, including the data broker ChoicePoint, for failing to safeguard personal consumer information.[133]

Private entities now electronically maintain detailed information on vast numbers of individuals. Not only are the companies with which individuals have a business relationship collecting this information, but a number of other entities regularly collect, maintain and sell personally identifiable information as well. However, there is no one U.S. law that defines and regulates the private use of personal information under all circumstances.[134] Rather, there are

[130] FTC Web site, Consumer Protection, Division of Privacy and Identity Protection, http://www.ftc.gov/bcp/bcppip.shtm (last accesses Feb. 20, 2009).

[131] Microsoft Corp., 134 F.T.C. 709 (2002).

[132] Gateway Learning Corp., 138 F.T.C. 443 (2004). The company's privacy contained the following disclosures: (1) "We do not sell, rent or loan any personally identifiable information regarding our consumers with any third party unless we receive a customer's *explicit* consent . . . . [and (2)] We do not provide any personally identifiable information about children under 13 years of age to any third party for any purpose whatsoever." *See i.d.*. (emphasis added). According to the FTC, without informing customers of any changes to its privacy policy or obtaining "explicit" consent from consumers, Gateway began renting to marketers their customers' personal information , "including first and last name, address, phone number, and purchase history." *Id*. The rented information also included information about children under the age of 13, including "the age range . . . and gender of consumers' children." *Id*. These third-party marketers used the rented information "to send direct mail and make telemarketing calls" to the company's customers." *Id*.

[133] U.S. v. ChoicePoint, No. 1:06 civ. 198, FTC File No. 052-3069 (N.D. Ga. Feb. 15, 2006).

[134] *See* GOV'T ACCOUNTABILITY OFFICE, PERSONALLY IDENTIFIABLE INFORMATION, GAO-08-343 (2008). "No single federal law governs all uses of personally identifiable information. In addition to the laws that govern federal agency use of such information, a number of statutes provide privacy protections for information used for specific purposes or maintained by specific types of entities. For example, the Fair Credit Reporting Act applies to

numerous laws and regulations that mandate some information privacy in certain contexts. In addition to those information privacy laws that apply to private entities, there are some specific laws that apply to the federal government's record-keeping practices.

Public Sector Regulations

While much of the focus of the privacy debate lately has been on private record holders, the government is still one of the largest record holders in the United States. However, while the FTC oversees and enforces the record-keeping practices of many private entities, there is no clear central authority that monitors and enforces the government's information privacy practices or penalizes federal agencies for security breaches.

In a January 2008 report to Congress, the GAO identified two primary federal laws that govern the information practices of the federal government. The Privacy Act of 1974 restricts federal agencies' uses of personal information.[135] The E-Government Act of 2002 was enacted specifically to protect the personal information held by federal agencies and implement information security protections on all federal agency databases.[136] Additionally, pursuant to the Freedom of Information Act, agencies must allow public access to information held by public agencies while simultaneously protecting some types of personally identifiable information.[137]

Public records, although physically kept in multiple separate places, offer a wealth of information about individuals. Private companies such as data brokers often amass individual

---

companies that prepare or furnish information on consumer creditworthiness, and the Video Privacy Protection Act applies to the use of video rental records." *Id*.

[135] 5 U.S.C. § 552a (2006).

[136] Pub. L. No. 107-347, 116 Stat. 2899 (2002) (codified in scattered sections of 44 U.S.C.A (West 2008)).

[137] *See* Federal Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2006).

information from public records to create individual dossiers on millions of people.[138] With the proliferation of information technology, assembling personal information has become easier for entities such as database companies, as well as for identity thieves.

The concern over privacy in government kept records, which dates back to the 1950s and 60s, is made more complex by virtue of the fact that the public also has a right of access to many government records. By the 1960s, the government had begun using computers to store data, using the SSN as an identifier.[139] In 1966 Congress passed the Freedom of Information Act, giving the entire public a right of access to federal government records unless the records fell within one of nine exemptions,[140] one for privacy.[141]

Under FOIA, the government can not simply close all of its records and refuse to share them in order to protect personal information. This factor led to concerns over the government's collection and use of personal information, including the fear that the government would create one national database to store all its information on individuals, using the SSN as an identifier.[142] This fear was not unfounded. In the 1960s and 1970s, the government twice considered creating

---

[138] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1149 (2002).

[139] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1400-1403 (2001).

[140] 5 U.S.C. § 552(b).

[141] FOIA exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." *Id*. Rather than limiting the exemption by emphasizing the clause "personnel and medical files and *similar files* [emphasis added]," the Supreme Court has broadly interpreted this exemption to generally exempt from disclosure personal records if such disclosure would "constitute a clearly unwarranted invasion of personal privacy." *See* Dep't of State v. Wash. Post Co., 456 U.S. 595 (1982).

[142] Daniel J. Solove, Access and Aggregation, *supra* note 138, at 1149.

just such a database.[143] More recently, in 2000, the Bush administration pushed for a national identification system that links the records from all government agencies to enable easier information sharing.[144]

The public concern for privacy in government records prompted the Department of Health, Education and Welfare to conduct a study. The resulting report, known as the HEW Report,[145] was released in 1973 and proved to be very influential in setting privacy goals for the federal government.[146] This report condemned the universal use of SSNs as personal identifiers and recommended the implementation of a Code of Fair Information Practices.[147] The Fair Information Practices detailed certain responsibilities of the government as a record keeper, including the obligations to: 1) refrain from maintaining secret databases; 2) grant individuals access to their own records; 3) allow individuals to control the different uses of their information; 4) permit individuals to correct mistakes regarding their personal information; and 5) implement information security measures.[148] While the Fair Information Practices were never directly included in any legislation adopted by Congress, they did prove influential in shaping federal policies on privacy standards.

---

[143] *See* DANIEL J. SOLOVE, MARC ROTENBURG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 524 (2006).

[144] *See id*.

[145] U.S. DEP'T OF Health, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973) [hereinafter HEW REPORT], *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited March 10, 2009).

[146] DANIEL J. SOLOVE, MARC ROTENBURG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 577 (2006).

[147] *Id*. at 588.

[148] HEW REPORT, *supra* note145.

Privacy Act: Privacy of government records

The HEW Report was a motivating factor behind the passage of the Privacy Act of 1974, which is intended to control the federal government's collection, use and dissemination of personal information.[149] This Act is the primary federal law regarding the federal government's information practices.[150] Unless information is classified as a public record or fits within another exception, the Privacy Act generally prohibits federal agencies from distributing any personal information without the consent of the individual to whom it pertains.[151] The Act also restricts agency collection of personal information to what is "necessary and relevant" to the agency's purpose.[152] Under the Privacy Act, federal agencies are also required to inform individuals of how their information will be used and to safeguard personal information.[153]

In an apparent attempt to limit the use of the SSN as an identifier, the Privacy Act also prohibited local, state and federal agencies from denying benefits to individuals who refused to provide their SSNs.[154] However, this has done little to quell the use of SSNs to identify individuals and their records. First, the rule only applies to the public sector, not the private

[149] GOV'T ACCOUNTABILITY OFFICE, GAO-08-343, *supra* note 134.

[150] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified in scattered sections of 44 U.S.C.A. (West 2008)). Title III of this act, known as the Federal Information Security Management Act of 2002, requires agencies to develop, document, and implement agency-wide programs to provide security for their information and information systems. *Id*. §§ 301-305. Section 208 imposes certain information privacy obligations on federal agencies with respect to the electronic collection and dissemination of personal information. *Id*. § 208.

[151] 5 U.S.C. §§ 551-552 (2006). Court records are not covered by the Privacy Act. *Id*.

[152] *Id*.

[153] *Id*. Subsequently, Congress enacted the E-Government Act of 2002 in part as an effort to further protect personal information held by federal agencies. § 301, 116 Stat. at 3541-3549. Under this act, federal agencies are required to conduct assessments of their information collection and storage systems in order to improve security. *Id*. § 301, 116 Stat. at 3545.

[154] 5 U.S.C. § 551a (2006).

sector, and second, Congress has created many exceptions to this rule.[155] For example, under the Tax Reform Act of 1976, state agencies are exempt from the Privacy Act restriction where the SSNs are used "in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction."[156]

E-Government Act: Security of government records

In 2002, Congress passed the E-Government Act, specifically addressing the information security practices of the federal government.[157] This Act requires federal agencies to regularly analyze how they collect, store, share and manage personally identifiable information.[158] Agencies must also analyze and report their information practices before developing or implementing any new information systems in an effort to ensure that the intended systems conform to established security standards. Agencies are also required to identify both the security risks posed by new systems and look for alternative systems that might better mitigate any potential privacy threats.[159]

Another part of the E-Government Act is the Federal Information Security Management Act of 2002 (FISMA) that requires all federal agencies to "develop, document, and implement agency-wide programs to provide security for their information and information systems."[160] In

[155] *See* Daniel J. Solove, *Access and Aggregation*, *supra* note 138, at 1166 (discussing the Privacy Act's weak protection of SSNs).

[156] 42 U.S.C. § 405(c) (2000).

[157] E-Government Act §§ 301-305.

[158] *Id*. § 301.

[159] *Id*.

[160] GOV'T ACCOUNTABILITY OFFICE, GAO-08-343, *supra* note 134.

light of the numerous and varied information systems of federal agencies, FISMA also requires agencies to maintain and annually update an inventory of their information systems.[161] The E-Government Act is the primary law that addresses federal information security with respect to the changing technological landscape of the past decade or so. Many of the acts provisions and rules were enacted specifically in response to widespread and serious information security weaknesses within federal agencies.

The problem with this framework is that there is no central authority charged with overseeing the information security and privacy practices of the federal government and its agencies. The FTC monitors private entities and enforces compliance with applicable information security and privacy rules. Federal law enforcement agencies enforce criminal identity theft laws. However, the compliance of federal agencies is generally tracked through self-monitoring and self-reporting requirements. This lack of accountability is troublesome, especially in light of the numerous reports of information security breaches within the federal government.

Federal government's information security track record

In 2007, the Government Accountability Office (GAO) released a report on the vulnerability of SSNs in public records.[162] The report warned that public records held by the federal government pose a significant threat to the integrity of individual SSNs.[163] According to the GAO, SSNs and other personally identifiable information are often mistakenly released in

[161] *Id*.

[162] GOV'T ACCOUNTABILITY OFFICE, FEDERAL ACTIONS COULD FURTHER DECREASE AVAILABILITY IN PUBLIC RECORDS, THOUGH OTHER VULNERABILITIES REMAIN, GAO-07-752 (2007).

[163] *Id*.

public records instead of being redacted or truncated.[164] One reason may be that federal record keepers such as the IRS and DOJ regularly provide records containing Social Security numbers (SSN) to local and state record keepers.[165] Some of these state record keepers have for years sold complete copies of their files to private companies.[166]

According to the GAO, there are persistent, systematic weaknesses in the federal government's information security that consistently puts personal information at risk.[167] The GAO has categorized information security as "high risk" since 1997 but the federal government has thus far failed to adequately secure its systems. In fiscal year 2006, twenty-one of the twenty-four major federal agencies surveyed by the GAO reported significant weaknesses in information security.[168] The significance of this problem is highlighted by the spate of federal data breaches since 2003.[169]

For example, in 2006 a laptop containing the personal information of millions of veterans was stolen from the home of an employee of the Department of Veteran Affairs.[170] In 2005 and

---

[164] *Id*.

[165] *Id*.

[166] *Id*.

[167] GOVERNMENT ACCOUNTABILITY OFFICE, DESPITE REPORTED PROGRESS, FEDERAL AGENCIES NEED TO ADDRESS PERSISTENT WEAKNESSES, GAO-07-837 (2007).

[168] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development. GOV'T ACCOUNTABILITY OFFICE, GAO-08-343, *supra* note 134.

[169] Nineteen of the twenty-four major federal agencies reported at least one data breach since 2003. These breaches have involved hacking, physical intrusion, theft, and phishing. *Id*.

[170] *Id*.

2006, hackers gained access to the databases of the Department of Energy and the Department of Agriculture, respectively.[171] Also in 2006, the Department of Commerce discovered a security breach of its computer system. After going through eight months of logs, the department was unable to determine when the hackers first gained access to the system, which may suggest that the initial breach occurred more than eight months prior to its ultimate discovery.[172] Collectively, the IRS and the Census Bureau—two agencies that regularly collect sensitive personal information on millions of Americans—have lost more than 1,100 laptop and desktop computers since 2003, most of which contained personal information on multiple people.[173] Overall, in 2006 federal agencies filed a record number of information security incidence reports—5,146.[174]

The GAO attributed much of the information security weaknesses within the federal government to human error, stating that "people are one of the weakest links in attempts to secure systems and networks."[175] The report further concluded that many federal employees do not receive adequate information security training and may not even consider basic information security precautions such as regularly changing passwords.[176] Additionally, the GAO found that agencies also failed to implement basic information system safeguards, including: 1) system management controls to prevent the installation of unauthorized software on computer networks;

---

[171] *Id*.

[172] *Id*.

[173] *Id*.

[174] *Id*.

[175] GOVERNMENT ACCOUNTABILITY OFFICE, GAO-07-837, *supra* note 167.

[176] *Id*.

2) security measures to protect the physical integrity of computer facilities; 3) appropriate segregation of duties to prevent any one individual from independently controlling key systems; and 4) employee access levels to restrict employee access to only those systems and files necessary to the performance of the employee's official duties.[177]

Reports from the GAO paint a fairly dismal picture of information protection at the federal-government level. The federal government, with its many agencies and many separate information systems, has been unable to implement adequate security measures. This may be due in large part to the fact that there are so many separate agencies with different information systems. A one-size-fits-all approach is untenable. Furthermore, there is no central authority which oversees and enforces the federal government's compliance with information security and privacy standards. On the other hand, in the private sector the FTC and other federal agencies routinely bring actions against businesses to enforce consumer privacy and information security laws.

[177] *Id*.

CHAPTER 4
FEDERAL ENFORCEMENT OF INFORMATION PRIVACY AND IDENTITY PROTECTION

Most federal identity protections that apply to private entities come from one of two sources: criminal statutes or administrative rules.[1] Criminal identity theft laws are enforced by law enforcement officials through federal investigations and criminal prosecutions of identity thieves. Administrative rules are generally enforced by the agency that originally promulgated the rule. For example, the Federal Trade Commission (FTC) enforces the Safeguards Rules of the Gramm-Leach-Bliley Act (GLB ACT) that the agency promulgated in 2002 for financial institutions.[2]

Criminal Enforcement: Investigations and Prosecutions of Identity Theft

Violations of federal identity theft criminal statutes are investigated by multiple federal agencies.[3] The Secret Service, the Federal Bureau of Investigation and the U.S. Postal Inspection Service have jurisdiction to conduct identity theft investigations.[4] Working with

[1] The FTC also lists the Driver's Privacy Protection Act (DPPA) as one of the federal identity theft protections, even though it was enacted for privacy-related concerns other than identity theft. FTC.gov, Federal Laws: Privacy & Information Security, http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/federal-privacy.html (last visited March 10, 2009).

The provisions of the DPPA were specifically enacted by Congress and not left to the rule-making authority of any federal agency. 18 U.S.C. §§ 2721-2725 (2004). Further, the FTC does not have any enforcement authority with respect to the DPPA. *Id*. For violations of the DPPA, the Act provides for criminal fines against individuals and civil fines against state departments of motor vehicles. *Id*. § 2723. The DPPA also provides individuals with a private right of action against a "person who knowingly obtains, discloses or uses [that individual's] personal information." *Id*. § 2724.

[2] 16 C.F.R. § 314 (2009).

[3] *See, e.g.*, DOJ.gov (U.S. Dep't of Justice), Fraud Section, http://www.usdoj.gov/criminal/fraud/websites/idtheft.html (last visited March 10, 2009) ("Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases.").

[4] *Id*.

these agencies, the U.S. Department of Justice (DOJ) prosecutes identity theft crimes.[5] According to the ID Theft Taskforce Report, the DOJ prosecuted nearly 2,000 criminal defendants in 2006 for criminal identity theft under federal statutes, obtaining more than 1,500 federal identity theft convictions.[6] In 2007, these numbers rose by more than 25% to nearly 2,500 prosecutions and nearly 2,000 convictions.[7]

Information Privacy and Security: Federal Agency Enforcement

Medical Information Privacy

The U.S. Department of Health and Human Services (HHS) oversees the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule or the Security Rule, both of which apply to health care providers.[8] The Privacy Rule imposes upon health care providers minimum standards and restrictions on the use, disclosure, disposal, access and safeguarding of patient information.[9] The Security Rule imposes information security standards for the protection of electronically maintained and accesses patient information.[10] Violations of both the Privacy Rule and the Security Rule within the ambit of HHS are punishable by civil penalties. [11]

---

[5] *Id*.

[6] PRESIDENT'S IDENTITY THEFT TASKFORCE, TASKFORCE REPORT 37, *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf (2008) (last visited March 10, 2009).

[7] *Id*.

[8] Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), 45 C.F.R. §§ 160, 164 (2009); 45 C.F.R. § (2009); Health Insurance Reform: Security Standards (HIPAA Security Rule), 45 C.F.R. §§ 160, 162, 164 (2009).

[9] 45 C.F.R. §§ 160, 164.

[10] 45 C.F.R. §§ 160, 162, 164.

[11] HIPAA Administrative Simplification: Enforcement, 45 C.F.R. §§ 160, 164 (2009).

The department's Office for Civil Rights (OCR) reviews all HIPAA complaints filed in order to determine whether the complaints relate to possible criminal violations, Privacy Rule violations, or Security Rule violations.[12] Possible criminal violations are not investigated by the OCR but may, when appropriate, be referred to the U.S. Department of Justice for further review and investigation.[13] Possible Security Rule violations are referred to the Centers for Medicare and Medicaid Services (CMS) for investigation.[14] From April 14, 2003 through January 31, 2009, CMS conducted nearly 400 investigations of possible Security Rule violations.[15] Examples of common violations include failing to limit employee access to sensitive patient information and failing to implement secure login procedures for information systems.

OCR reviews the remaining Privacy Rule complaints by first conducting a preliminary inquiry into the allegations and then, when necessary, formally investigating any identified possible Privacy Rules violations.[16] If OCR determines that an entity has violated the Privacy Rule, it either obtains a voluntary compliance agreement from the violating entity or takes corrective action.[17] Such corrective action often involves OCR entering into a written consent agreement with the violating entity that details the steps the entity will take to bring its actions in

[12] HHS.gov (Dep't of Health and Human Services), Office for Civil Rights, *Health Information Privacy*, http://www.hhs.gov/ocr/privacy/index.html (last visited March 10, 2009).

[13] *Id*.

[14] *Id*.

[15] HHS.gov (Dep't of Health and Human Services), Centers for Medicare & Medicaid Svcs., *Security Standards*, http://www.cms.hhs.gov/SecurityStandard/ (last visited March 10, 2009).

[16] HHS.gov, *Health Information Privacy*, *supra* note 12.

[17] *Id*.

compliance with the HIPAA Privacy Rule.[18] OCR also may issue formal findings, detailing the ways in which the entity has violated the rule and mandating certain corrective action.[19] In addition, OCR may impose civil penalties against entities for HIPAA violations that may subsequently be challenged in front of an Administrative Law Judge (ALJ).[20] After the period for appeal of a civil penalty has expired or an ALJ has affirmed the agency determination, OCR may file an action in U.S. District Court to collect the fines imposed.[21]

According to OCR, the most common violations of the HIPAA Privacy Rule involve the unauthorized use or disclosure of patient information, including disclosures to third parties such as law enforcement officials, patient employers and the media.[22] The other most common violations include failing to safeguard patient information, failing to grant individuals access to their own medical records, and failing to limit the disclosure of patient information to the "minimum necessary."[23] The HIPAA Privacy Rule went into effect in April 2003. Through January 1, 2009, OHS had conducted more than 11,000 formal investigations of possible Privacy Rule violations.[24] In approximately two-thirds of these investigations, OCR found actual violations of the Privacy Rules and, subsequently, took corrective action.[25] In addition to the

[18] *Id*.

[19] *Id*.

[20] *Id*.

[21] *Id*.

[22] *Id*.

[23] *Id*.

[24] *Id*.

[25] President's Identity Theft Taskforce, Taskforce Report, *supra* note 6, at 42.

privacy violations investigated by OCR, the Department of Health and Human Services has investigated identity theft related to the healthcare system.[26] According to the ID Theft Taskforce, these thefts have involved either using a stolen identity to obtain medical services or using a doctor's stolen identity to fraudulently bill Medicare or Medicaid.[27]

Financial Information

The FTC has one of the broadest roles in setting and enforcing federal privacy and identity theft policies and regulations. The FTC is specifically responsible for enforcement of the Gramm-Leach Bliley Act (GLB Act) privacy and information protection rules that apply to financial institutions, as well as the Fair Credit Reporting Act (FCRA) protections for consumer credit report information.[28] In addition, the FTC has broad consumer protection powers that give the agency the authority to bring actions against "persons, partnerships, or corporations" which engage in "unfair" practices, including those "involving the use or protection of consumers' personal information."[29] Sometimes, the FTC also assists law enforcement agencies in the investigation and prosecution of identity theft crimes.[30]

---

[26] *Id*.

[27] *Id*.

[28] *See, supra,* Chapter Three, pp. 57-60. The FTC's enforcement authority under these rules applies to all financial institutions except those, such as banks, thrifts, credit unions, brokers and dealers, which are specifically regulated by other federal financial regulatory agencies, such as the SEC, the Federal Deposit Insurance Corporation and the Federal Reserve Board. Laws against financial institutions not within the authority of the FTC are enforced by the federal agency with specific jurisdiction over that institution.

[29] Federal Trade Commission Act (FTC Act) § 5(a)(2), 15 U.S.C § 45 (a)(2) (2000) ("However, the Commission's power under Sec. 5 does not extend to " banks, savings and loan institutions . . . federal credit unions . . . common carriers . . . air carriers and foreign air carriers . . . and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921.").

[30] *See* FTC.gov, Privacy Initiatives Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/ promises_enf.html (last visited March 10, 2009).

The FTC is the federal agency that maintains the ID Theft Clearinghouse, the federal database of consumer identity theft complaints. In 1999, Congress passed its first identity theft bill, the Identity Theft Assumption and Deterrence Act of 1998, which specifically established identity theft as federal criminal offense.[31] In addition to the act's criminal provisions, Congress directed the FTC to establish and maintain a central repository for all consumer identity theft complaints.[32]

The FTC is responsible for tracking and forwarding identity theft complaints to law enforcement agencies and consumer reporting agencies as appropriate.[33] Additionally, the FTC provides identity theft victims with helpful information and guidance.[34] Essentially, the FTC serves as a central point of contact for identity theft complaints in the United States, collecting information from consumers and sharing it with law enforcement and businesses. In addition to its reporting and tracking duties, the FTC chairman serves as the co-chair of the President's Identity Theft Taskforce (ID Theft Taskforce" or 'Taskforce).[35]

The FTC enforces the consumer protection laws within its ambit through its Consumer Protection Bureau.[36] According to the FTC's Web site, "the Bureau conducts investigations, sues companies and people who violate the law, develops rules to protect consumers, and

[31] Pub. L. No. 105-318, 112 Stat. 3007 (codified at 18 U.S.C. § 1028 (2006)).

[32] *Id*. § 5.

[33] *Id*.

[34] *Id*.

[35] IDTheft.gov, President's Identity Theft Taskforce, *About the Taskforce*, http://www.idtheft.gov/about.html.

[36] *See* FTC.gov, Bureau of Consumer Protection, http://www.ftc.gov/bcp/about.shtm (last visited March 10, 2009).

educates consumers and businesses about their rights and responsibilities."[37] The agency's newest division, the Division of Privacy and Identity Protection, "oversees issues related to consumer privacy, credit reporting, identity theft, and information security."[38]

Federal Trade Commission enforcement proceedings

In general, the FTC's enforcement authority includes the power to investigate and prosecute claims, on behalf of the United States, against private entities that violate U.S. consumer privacy and protection laws.[39] The agency may investigate the practices of private entities that it believes are violating these laws.[40] The FTC's investigative power includes the authority to subpoena witnesses and documentary evidence "relating to any matter under [FTC] investigation."[41] Further, if a business or witness fails to comply with an FTC subpoena, the agency may seek enforcement of its subpoena in a U.S. district court.[42] After conducting an investigation, the agency may institute enforcement proceedings where it has "reason to believe" the law is, or has, been violated.[43]

[37] *Id*.

[38] FTC.gov, Division of Privacy and Identity Protection, http://www.ftc.gov/bcp/bcppip.shtm (last visited March 10, 2009).

[39] FTC Act § 3, 15 U.S.C. § 43 (2006) (giving the FTC the authority to "prosecute any inquiry necessary to its duties in any part of the United States").

[40] *Id*. § 6(a).

[41] *Id*. § 9.

[42] *Id*.

[43] *Id*.

The FTC may enforce consumer privacy and protection laws by initiating administrative enforcement proceedings or by filing an action in district court.[44] In an administrative action, the FTC issues a complaint alleging violations of the law.[45] The respondent may either challenge the complaint or consent to the entry of a final order.[46] By signing a consent agreement, the respondent accepts the order of the FTC without admitting liability and waives the right to appeal the order.[47] The full commission then votes on whether to accept the consent agreement. Once the consent agreement is accepted, it becomes a final order.[48]

If a respondent challenges an FTC complaint, it is adjudicated before an administrative law judge, who then issues an initial decision recommending either the entry of a cease-and-desist order or dismissal of the action.[49] The initial decision may be appealed to the full commission.[50] Once the commission conducts its own hearing on appeal, it issues a final decision and order.[51] If the initial decision is not appealed, it becomes a final order after sixty days.[52]

---

[44] *See* FTC, Office of the Inspector General, *A Brief Overview of the FTC's Investigative and Law Enforcement Authority* (July 2008), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm (last visited March 10, 2009).

[45] FTC Act § 5.

[46] *Id*.

[47] *Id*.

[48] *Id*.

[49] *Id*. Either party—the FTC or the responding party—may appeal the administrative law judge's initial decision to the whole Commission. *Id*.

[50] *Id*.

[51] *Id*. Such a final decision and order of the FTC may be appealed to one of the U.S. Courts of Appeal. *Id*.

[52] *Id*.

If a respondent violates a final order of the FTC, the FTC may file an action against the respondent in federal district court, seeking civil penalties of up to $11,000 per violation.[53] Further, after a final order is issued by the FTC, the agency may subsequently file an action in federal district court seeking consumer redress or other equitable or monetary relief from a respondent.[54] While the FTC must file a civil action in federal court to obtain monetary relief, the commission may as part of a final order directly issue a cease-and-desist order and also impose reporting or oversight requirements on respondents.[55]

Since the FTC must file suit in federal court to request civil penalties or other monetary relief stemming form its administrative proceedings, many of its enforcement actions are filed directly in federal district court in lieu of initiating the action before an administrative tribunal.[56] Bypassing the administrative process and filing an action directly in federal district court is often a more efficient process.[57] At the outset of a district court action, the FTC may seek a preliminary injunction temporarily barring a respondent's allegedly violating conduct pending final adjudication of the matter.[58] On the other hand, an FTC cease-and-desist order does not become effective until the administrative action is final and the time to appeal has expired. Additionally, if a respondent violates an FTC cease-and-desist order, the FTC may ultimately have to file an action for injunctive relief in federal district court requesting the court order the

[53] *Id*.

[54] FTC Act § 19.

[55] FTC Act § 5.

[56] *See* FTC, Office of the Inspector General, A Brief Overview, *supra* note 44.

[57] *Id*.

[58] FTC Act § 13(b).

respondent to comply with the FTC's order. Filing directly in district court and bypassing an administrative proceeding may enable the FTC to streamline some enforcement actions. In a district court action the FTC may seek a determination that the conduct in question is unlawful in the same action as its request for a preliminary injunction and award of other equitable relief and civil penalties.[59]

Remedies in Federal Trade Commission enforcement actions

In any consumer protection action the FTC may seek monetary relief to redress consumer harm and to require respondents to "disgorge" the profits they have derived from their unlawful conduct.[60] In addition, the FTC may seek civil penalties in some actions. The consumer credit provisions of the FCRA specifically provide for the levying of civil fines of up to $2,500 per violation of the act.[61] However, the agency does not have the same ability to seek civil fines for initial violations of the GLB Act or Section 5 of the Federal Trade Commission Act (FTC Act).[62] Only after a final determination that a company's conduct violates one of these acts will a respondent be subject to civil penalties for subsequent violations of the same kind. In April 2008, the FTC testified before Congress that its inability to levy civil fines in most information security and pretexting enforcement actions hinders the deterrent effects of its enforcement authority.[63] Seemingly, the actions the FTC brings pursuant to the FCRA carry a greater threat

[59] *Id*. §§ 13, 19.

[60] *Id*.

[61] 15 U.S.C. § 1681s(a) (2006).

[62] FTC Act § 5(m).

[63] *Prepared Statement of the FTC: Hearing on the FTC Reauthorization Act of 2008 Before the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. (2008), *available at* http://www.ftc.gov/os/testimony/P034101reauth.pdf (last visited March 10, 2009).

of immediate financial penalties, as opposed to those brought for non-FCRA violations in which civil penalties are not initially assessed.

Since 1999, the FTC has brought a number of actions to enforce the privacy and identity theft regulations under its authority. The agency has brought at least eleven actions[64] against private businesses and individuals for pretexting.[65] Additionally, the agency has brought more than forty actions against businesses, ranging from mortgage companies to retailers, for privacy and information-security-related violations.[66]

Enforcement of information privacy and security standards

FTC actions that relate to the privacy or information security standards of private businesses are brought pursuant to the agency's authority to enforce the GLB Act, the FCRA or Section 5 of the FTC Act. Pursuant to Section 5 of the FTC Act, the FTC filed an action in 2002 against Microsoft Corporation for misrepresenting the security and data collection procedures of its .NET Passport program .[67] One of the services offered by .NET Passport is Passport Wallet, a secure payment service. Passport Wallet collects and stores consumers' credit card numbers and address information and enables consumers to use the stored information to make purchases at participating Web sites.[68] According to the FTC, Microsoft made "false or misleading"

[64] *See* FTC.gov, Privacy Initiatives, *supra* note 30.

[65] "Pretexters" use false information to solicit personal information from financial institutions which they then sell to third parties. *See* Gramm-Leach-BlileyAct, 15 U.S.C. § 6821(a) (2006).

[66] *See* FTC.gov, Privacy Initiatives, *supra* note 30.

[67] Microsoft Corp., 134 F.T.C. 709 (2002).

[68] *Id*.

representations that purchases made using Passport Wallet were more secure than those made using other secure payment services. [69]

In addition, the FTC alleged that Microsoft collected personally identifiable information, including user sign-in history, despite its representations to the contrary.[70] As part of its settlement with the FTC, Microsoft agreed to change its privacy policies, implement tougher security measures for its Passport program, and submit biannual security certifications to the FTC.[71] The Microsoft settlement did not include any fines or monetary penalties.[72] However, the company may be subject to civil penalties in the future for violations of the order.[73]

In another Section 5 action, the FTC filed a complaint against CardSystems Solutions, Inc. in 2006 for failing to take appropriate measures to secure personal financial information.[74] CardSystems processes the credit and debit card transactions of more than 119,000 merchants. In 2005 the company processed more than 200 million transactions, totaling more than $15 billion.[75] According to the FTC complaint, "CardSystems collected personal information from the magnetic strip of the [credit cards it] processed, including the card number, expiration date,

---

[69] *Id*. at 715.

[70] *Id*.

[71] *Id*.

[72] *Id*.

[73] Violations of final orders issued by the FTC are subject to up to an $11,000 civil fines per violation. FTC Act § 5, 15 U.S.C. § 45 (2006).

[74] CardSystems Solutions, Inc., 2005 F.T.C. LEXIS 176, FTC File No. 052-3148 (Sep. 5, 2006)*; see also* Press Release, FTC, CardSystems Solutions Settles FTC Charges: Tens of Millions of Consumer Credit and Debit Card Numbers Compromised (Feb. 23, 2006) (available in electronic form at http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm).

[75] 2005 F.T.C. LEXIS 176.

and other data.[76]" The information collected was then stored on CardSystems' computer network.[77] In what the FTC characterized as the "largest known compromise of financial data to date," hackers gained access to CardSystem's computer networks, compromising millions of credit and debit cards and resulting in millions of dollars in fraudulent purchases.[78]

No fines were levied against Microsoft or Card Systems since both actions were brought pursuant to Section Five of the FTC Act. However, the settlement of other FTC actions has resulted in steep monetary fines.[79] For example, in 2006 ChoicePoint—one of the largest data brokers in the United States—was fined $15 million after at least 163,000 consumer records under its control were compromised.[80] According to the FTC, at least 800 cases of identity theft resulted from ChoicePoint's negligence.[81]

The company was charged with violating the FCRA and Section 5 of the FTC Act by providing consumer credit reports to people and entities that were not legally permitted to obtain such information.[82] In some instances, ChoicePoint actually approved subscribers who applied to receive consumer reports using SSNs that had shown up on the company's own internal

---

[76] *Id*.

[77] *Id*.

[78] *Id*.

[79] *See* FTC.gov, Privacy Initiatives, *supra* note 30.

[80] U.S. v. ChoicePoint, No. 1:06 civ. 198, FTC File No. 052-3069 (N.D. Ga. Feb. 15, 2006); *see also* Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

[81] ChoicePoint, No. 106-CV-0198, FTC File No. 052-3069.

[82] *Id*. The FTC also alleged that ChoicePoint had engaged in unfair and deceptive trade practices by representing in its privacy policies that it had "implemented reasonable and appropriate measures . . . to maintain the confidentiality and security of consumers' personal information." *Id*.

reports as being linked to fraud on other subscriber accounts.[83] The FTC complaint against ChoicePoint alleged that the data broker regularly approved subscriber applications without sufficiently verifying the information and credentials supplied by subscribers.[84]

In order to verify the information supplied by an applicant, ChoicePoint regularly accepted without further inquiry items that "called into question the authenticity of the applicant's business."[85] For example, the data broker approved business applications that listed an address containing an apartment number or a P.O. Box as the physical business address.[86] In some cases, the data broker accepted a statement for residential phone service as verification of an applicant's business address.[87] In order to authenticate the actual existence of an applicant's business, ChoicePoint apparently routinely accepted documentation that the FTC characterized as "facially contradictory or illogical."[88] The FTC complaint alleged that ChoicePoint sometimes accepted articles of incorporation for inactive or suspended corporations and tax registration documents that showed that a business' registration had been cancelled prior to submission of the application.[89] In addition, the FTC reported that ChoicePoint "approved without further inquiry"

[83] *Id*.

[84] *Id*.

[85] *Id*.

[86] *Id*.

[87] *Id*.

[88] *Id*.

[89] *Id*.

applications despite the fact that applicants left blank "critical information," such as a business license number, contact information or even an applicant's last name."[90]

While the ChoicePoint case involves the largest FTC fine ever imposed, the FTC also has levied some hefty fines against other businesses.[91] In 2000, the FTC filed actions against each of the three major U.S. credit reporting companies—Experian, Trans Union and Equifax—that resulted in a total of $2.5 million in fines.[92] In its complaints, the FTC alleged that the businesses had routinely blocked calls from consumers who were calling to dispute credit report items.[93]

Each of the three credit reporting companies has a dedicated toll-free number for consumers to call "concerning questions [about] their consumer reports or to dispute items that they believe to be inaccurate in their consumer reports."[94] According to the FTC complaints, over one million calls to both Experian and Trans Union, as well as hundreds of thousands of calls to Equifax, "received a busy signal or message indicating that the consumer must call back because all representatives are busy."[95] Other callers had to wait on hold for an "unreasonable" amount of time.[96] All in all, the FTC concluded that a substantial number of consumers were

---

[90] *Id*.

[91] *See* FTC.gov, Privacy Initiatives, *supra* note 30.

[92] *See* Press Release, FTC, Nation's Big Three Consumer Reporting Agencies Agree To Pay $2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act (Jan. 13, 2000), *available at* http://www.ftc.gov/opa/2000/01/busysignal.shtm (last visited March 10, 2009).

[93] *Id*.

[94] *See* FTC.gov, Privacy Initiatives, *supra* note 30.

[95] *Id*.

[96] *Id*.

unable to reach representatives of the three credit agencies during normal business hours.[97] Pursuant to Section 621 of the FCRA, these agencies could have been fined up to $2,500 for each knowing violation of the FCRA. Potentially, this means the credit agencies faced billions of dollars in fines as opposed to the $2.5 million imposed.[98]

The FTC also has acted against debt collectors under the FCRA for failing to comply with the act. For example, the FTC brought an action against a California debt collection agency, Performance Capital Management, for numerous violations of the FCRA.[99] According to the FTC's complaint, the company provided credit agencies with inaccurate information on delinquent debts that had placed in collection with the company.[100] Further, the debt collector failed to conduct fraud investigations when it received fraud reports from credit agencies or directly from consumers.[101] Ultimately, Performance Capital Management was required to pay to the FTC a $2 million civil penalty for its violations of the FCRA.[102]

In 2007, the FTC brought action against American United Mortgage Company for violating the FCRA and the GLB Financial Privacy and Safeguards Rules. According to the FTC, the company improperly disposed of consumer credit reports and other records containing the personal information of its customers and also failed to implement a documented information

[97] *Id*.

[98] *Id*.

[99] U.S. v. Performance Capital Mgmt., 2:01 civ. 1047, FTC File No. 982-3542 (C.D. Cal. Feb. 6, 2001).

[100] *Id*.

[101] *Id*.

[102] *Id*.

security program.[103] According to the FTC complaint, near the company's office "intact American United documents containing consumers' personal information were found on multiple occasions in and around a dumpster [that] was unsecured and easily accessible to the public."[104] In one instance, the credit reports and other personal information of twenty-six individuals were found intact in the company's dumpster.[105]

In March 2006, the FTC notified American Mortgage of its violations of the GLB Safeguards Rule and the FCRA Disposal Rule.[106] Despite the FTC notice, the company violated the rules on at least two more occasions by disposing of intact customer information in the same unsecured dumpster.[107] Further, the FTC alleged that the company violated the GLB Privacy Rule when it failed to provide its customers with privacy notices and the opportunity to opt out of having their information shared with third parties. The company apparently was in violation of the GLB Privacy Rule from July 1, 2001—the date the Privacy Rule went into effect—through March 2006.[108] Ultimately, American United was fined $50,000 for its violations of the FCRA.[109] Further, the court ordered the company to make regular reports to the FTC regarding

[103] U.S. v. Am. United Mortgage Co., No. 07C civ. 7064, FTC File No. 062-3103 (N.D. Ill. Dec. 18, 2007).

[104] *Id*.

[105] *Id*.

[106] *Id*.

[107] *Id*.

[108] *Id*.

[109] *Id*.

its compliance with the FCRA and GLB, as well as submit to compliance monitoring by the FTC.[110]

Enforcement of the federal ban on pretexting

In addition to policing the information security and protection practices of private businesses, the FTC also has brought actions against private businesses and individuals for pretexting.[111] When Congress passed the GLB Act, giving the FTC the authority to promulgate and enforce financial privacy and information security rules, it also banned pretexting and gave the FTC the authority to prosecute offenders of the ban.[112] Since the GLB Act took effect in 2001, the FTC has brought ten anti-pretexting actions, but none since 2004.[113]

In some instances, these pretexting actions have been brought against so-called "information brokers." In January of 2001, the FTC initiated "Operation Detect Pretext" in order to implement the federal ban on the practice of pretexting.[114] As part of the initiative, the agency screened Web sites and advertisements, identifying more than 200 businesses that "offered to obtain and sell asset or bank account information."[115] In 2002 the FTC brought three actions against individuals and businesses for such offers.

---

[110] *Id*.

[111] "Pretexters" use false pretenses, to solicit personal information from individuals or businesses, which they then sell to other people. *See* GLB Act, 15 U.S.C. § 6821 (2006).

[112] *Id*.

[113] Prior to the enactment of the GLB Act, the FTC brought at least one consumer protection action for pretexting, based on it Sec. 5 powers. *See* FTC v. Rapp, No. 99-WM civ. 783, FTC File No. 982-3542 (Dist. Colo. June 22, 2000).

[114] *See* FTC, Press Release, As Part of "Operation Detect Pretext" FTC Sues to Halt "Pretexting" (April 18, 2001), *available at* http://www.ftc.gov/opa/2001/04/pretext.shtm.

[115] *Id*.

For example, one of the individuals, Paula Garrett, allegedly "advertised over the World Wide Web that she [could] obtain asset information, including customer information from financial institutions, and make such information available to her clients for a fee."[116] According to the FTC complaint, Garrett obtained such asset information "using false pretenses, fraudulent statements, fraudulent or stolen documents or other misrepresentations, including posing as a customer of a financial institution, to induce [employees] of financial institutions . . . to disclose customer information."[117]

In November 2002, the FTC announced a multi-agency initiative called "Spam Harvest."[118] The anti-spam initiative targeted individuals that used deceptive email and online practices to trick individuals into disclosing their personal information.[119] According to the FTC, this initiative resulted in at least thirty criminal actions, three FTC actions and four additional FTC settlements.[120] One of the FTC actions was targeted at defendants who reportedly sent spam emails to individuals, claiming to be from various well-known financial institutions, such as Fannie Mae.[121] The spam emails solicited detailed personal information from consumers under a number of false pretenses. The FTC has also brought additional pretexting actions for spam-related online fraud.

---

[116] FTC v. Garrett, No. H-01 civ. 1255, FTC File No. 12-3067 (S.D. Tex March 8, 2002).

[117] *Id*.

[118] FTC, Press Release, Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams (Nov. 13, 2002), *available at* http://www.ftc.gov/opa/2002/11/netforce.shtm.

[119] *Id*.

[120] *Id*.

[121] *Id*.

For example, the FTC brought action in 2003 against the company 30 Minute Mortgage, Inc., as well its president and director, for pretexting and numerous violations of federal lending laws.[122] According to the complaint, the respondents solicited detailed information from consumers by advertising low interest rate mortgages in spam emails and on the company's Web site. The company falsely represented itself as a mortgage lender in order to induce consumers to fill out detailed loan applications.[123] The company then sold the applications to third parties without the consumers' consent.[124] As part of the final judgment, the company, its president and its director were permanently enjoined from sending spam emails of any kind, whether in connection with 30 Minute Mortgage or any other business.[125]

Also in 2003, the FTC filed an action against a minor, named in the complaint as C.J., for pretexting and other unfair and deceptive trade practices.[126] C.J. allegedly engaged in an online "phishing scam"[127] to solicit credit card information from individuals.[128] He then committed identity theft by using the fraudulently obtained information to make fraudulent purchases.[129] The FTC complaint does not indicate whether criminal charges were also brought against C.J.

[122] FTC v. 30 Minute Mortgage, Inc, 03 civ. 60021, FTC File No. 022-3224 (S.D. Fla. Nov. 26, 2003).

[123] *Id*.

[124] *Id*.

[125] *Id*.

[126] FTC v. C.J., 03 civ. 5275, FTC File No. 03-5275 (C.D. Cal. July 25, 2003).

[127] "Phishing" is a scam "by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly." Merriam-Webster Dictionary and Thesaurus (online edition), *phishing*, http://merriam-webster.com/ dictionary/phishing.

[128] C.J., 03 civ. 5275, FTC File No. 03-5275.

[129] *Id*.

However, the stipulated final judgment included a permanent injunction barring C.J. from sending any unsolicited commercial emails or engaging in any activities designed to solicit personal information.[130]

Similar to the C.J. case, in 2004 the FTC filed an enforcement action against an individual, Zachary Hill, for violations of federal law, including pretexting and other unfair and deceptive trade practices.[131] According to the FTC, Hill conducted an online "phishing scam" to obtain personal information and credit card numbers from individuals that he used to make fraudulent purchases.[132] The FTC worked jointly with the Department of Justice to prosecute Hill, who was also criminally charged under federal fraud statutes for his conduct.[133] Pending resolution of the criminal action, the FTC sought a preliminary injunction requiring that Hill cease the activities in question and shut down his online operations.[134] Subsequently, Hill pled guilty and was convicted by the U.S. District Court for the Southern District of Texas and sentenced to forty-six months in prison.[135]

In addition to the FTC enforcement actions, the commission has investigated at least twelve other companies, ultimately declining to take official action.[136] For example, in 2001 the

---

[130] *Id*.

[131] FTC v. Hill, No. H-03 civ. 5537, FTC File No. 032-3102 (S.D. Tex Dec. 18, 2003).

[132] *Id*.

[133] U.S. v. Hill, H-04 cr. 4-ALL (S.D. Tex. Feb. 9, 2004); s*ee also* FTC, Press Release, FTC Justice Dep't Halt Identity Theft Scam (March 22, 2004), *available at* http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm.

[134] *Id*.

[135] Hill, H-04 cr. 4-ALL.

[136] *See* FTC.gov, Privacy Initiatives, *supra* note 30. The FTC conducted investigations of the following businesses: NovaStar Financial, Inc. and NovaStar Mortgage Inc.; Monster Worldwide, Inc.; Dollar Tree Stores, Inc.; Longs

FTC investigated the online privacy practices of the major online retailer Amazon.[137] The investigation centered on whether the company tracked customer Web activity, collecting and maintaining personally identifiable consumer information contrary to its claim that any consumer information collected was anonymous.[138] According to the FTC, its investigation revealed that Amazon's practices were likely "deceptive" and in violation of Section 5 of the FTC Act.[139] Nevertheless, the FTC declined to enjoin or punish Amazon, largely because the Web tracking services in questions were no longer operational and there was no evidence that Amazon had sold or shared the information with any third party.[140]

Overall, the FTC has taken enforcement action fifty times since 1999 against private businesses and individuals for personal and information-privacy related offenses pursuant to the FTC Act, the GLB Act or the FCRA. The FTC's enforcement authority, however, does not extend to banks, credit unions, securities brokers, and other financial institutions or entities that fall within the specific jurisdiction of one of the federal financial regulatory agencies. These financial regulators have brought actions, similar to the FTC's, to enforce the information privacy and security standards that apply to the entities within their respective authority.

Drug Store Corp.; Rite Aid Corp.; Wal-Mart Stores, Inc.; Compaq Computer Corp. (Hewlett-Packard Co.); Earthlink, Inc.; Amazon.com and Alexa Internet; DoubleClick, Inc.; Yahoo! Inc. *Id*.

[137] *Id*.

[138] *Id*.

[139] *Id*.

[140] *Id*.

According to the ID Theft Taskforce, several federal financial regulatory agencies have taken formal actions to enforce personal information safeguards.[141] From January 1, 2002 to December 31, 2006, the Federal Deposit Insurance Corporation took actions against seventeen different financial institutions within its control.[142] During the same time period, the Federal Reserve Board took formal enforcement actions against fourteen companies, the Office of the Comptroller of the Currency took eighteen formal actions, and the Office of Thrift Supervision took eight formal actions.[143] On the other hand, the Securities and Exchange Commission has not taken any formal actions against securities brokers and entities within its jurisdiction, opting to resolve potential disputes through informal procedures such as counseling, advising and working with entities to correct possible violations.[144]

A number of federal agencies are responsible for enforcing federal identity theft rules, regulations and laws. Essentially, each of these agencies has different procedures for enforcing the laws within their jurisdiction and, likewise, imposes different penalties or remedial measures against offenders. Law enforcement agencies investigate identity theft crimes in conjunction with the federal prosecutors that bring criminal actions against identity thieves. Convicted identity thieves face varying criminal penalties, including prison sentences and monetary penalties in the form of financial restitution to victims. Federal identity theft crimes are prosecuted in federal district court. Even if a defendant signs a plea agreement, rather than

[141] PRESIDENT'S IDENTITY THEFT TASKFORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, vol. II supp. at 12 (2007), *available at* http://www.idtheft.gov/reports/VolumeII.pdf (last visited March 10, 2009).

[142] *Id*.

[143] *Id*.

[144] *Id*. at 13.

opting for a federal jury trial, the agreement must be accepted and the sentence must be imposed by a federal district court.

On the other hand, administrative enforcement actions are not always brought in federal district court. Administrative agencies may take action against businesses and individuals for violations of federal information privacy rules and regulations. In the context of administrative enforcement, agencies may take more informal or less punitive action against violators such as the execution consent agreements where violators agree to stipulated terms that define the specific actions they will take to remedy their violating conduct. Agencies may also issue formal complaints against violators and adjudicate those complaints before an administrative law judge. Often such administrative actions are resolved when a final order is issued declaring the conduct in question unlawful and requiring the respondent to cease-and-desist from engaging in the unlawful conduct. Additionally, in many instances agencies may institute enforcement proceedings against violators in federal district court, seeking injunctive and monetary relief. The monetary and equitable relief available in administrative enforcement actions depends on the statutory or regulatory authority under which the action is brought.

Civil fines may be levied against violators in some enforcement actions, such as those brought pursuant to the Fair Credit Reporting Act (FCRA) or the Health Insurance Portability and Accountability Act (HIPAA). On the other hand, civil fines may not be available in other enforcement actions, such as those brought for initial violations of the Gramm-Leach-Bliley Act or the Federal Trade Commission Act. Other remedies available in most administrative enforcement actions may include preliminary and permanent injunctive relief or monetary awards in the form of equitable relief intended to redress consumer harm or require violators "disgorge" profits from the fruit of their crimes. The threat of civil fines generally poses a

greater financial risk to businesses and individuals than do other forms of relief that are equitable or remedial in nature. Thus, enforcement proceeding brought pursuant to the FCRA or HIPPA are more likely to deter businesses from engaging in activities that threaten the financial privacy of consumers.

CHAPTER 5
PROPOSED IDENTITY THEFT PROTECTIONS

The potential for the misuse of personal information has no doubt risen with increased electronic information sharing and the use of electronic means of conducting financial transactions. Congress, for its part, has attempted to legislatively address the problem of identity theft. It has enacted several laws over the past ten years that are aimed, at least partially, at mitigating the threat of identity theft. Between 1998 and 2008, 200 identity theft-related bills were introduced in Congress.[1] These figures are based upon a search of the Library of Congress database, which provides public access to federal legislation that is freely available to and easily searchable.

This Chapter analyzes the text of identity theft-related bills introduced during the current 111th Congress and the previous 110th Congress. Since the 110th Congress began in 2007, Congress has considered numerous and varied identity theft bills. However, the only legislation passed was the Identity Theft Enforcement and Restitution Act of 2008, which increased criminal penalties for identity theft crimes. Based on the congressional attention given to the issues of identity theft and personal information privacy, it is likely that Congress will ultimately pass new identity theft legislation. Further, it is likely that any new legislation will contain provisions similar to those of bills that are either currently pending or have previously been introduced in Congress.

[1] These results are based on a search of the Library of Congress THOMAS database. Library of Congress, THOMAS, Advanced Bill Summary & Status Search, http://thomas.loc.gov/bss/ (last visited March 10, 2009). The totals were based on a the results of search for the terms "identity theft" or "identity fraud" in the bill summary and status of all bills introduced during the 105th—110th Congress. One bill from the 105th Congress was not counted because it was introduced during the 1997 Session. These totals do not include amendments to bills or resolutions.

111th Congress: Current Legislative Proposals

The current 111th Congress began on January 6, 2009. Between January 6 and February 20, 2009, eight identity theft-related bills have been introduced in Congress—one bill in the Senate and seven in the House.[2] These bills have some common themes. Several bills would impose additional reporting requirements on public and private entities. Others would restrict the use of Social Security numbers (SSN) by public agencies and private businesses. A few of the bills would require agencies or businesses to notify a consumer when it suspects fraud involving that consumer's identity.

The first identity theft-related bill of the 111th Congress was introduced in the House on January 6, 2009, the first day of the new session.[3] This bill, the Social Security Identity Theft Prevention Act, would require the use of specific security features in Social Security cards.[4] For instance, the Act would require Social Security cards, which are currently made of paper, be constructed with some kind of "tamper-proof" material.[5] Additionally, the Act would require all cards to have a "digital image of the cardholder as well as an encrypted, machine-readable electronic record containing biometric identifiers.[6]

[2] This number is based on a search of the Library of Congress THOMAS database for the term "identity theft" in the bill summary and status of any bills introduced since the start of the 111th Congress. Library of Congress, THOMAS Advanced Bill Summary & Status Search, http://thomas.loc.gov/bss/ (last visited March 10, 2009).

[3] *Id*.

[4] *Id*.

[5] *Id*.

[6] *Id*.

Another bill, the Protecting the Privacy of Social Security Numbers Act of 2009 was introduced in the House on January 6, 2009 and is now awaiting committee action.[7] An identical bill was also introduced in the Senate on January 6, 2009.[8] The Act would prohibit any commercial entity from requiring individuals to provide their SSNs in order to receive goods or services from that entity.[9] The Act would establish criminal and civil penalties for violations of the act, and would provide for federal injunctive authority over any public entity that violates the act.[10] Subject to certain exceptions, the bills would prohibit the "display, sale, or purchase of SSNs" unless the individual to whom the SSN belongs affirmatively consents.[11] Overall, the Protecting the Privacy of Social Security Numbers Act aims to give individuals more control over how their SSNs are used.

The Identity Theft Prevention Act, introduced in the House on Jan. 6, 2009, would also restrict the use of SSNs as identifiers.[12] However, the act's restrictions apply to government entities, not private businesses.[13] The Act would amend the Social Security Act,[14] removing provisions that allow state and federal agencies to use SSNs as identifiers and that require the

[7] *Id*.

[8] S. 141, 111th Cong. (2009).

[9] H.R. 122; S. 141.

[10] H.R. 122; S. 141.

[11] H.R. 122; S. 141.

[12] H.R. 220, 111th Cong. (2009).

[13] *Id*.

[14] *Id*.

disclosure of SSNs from individuals seeking public services.[15] The Act would also stipulate that an individual's SSN is "the exclusive property of such individual."[16] Further, it would prohibit the Social Security Administration from divulging individual's SSNs to any federal or state agency except as necessary under the Internal Revenue Code, and bar the establishment of any uniform system of identification to replace the SSN.[17] Essentially, the Identity Theft Prevention Act of 2009 would reduce the vulnerability of SSNs by eliminating the governments' ability to use them to establish individuals' identity.

At least three of the 2009 identity theft-related bills introduced in Congress would require certain entities to report suspected instances of identity theft or SSN misuse. The Credit Agencies Identity Theft Responsibilities Act of 2009 would impose reporting requirements of credit agencies.[18] Not only would the Act require credit agencies to report any suspected identity thefts to the Secret Service, but it would also require such agencies to regularly review consumer reports to look for signs of identity theft.[19]

The Identity Theft Notification Act of 2009 would require the Commissioner of Social Security to report suspected fraud to federal law enforcement officials and to individuals when there is evidence that a SSN has been fraudulently used to obtain employment.[20] First, the Act would require an employer to report employee address information and SSN on any employee

[15] *Id*.

[16] *Id*.

[17] *Id*.

[18] H.R. 123, 111th Cong. (2009).

[19] *Id*.

[20] H.R. 133, 111th Cong. (2009).

wage reports it submits to the Commissioner.[21] The Commissioner would then be required to investigate instances of suspected employment fraud—those where the same SSN has been used on eight or more wage reports or been associated with four or more addresses during a one-year period.[22] If the Commissioner suspects that the SSN was used by someone other than the individual to whom it belongs, the Commissioner would be required to report such use to law enforcement and to the individual to whom the SSN belongs.[23] Ultimately, this bill seems to target identity fraud with respect to illegal immigration and undocumented workers, not financial identity theft.

Taking a different approach than that of any of the other 2009 bills, the Cybersecurity Education Enhancement Act of 2009 would target cyber crimes, such as online identity fraud, through public education.[24] The Act would establish a grant program to help fund the establishment of cybersecurity degree programs at institutions of higher education.[25] It would also establish a fellowship program to encourage workers from state government and private industry to work with the National Cybersecurity Division of the Department of Homeland Security.[26] Overall, this Act does not specifically address identity theft; rather, it seeks to improve current security efforts with respect to the Internet and new technologies.

---

[21] *Id*.

[22] *Id*.

[23] *Id*.

[24] H.R. 266, 111th Cong. (2009).

[25] *Id*.

[26] *Id*..

In sum, since January of 2009 several legislative proposals to identity theft have been introduced in Congress. These bills have provided for a range of solutions to identity theft, from restricting information sharing to imposing investigative and reporting duties on private industry. Many of the legislative themes in the current session of Congress are similar to bills that passed one but not both bodies of Congress during the 2007-2008 session of Congress.

110th Congress: Previous Legislative Attempts

During the previous session of Congress,[27] nearly sixty identity theft-related bills were introduced in the House and Senate.[28] Of those bills, seven passed the House only,[29] one passed the Senate only,[30] and one was passed by both houses. As previously discussed, the Identity Theft Enforcement and Restitution Act of 2008, which established criminal restitution orders for federal identity theft convictions, was signed into law on September 26, 2008.[31] Of the legislation that failed to pass, some bills approached the identity theft problem by focusing on the security of SSNs, others focused on the Internet as a source of identity theft, and others still would have implemented reporting or notification requirements.

The Internet Spyware Prevention Act of 2007 (I-SPY Act) was passed by the House on May 22, 2007 and referred to the Senate Judiciary Committee on May 23 where it remained until

[27] The 110th United States Congress began on January 4, 2007 and ended on January 3, 2009.

[28] This number is based on a search of the Library of Congress THOMAS database for the term "identity theft" in the bill summary and status of any bills introduced since the start of the 111th Congress. Library of Congress, THOMAS, *supra* note 28.

[29] H.R. 1525, 110th Cong. (2007); H.R. 1684,110th Cong. (2007); H.R. 5719, 110th Cong. (2008); H.R. 1677,110th Cong. (2007).

[30] S. 2168, 110th Cong. (2007).

[31] Pub. L. No. 110-326, §§ 201-09, 122 Stat. 3560, tit. II (2008) (2008) (codified in scattered sections of 18 U.S.C. (2006)).

it expired when the 110th Congress adjourned.[32] The I-SPY Act would have imposed criminal penalties for anyone who intentionally accesses a protected computer without valid authorization and increased criminal penalties for the intent to steal personal information for fraudulent purposes.[33] Additionally, the House appropriations bill for the Department of Homeland Security would have set aside $300 million in grants over the next three years for state projects aimed at reducing identity theft and document fraud by developing more secure identification documents.[34] However, the grant program did not make it into the final appropriations bill.[35]

The Taxpayer Protection Act of 2007, passed by the House on April 17, 2007, would have required the Secretary of the Treasury to notify taxpayers when their identities are suspected of being stolen and to inform taxpayers if someone has been charged for fraudulently using their identity.[36] On April 15, 2008, the House passed the Taxpayer Assistance and Simplification Act of 2008, which contained an identity theft notification provision nearly identical to the Taxpayer Protection Act of 2007.[37] Both of these bills were received in the Senate and referred to the Senate Committee on Finance but received no further action before expiring at the end of the 110th Congress.[38]

---

[32] H.R. 1525, 110th Cong (2007).

[33] *Id*.

[34] H.R. 1684,110th Cong. (2007).

[35] Pub. L. No. 110-161, 121 Stat. 2169 (2007).

[36] H.R. 1677, 110th Cong. (2007).

[37] H.R. 5719, 110th Cong. (2008).

[38] H.R. 1677; H.R. 5719.

On December 4, 2007, the Senate passed the Identity Theft Enforcement and Restitution Act of 2007.[39] This 2007 Act contained many of the same provisions as the Identity Theft Enforcement and Restitution Act of 2008 that became law in September 2008. In order facilitate federal identity theft prosecutions, the 2007 Act would have, among other things, expanded the definitions of identity theft, computer fraud and cyber-extortion.[40] However, the 2007 Act contained some notable provisions that were ultimately left out of the final 2008 act. The 2007 Act would have required companies to notify the FTC of any security breach of personally identifiable information if that breach may have reasonably resulted in identity theft and to notify all consumer reporting agencies if the breach had affected more than 1,000 consumers.[41] Notably, this bill would also have, subject to certain exceptions, prohibited all businesses from soliciting an individual's SSN unless it was necessary for business purposes and no alternative identifier would suffice.[42] Ultimately, the provisions of the Act that would have implemented additional regulations on private business were taken out. However, the bill was referred to the House where it remained until its expiration at the end of the 110th Congress.

On June 3, 2008, the Federal Agency Data Protection Act was passed by the House.[43] The Act would have required the Director of the Office of Management and Budget (OMB) to assess federal agency information security practices and develop minimum information security

[39] S. 2168, 110th Cong. (2007).

[40] *Id*.

[41] *Id*.

[42] *Id*.

[43] H.R. 4791, 110th Cong. (2007).

standards for federal agencies.[44] The OMB Director would have been required to regularly report federal data breaches to Congress.[45] Notably, the Act also would have required the director to develop standard procedures for federal agencies to follow in the event of data breaches—including breach notification rules.[46] The bill was received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs but received no further action.

On September 29, 2008, the House passed the Medicare Identity Theft Prevention Act.[47] It would have required the Secretary of Health and Human Services to "establish cost-effective procedures to ensure that Social Security account numbers are not included on Medicare cards."[48] This Act was the last identity theft-related act passed by the House during 110th Congress.

In addition to the bills passed by either the House or Senate in 2007 and 2008, six more were awaiting floor action in either the Senate or the House when Congress adjourned. Three of the bills, which had been placed on the calendar of either the House or Senate in 2007, would have required breach notification, among other things.[49] One calendared bill, the Personal Data

[44] *Id*.

[45] *Id*.

[46] *Id*.

[47] H.R. 6600, 110th Cong. (2008).

[48] *Id*.

[49] H.R. 3046, 110th Cong. (2007); S.239, 110th Cong. (2007); S. 1178, 110th Cong. (2007).

Privacy and Security Act of 2007 (PDPS Act), was perhaps the most comprehensive identity theft bill to emerge in Congress during the 2007-2008 session.[50]

Among other things, the PDPS Act would have increased criminal identity theft penalties, enhanced consumer protections and imposed additional regulations upon public agencies. The Act would have enhanced identity theft punishment in two significant ways. First, the PDPS Act would have criminalized the intentional and willful concealment of data breaches that involve "sensitive personally identifiable information" (SPII).[51] Second, it would have amended racketeering[52] laws to include the crime of accessing a computer without authorization.[53] Public agencies would also have been required to evaluate the information security practices of all data brokers to which they award contracts.[54]

Moreover, the PDPS Act would have imposed information security standards on all businesses that maintain SPII in their records,[55] as well as regulations on data brokers similar to those found in the FCRA.[56] A data broker would have been required to notify individuals when

[50] S. 495, 110th Cong. (2007).

[51] "Sensitive personally identifiable information" includes "an individual's name in combination with his or her social security number, home address, date of birth, biometrics data, or financial account information." S. 495.

[52] "Racketeering activity" means "any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical," which is punishable by more than one-year imprisonment under state law or illegal under a federal racketeering statute. 18 U.S.C. § 1961 (2006).

[53] *Id*.

[54] *Id*.

[55] This provision is similar to the GLB Act's Safeguard Rule. *See supra* Chapter Three, pp. 57-60. According to the PDPS Act's committee report, this provision is especially important because since 2005 public and private entities have reported more than 500 data security breaches, which have compromised more that 154 million records. S. Rep. 110-70, 110th Congress (2007).

[56] S. 495, 110th Cong. (2007); *see also, supra* Chapter Three, pp. 51-70 (discussing the FCRA's regulation of the credit industry, including its identity the protections).

that broker's records lead a third party to take any adverse action against the individual, and allow individuals, upon request, to view all of their personal information held by the broker and correct any inaccuracies.[57] The PDPS Act would also have imposed civil penalties upon data brokers and private businesses for violations of the law, and preempted any state laws that regulate data brokers.[58] Furthermore, it would have required all companies to provide breach notification to any individual whose SPII has been compromised.[59]

Senator Patrick Leahy, Chairman of the Senate Judiciary Committee,[60] and Senator Arlen Specter, ranking member of the Judiciary Committee,[61] introduced the bill in February 2007. It was co-sponsored by three other members of the Senate Judiciary Committee[62] and three other Senators who are not members of the Judiciary Committee.[63] The Act was first introduced by Senators Leahy and Specter, during the prior, 109th Congress, as the Personal Data Privacy and Security Act of 2005.[64] However, the 2005 bill, which was placed on the legislative calendar,

[57] S. 495.

[58] *Id*.

[59] *Id*.

[60] *Id*.

[61] *Id*.

[62] *Id*. All Judiciary Committee co-sponsors, other than republican Senator Arlen Specter from Pennsylvania, are democrats: Senators Charles Schumer of New York, Russ Feingold of Wisconsin, and Benjamin Cardin of Maryland. *Id*.

[63] *Id*. Additionally, two of the other co-sponsors were Democrats—Senator Sherrod Brown of Ohio and former Senator Barrack Obama from Illinois—and the third was an Independent who caucuses with Democrats—Senator Bernard Sanders of Vermont. *Id*.

[64] S. 1789.109th Congress (2005). The differences between the 2005 and 2007 bills are the five amendments approved, out of six proposed, to the 2007 bill.

was never debated or voted on by the full Senate so it expired at the end of the 109th Congress.[65] Similarly, the 2007 PDPS Act expired with the end of the 110th Congress.[66]

The comprehensive PDPS Act had its share of detractors.[67] A major point of contention[68] appeared to be the mandatory breach notification provision. A less stringent provision, such as one that gives the FTC discretion to mandate breach notification or only requires notification if the breach is expected to result in identity theft, may have garnered more support.

Based on the content and status of current and previous identity theft legislative proposals, there is no clear indication that Congress is close to passing any comprehensive identity theft legislation. There does seem to be some congressional will to pass legislation dealing with the vulnerability of SSNs and their deficiencies as a means of identification. Given that several pending and previous bills would strengthen SSNs protections, Congress may implement

---

[65] S. 495.

[66] S. 495.

[67] It also appears to lack the requisite political momentum: in 2007, the PDPS Act for the second time failed to garner the necessary consent to be brought before the Senate for consideration, and it still awaiting debate in the Senate. 153 Cong. Rec. S14276 (daily ed. Nov. 13, 2007) (remarks of Sen. Leahy) ("I urge whoever is holding up this bipartisan bill to stop delaying this measure so that the Senate can promptly pass this important and much needed privacy bill before the Thanksgiving recess."); *see also* 153 Cong. Rec. S12938-9 (daily ed. Oct. 16, 2007) (remarks of Sen. Leahy) ("The Judiciary Committee has twice favorably reported the Leahy-Specter Personal Data Privacy and Security Act, most recently in May 2007, and that important privacye bill is now awaiting consideration by the full Senate . . . . and I sincerely hope that the Senate will fulfill its obligation to bring meaningful privacy protections to the American people."); 153 Cong. Rec. S379 (daily ed. Jan. 10, 2007) (remarks of Sen Leahy) ("In November 2005, the Judiciary Committee approved the Personal Data Privacy and Security Act . . . Unfortunately, the Senate took no further action and the bill expired at the end of the 109th Congress."); 153 Cong. Rec. S7086 (July 22, 2008) (remarks of Sen. Leahy) ("We have reported legislation to protect Americans' data privacy like my Personal Data Privacy and Security Act . . . I look forward to a time when Republicans work with us on these matters instead of obstructing us at every turn . . . Legislation with broad bipartisan support that I have managed to move through the Judiciary Committee has then been stalled on the Senate floor by the obstruction of a few Republicans.").

[68] An additional point of contention includes the amendment to the bankruptcy law, which one Senator argued should be a measure drafted and debated by the Senate Banking Committee, not the Judiciary Committee. S. Rep. 110-70 (2007).

increased safeguards for the sharing of SSNs. On the other hand, there doesn't seem to be much political will behind efforts to implement mandatory breach notification requirements on private entities. With the current economic crisis in the United States, congressional attention of late has been primarily focused on improving economic conditions and jumpstarting the stalled consumer credit market in the United States. Thus, other legislative issues, such as identity theft may not get as much attention during the current session of Congress as they have in the past.

CHAPTER SIX
CONCLUSION AND ANALYSIS

This thesis is intended to comprehensively analyze the federal framework of identity theft regulation. To that end, this thesis has examined the current laws that address identity theft—some of them are criminal laws and others are information privacy laws—as well as how these laws are enforced. Additionally, this thesis examined recently proposed identity theft legislation in order to identify how Congress might address some of the current weaknesses in federal identity theft protections.

In comprehensively analyzing the federal framework of identity theft protection, this thesis posed the following four research questions: **(RQ1)** What are the federal laws or regulations that address the prevention of financial identity theft and how are these laws enforced? **(RQ2)** To what extent do these laws address the identity theft problems identified in the literature review? **(RQ3)** What identity theft legislation might Congress adopt in the near future? **(RQ4)** What kinds of laws may address the problems identified in the literature review? This Chapter will explain how these questions were addressed in this thesis and conclude by suggesting some ways the federal government may improve current identity theft protections and develop solutions for a long-term approach to adequately and effectively combat identity theft.

Research Question 1: Current Federal Laws and Regulations

In Chapter 3, this thesis identified two kinds of federal identity theft protections—criminal statutes and information privacy rules and regulations. Since 1998, Congress has passed three new criminal laws addressing identity theft.[1] These criminal identity theft laws are used to

[1] *See supra* Chapter Three, pp. 49-51.

prosecute identity thieves, often in conjunction with other fraud statutes. These laws are intended to mitigate identity theft by deterring potential identity thieves with threats of criminal punishment. In addition to criminal laws, several distinct federal information privacy laws provide varying degrees of protection for personally identifying information, depending upon the source of the information.[2]

Many of these information privacy laws approach the problem of identity theft by focusing on the sources of personal information which are potentially available to identity thieves. Such laws may attempt to mitigate identity theft by restricting the availability and sharing of personal information among businesses or by imposing duties upon record holders to protect personal information. Additionally, some information privacy laws may focus on consumer protection by giving individuals specific rights to mitigate the harm which results from identity theft.

Criminal Laws. In 1998, Congress first specifically addressed identity theft as a distinct form of criminal fraud through its enactment of the Identity Theft Assumption and Deterrence Act.[3] Dissatisfied with the limitations on the scope and punishment available in identity theft prosecutions, Congress twice amended criminal identity theft laws in order to increase penalties and widen the scope of prosecutions for identity theft crimes.[4] Currently, there are two classes of identity theft crimes, the lesser offense of identity theft and the greater offense of aggravated identity theft. Identity theft occurs when a criminal "knowingly transfers or uses" another individual's "means of identification" in order to commit fraud or other federal crimes or state

[2] *See supra* Chapter Three, pp. 51-70.

[3] Identity Theft Assumption and Deterrence Act of 1998, Pub. L. No, 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C. § 1028 (2006)).

[4] *See supra* Chapter Three, pp. 48-50.

felony crimes. Aggravated identity theft occurs when the fraudulent identity is used in connection with more serious crimes, such as felonies involving the theft of public monies, bank or wire fraud, and immigration fraud.

Information privacy laws. Numerous federal information privacy laws also protect consumers and their personal information from identity theft. However, there is no universal information privacy law or regulation that acts to protect the privacy of the personal information held by all public and private entities.[5] Rather, information privacy laws impose different requirements for the protection of personal information or different restrictions on the sharing of personal information depending on the source of that information. Some of these laws, such as the Fair Credit Reporting Act (FCRA), have recently been amended to protect the privacy of personal information in response to growing concerns over identity theft.

Other information privacy laws were enacted to address different concerns but nonetheless affect identity theft regulation and protection. For example, the Customer Identification Program requiring financial institutions to implement institutional standards for verifying the identity of new customers was implemented by the USA Patriot Act.[6] The primary purpose of the program is to inhibit terrorist financing and money laundering but its identity verification requirements potentially hinder identity theft as well.[7] Additional non identity-theft specific privacy laws impose different regulations on varying public or private record keepers such as federal agencies, educational institutions, credit reporting companies, medical providers and financial institutions.

[5] *See supra* Chapter Three, notes 14-17 and accompanying text.

[6] USA PATRIOT Act, Pub. L. No. 107-56, § 326, 115 Stat. 272 (2001).

[7] *Id*.

Public record keepers. Public entities are treated separately from private entities for the most part under U.S. information privacy laws.[8] Within the context of public entities, federal privacy laws also may distinguish between state and federal agencies. State departments of motor vehicles are restricted, under the Driver's Privacy Protection Act (DPPA), from sharing the personal information contained in driving records, subject to specific exceptions.[9] The collection and use of personal information by agencies within the federal government is generally controlled by the Privacy Act of 1974, which limits the ways that federal agencies may collect and share individuals' personal information.[10] Generally, these agencies may only collect personal information that is "necessary and relevant" to the agency's purpose and may not, subject to specific exceptions, share this information without the consent of the individual to whom it pertains. The Privacy Act also limits the ability of both federal and state agencies to require individuals to disclose their Social Security number (SSN) in connection with applying for public services. However, there are so many exceptions to this restriction that it has done little to curb the widespread availability of SSNs in state and government records as the proliferation of information technology has led to the prevalence of electronic government databases.

SSNs and other personal information are permissibly collected and stored by numerous federal and state agencies and may thus be found in myriad individual records and databases maintained by these agencies. This raises serious information security concerns that the federal

[8] *See supra* Chapter Three, pp. 70-72.

[9] 18 U.S.C. §§ 2721-2725 (2006); *see also, supra* Chapter Three, notes 115-118 and accompanying text.

[10] 5 U.S.C.§552a (2006).

government has attempted to address in part by enacting the E-Government Act of 2002, which imposes information security standards on federal agencies.[11] However, these standards are not strictly defined and their implementation is largely left to the discretion of individual agencies. Under the E-Government Act, agencies are directed to "develop, document, and implement agency-wide programs" for the security of the information and information systems particular to those individual agencies.[12] Within the federal government there is no universal information system, and within each federal agency multiple, unique information networks and databases may exist. On the one hand, this may be good for individual privacy because in practice it limits the sharing or compilation of personal information held by federal agencies. On the other hand, it makes developing standardized comprehensive information security practices difficult. Further, agency compliance is not overseen by any central authority but is self monitored and self reported. In addition, individuals may bring civil actions for violations of the Privacy Act.

Private record keepers. Private entities are generally subject to the oversight of one or more federal agencies within the federal government. However, there is no universal enforcement authority or law that controls the information privacy practices of private record keepers. There are multiple information privacy laws in the federal government, many that were not germane to the research questions posed in this research. The information privacy laws discussed in this thesis are those that play a role in either restricting the sources of personal information or mitigating the harm identity theft victims face. The financial and credit industries—and therefore financial records and credit reports—are subject to specific

[11] Pub. L. No. 107-347, 116 Stat. 2949 (2002) (codified in scattered sections on 44 U.S.C.A. (West 2008)); *see also, supra* Chapter Three, notes 155-163 and accompanying text.

[12] § 301, 116 Stat. 2949 at 3544.

information privacy laws. The healthcare industry is subject to the privacy regulations that apply to the personal information contained in medical and health insurance records. Other information privacy laws protect the privacy of the personal information contained in driving records and education records by restricting the disclosure of these records, subject to several exceptions, without the consent of the individuals to whom the records pertain. Another source of information privacy protection is found within the federal ban against all "unfair and deceptive" business practices. The scope of this ban extends to bar information privacy practices that are egregious enough to be considered "unfair or deceptive."

Some of the federal information privacy protections are somewhat limited in scope, such as the Family Educational Rights and Privacy Act which applies only to schools that receive funding from the U.S. Department of Education. Other laws apply to a somewhat broad spectrum of entities, such as the general ban on all "unfair and deceptive" business practices. The FCRA, which is possibly the most comprehensive federal identity theft regulation, sets standards for information privacy and consumer protection within the consumer credit industry. The Act contains provisions that restrict the ways that any credit reporting company may disclose consumer credit reports, as well as the ways that any creditor or lender may report consumer credit information. While the credit industry in general encompasses a rather large class of businesses—including credit reporting agencies, lenders, creditors, and debt collectors—the types of entities that use the information the credit industry generates is even wider—e.g., employers, landlords, government agencies, lenders and auto dealers.

The FCRA and other information privacy laws are generally overseen by specific federal agencies, such as the Federal Trade Commission (FTC), which may take enforcement actions against violators. Enforcement actions may include administrative proceedings against violators

that ultimately impose regular reporting requirements, order that specific violating conduct cease and desist, or stipulate the specific steps a violator agrees to take to rectify its conduct. At other times, enforcement proceedings may take the form of civil actions filed by the enforcing agency that seek temporary or permanent injunctive relief, civil penalties, or other equitable remedies.

Research Question 2: Effectiveness of Current Federal Identity Theft Protections

In the literature review, several issues surrounding identity theft regulations were identified: (1) an inadequate understanding of the contours of identity theft, (2) the widespread use and availability of SSNs and other personally identifiable information in public and private records, (3) vulnerabilities in information security, (4) a lack of individual control over personal information, and (5) fragmented federal privacy protections that have led to both inconsistent protection for individuals and inconsistent accountability of record holders. These issues illustrate the challenges inherent in designing a framework for effectively mitigating identity theft. As discussed below the current federal framework inadequately addresses the problems associated with identity theft.

Inadequate Understanding of the Contours of Identity Theft

Identity theft costs businesses billions of dollars every year and costs consumers the considerable time and money it takes to resolve the financial harm caused by identity theft.[13] According to the most recent annual identity theft survey, nearly 10 million Americans were victims of identity theft in 2009.[14] Current estimates put the total amount of identity theft fraud

[13] FEDERAL BUREAU OF INVESTIGATION (FBI), FINANCIAL CRIMES REPORT TO THE PUBLIC FISCAL YEAR 2006 (Oct. 1 2005 – Sept. 30, 2006), at http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm#Identity.

[14] JAVELIN STRATEGY AND RESEARCH , 2009 IDENTITY FRAUD SURVEY REPORT 15 (Consumer Version) (Feb. 2009), *available at* http://www.javelinstrategy.com/ research/2.

in 2008 at around $48 billion, an average of nearly $500 per instance of identity theft.[15] Unfortunately, these numbers may not accurately represent the problem.

All of the most comprehensive research studies on identity theft have measured the crime by conducting surveys of randomly selected individuals. The data obtained is based solely on the responses of these individuals. Those who indicate that they have been victims of identity theft are asked a series of questions regarding the source of the stolen information and the cost of the theft. The data are not corroborated by comparing the results with other sources of identity theft information, such as consumer information from the Identity Theft Clearinghouse or law enforcement data.

The FTC conducted the first comprehensive annual identity theft survey in 2003. Since then, the FTC conducted a similar survey in 2006 and Javelin Strategy and Research (Javelin), a privately-funded research company, has conducted its own annual identity theft surveys using a methodology similar to the FTC's. However, these series of identity theft surveys do not provide a conclusive picture of overall trends in the costs, incidences, or characteristics of identity theft. The FTC survey methodology was changed between its 2003 and 2006 surveys, limiting the comparability of its two studies. Further, the identity theft survey reports produced by Javelin have been criticized as having a perceived bias towards the financial industry, where some of the funding for its surveys originates.[16]

Javelin has downplayed the role of data breaches in identity theft crimes, pointing to less technologically-savvy means of identity theft, such as wallet and purse theft, as the most likely

[15] *Id*.

[16] *See supra*, Chapter Two, notes 18-24 and accompanying text.

source of stolen information. However, the company doesn't make a very convincing argument because its conclusions are based only on the responses of the 35% of survey respondents who reported having knowledge about how their information was stolen. What Javelin fails to mention is that it is conceivable that data breaches were involved in many of the remaining 65% of identity thefts in which respondents did not know how their personal information was stolen. Consumers are not notified every time a data breach occurs.[17] So, in many instances consumers may have no way of knowing how their personal information was compromised until they discover the actual identity theft. Additionally, Javelin does not make its entire survey results public. So, scholars and others cannot view all of the data collected or scrutinize the analysis and findings presented. The company releases an annual "Consumer Version" with selected findings. The full survey report is available only by purchasing the entire report for $3,000. Further, it is unclear whether the "Full Report" includes the full data set or merely a more in-depth analysis and explanation of Javelin's findings. The company's Web site describes the "Full Version" as a "detailed, comprehensive analysis of identity fraud."[18]

The sources of stolen personal information include wallet and purse theft, mail theft, dumpster diving, hacking, employee theft and data breaches. However, which of these sources are most common in identity theft is unknown. Although the true extent to which data breaches contribute to identity theft is unknown, it is certain that data breaches are the cause of at least

[17] However, at least 43 states have passed laws requiring breach notification in certain instances. *See* Fred H. Cate, Centre for Information Policy Leadership, *Information Security Breaches* 3 (2008), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf (last visited March 10, 2009).

[18] Javelin Strategy and Research , Preview of 2009 Identity Fraud Survey Report "Full Report", http://www.javelinstrategy.com/uploads/901.R_IdentityFraudSurveyBrochure.pdf (last visited March 10, 2009).

some identity thefts. For example, in a 2006 breach of data broker ChoicePoint's information security, the personal information of up to 163,000 individuals was compromised, which resulted in at least 800 cases of identity theft.[19] While there is no concrete evidence of just how much information security or data breaches are to blame, the potential for misuse of this information is great.[20]

Accurately analyzing identity theft trends is difficult with no central reporting system. As the President's Identity Theft Taskforce (ID Theft Taskforce) reported, "identity theft data currently reside in numerous databases [and] there is no standard reporting form for all identity theft complaints."[21] The primary source of information about consumer identity theft complaints is the FTC's Identity Theft Clearinghouse.[22] However, while consumers may report identity thefts to the FTC's database, they are not required to file consumer complaints. Neither, unfortunately, are financial institutions and other private entities required to report data from internal identity theft investigations. Financial institutions, especially, are essentially on the frontlines with respect to identity theft and in the best position to identify emerging trends in identity theft crimes.[23] Without a clear reporting mechanism, the identity theft information

[19] *See* Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/ choicepoint.shtm.

[20] *See infra* Chapter Six, notes 29-31 and accompanying text (discussing the increasing number of breaches since 2005).

[21] PRESIDENT'S IDENTITY THEFT TASKFORCE, TASKFORCE REPORT 63 (2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf (last visited March 10, 2009).

[22] *Id*. at 64.

[23] *Id*.

collected is incomplete and difficult to analyze in a way that lends itself to generalizations about the overall contours of the crime.

Widespread Use and Availability of Social Security Numbers

"Consumer information is the currency of identity theft," according to the ID Theft Taskforce, and "perhaps the most valuable piece of information for the thief is the SSN."[24] The continued use of SSNs as the primary way both individuals and their records are identified greatly exacerbates the risk of identity theft.[25] Public and private record holders frequently use SSNs to authenticate individuals' identity and to link individuals with their particular records, which means SSNs are stored along with other personally identifying information in numerous and varied locations. In the private sector, many businesses verify new customers' identities by requiring them to disclose their SSNs. Simultaneously, these same businesses also use SSNs to connect individuals with their records. For example, the ID Theft Taskforce reported that SSNs are the critical component used to establish consumer identities in the financial sector where they also serve as "unique and permanent identifiers [linking] consumers to their records."[26] Similarly, federal and state agencies often use SSNs to identity records and require individuals to provide their SSNs as a prerequisite to receiving public services or benefits. Due in large part to the practice of collecting SSNs and using them to identity individual records, there are now myriad electronic sources from which an identity thief may obtain an individual's SSN.

[24] *Id*. at 22.

[25] *See id*. at 31 (discussing the "integral role [SSNs] play as unique and permanent identifiers to link consumers to their records in our financial system," as well as the "increased risk of identity theft associated with the widespread use and availability of SSNs").

[26] *Id*.

The widespread use and availability of SSNs is clearly one of the underlying causes of identity theft. The use of SSNs by public entities is arguably somewhat restricted but the same is not true of private entities. The Privacy Act of 1974 restricts the ability of state and federal government agencies to require individuals to disclose their SSNs in order to receive public services. The Act does not impose any similar restriction on private entities. Further, even the restrictions on state and federal agencies are subject to many exceptions. Despite the harm inherent in using the SSN as a universal identifier, this use continues to be "business as usual" in the public and private sector. Sometimes, all an identity thief needs to open a credit account or to gain access to an existing account is the name and SSN of the victim.[27]

Vulnerabilities in Information Security

The electronic collection and storage of personal information by public and private record holders demands the implementation of effective information security practices that protect against data breaches. This need seems especially pressing for information databases that can be remotely accessed and are therefore susceptible to hacking. Recent accounts of data breaches indicate that, collectively, the personal information of millions of individuals has been compromised over the past five years, potentially exposing millions to identity theft. Sometimes these data breaches are attributed to hackers who exploit information security weaknesses in order to remotely access a computer network and steal the information contained on or available through the network. Other times, record keepers may mistakenly disclose or expose personal information. An employee's loss of a laptop or other storage device containing unprotected sensitive personal information exposes the information to potentially unauthorized access and

[27] *Id*. at 14.

use. Disclosing public records or reports without first redacting any private, personal information also can leave personal information vulnerable to fraudulent uses such as identity theft.

Notions of fairness imply that all record holders, both private and public, should have at least an implicit duty or responsibility to protect personal information. Yet, the number of reported information security breaches has been increasing since 2005.[28] Perhaps this is due in part to the fact that there is no universal mandate for the reasonable protection of personal information. Identity thieves can capitalize on the many recent information security breaches in order to gain access to SSNs and other personally identifiable information. The personal information of millions of consumers is compromised each year by inadequate security systems, inadequate screening and sometimes just plain carelessness.

In 2008 alone 641 data breaches were reported, compromising more than 35 million consumer records.[29] According to the Identity Theft Resource Center, the total number of breaches in the United States has increased sharply since 2005, when the center first began tracking data breaches.[30] In 2008, there were 47% more data breaches than in 2007. According to Javelin, the total number of identity thefts also increased in 2008, by 19%.[31] In light of the potentially harmful effects of data breaches, information security should be a priority for public and private entities alike.

---

[28] Identity Theft Resource Center, Breach Report 2008 (Jan. 2, 2009), http://www.idtheftcenter.org /BreachPDF/ITRC_Breach_Report_2008_final.pdf (last visited March 10, 2009).

[29] *Id*.

[30] *See* Identity Theft Resource Center, Reference Library, ITRC Surveys & Studies, http://www.idtheftcenter.org/artman2/publish/lib_survey /index.shtml (last visited March 10, 2009).

[31] JAVELIN STRATEGY AND RESEARCH , 2009 IDENTITY FRAUD SURVEY REPORT, *supra* note 14, at 15.

The current speculation on whether or not data breaches account for a large portion of identity thefts detracts attention from the real issue: public and private entities frequently fail to safeguard the sensitive personal information of the individuals these entities exist to serve. Individuals are vital to public and private entities and financially support both kinds of entities.[32] In return these entities offer products and services to individuals but require them to disclose their personal information in order to receive products or services. Once personal information is disclosed, individuals retain little control over the public or private uses of their personal information and cannot meaningfully prevent its theft. Thus, record holders that collect, maintain, or use personal information in order to further their own interests or goals should have an explicit responsibility to ensure that such information is not used in a way that harms individuals.

Consumers are left more vulnerable to identity theft every time a data breach occurs but have little recourse against the entities responsible for preventing such breaches. The government and private businesses both need to do more to prevent data breaches but without clear federal standards for information privacy it is difficult to ensure that reasonable information practices are universally followed. The federal government, with its many agencies and many separate information systems, has been unable to implement adequate security measures. This may be due in part to the fact that there are so many separate agencies with different information systems; thus, a one-size-fits-all approach may not be feasible.

[32] In the public sector, these entities exist to serve the public by providing services funded by taxpayer money. In the private sector, these entities exist on the profits derived from selling products and services to consumers.

Private financial institutions are required to disclose privacy practices, restrict some information sharing, and reasonably safeguard consumer information. Credit agencies are required to afford consumers some degree of control over their credit histories and remove incorrect information. The sharing of health information by and between health care providers is restricted to what is necessary in order to "adequately" conduct business and provide healthcare services. However, many other industries are not regulated by any specific information privacy or protection rule, which means that no clear standard of privacy applies to records held by these companies. For example, data brokers, which arguably hold the most detailed individual records, are not directly regulated by any specific identity theft law, except with regard to information obtained from consumer credit reports.

Section 5 of the Federal Trade Commission Act (FTC Act), which prohibits unfair business practices, applies to data brokers as well as other private businesses.[33] It has been used by the FTC to enforce information privacy and protection standards.[34] However, the majority of these Section 5 actions are not brought simply because a company inadequately protected consumer information. Most of the cases are framed in terms of a quasi breach of duty: the company made a promise about how they would protect consumer privacy and the lapse in the company's security or privacy practices indicates that the company has breached its promise to consumers.

Often such "promises" are made by companies in their privacy policies. However, excluding those in the financial, credit and healthcare industries, most companies are not even

[33] 15 U.S.C. § 45 (2006).

[34] *See supra* Chapter Three, notes 132-135 and accompanying text.

required to disclose privacy policies and practices to consumers. For many companies, unless they make promises not to, they may freely share personal information in a number of ways, including selling it to data brokers and third party marketers. Essentially, there are no standards for the information sharing and protection practices of many private businesses other than the standards they set for themselves.

The FTC may take action against private businesses that fail to honor their privacy policies, even where the disclosure of a privacy policy was not mandated by law. However, initial violations of the FTC Act are essentially just warnings to businesses—no civil fines can be imposed unless a company continues its unfair information practices after a final FTC order declaring the practice unfair. The FTC Act does not mandate any specific standard for information protection. Nor does it act as a strong disincentive against lax information sharing and protection practices.

Lack of Control over Personal Information

There are no universal standards regulating the protection and use of personal information by public and private record keepers. Many public and private entities may have wide latitude to control how they collect, use and share personal information. Individuals, on the other hand, have little control over whether or not to disclose or share personal information with private businesses or the government. These individuals may "control" their information by opting not to disclose it. However, the disclosure of personal information is often a prerequisite to receiving services. So, individuals must choose between either keeping their personal information private or receiving the private services or public benefits they are seeking. Once disclosed, consumers retain little control over how their personal information is treated by private businesses or the government.

Consumers have some limited ability to control their personal information and protect their identities under consumer rights laws such as the provisions of the FCRA—which entitle individuals to free credit reports—and the provisions of the GLB Act—which allow consumers to "opt out" of allowing financial institutions to share their personal information with third-party marketers. However, the scope of these laws is limited to the personal information under the control of specific industries. Even those consumers that proactively avail themselves of all of their information privacy rights under federal law have limited means to prevent the theft of their own identities.

The Fair Credit Reporting Act (FCRA) gives consumers specific rights over the personal information contained in their credit reports. The FCRA limits who can receive a consumer's credit reports without express consumer consent. Consumers also have a right of access to their credit report information. Further, if a consumer notices fraudulent information on their credit report they may report that information to a credit reporting company. That company then has the duty to place a fraud alert on the consumer's credit file, conduct an investigation and remove any fraudulent information. The company also must notify the other credit reporting companies and those companies must also place a fraud alert on the consumer's credit file. Additionally, the FCRA limits the liability of consumers to creditors for fraudulent financial charges. Most of the consumer protection provisions of the FCRA are remedial in nature and help consumers by limiting the resulting harm caused by identity theft. While they offer some protection, they do not give consumers the tools to prevent the actual theft of their identities.

The Gramm-Leach-Bliley Act (GLB Act) also gives consumers some rights to protect their personal information. However, the true value of these protections is debatable. Under the GLB Act, every financial institution must send its consumers an annual privacy notice that discloses

the institution's information sharing practices and also give consumers the ability to "opt out" of specific kinds of information sharing. However, the "opt out" provisions are limited, and consumers cannot control the way financial institutions share their personal information for routine business operations, such as servicing accounts, processing payments and printing statements. Consumers further cannot "opt out" of all types of information sharing for marketing purposes. For example, a financial institution is permitted to continue to share consumer information with any third parties that market that institution's financial products.

Additionally, consumers may not be aware of their right to "opt out" of information sharing. The typical consumer receives numerous privacy notices every year. Often consumers either do not "read the fine print" of these notices or may not fully understand the often complex notices. Even consumers who are aware of their right to "opt out" of information sharing must take additional affirmative steps to do so. A consumer receiving a privacy notice by mail will typically have the option to call, go online or write a letter informing the institution involved that they do not want their personal information shared with third parties. Conceivably, only the most proactive or diligent consumers ultimately avail themselves of the "opt out" options.

Arguably, the GLB Act privacy provisions do not offer consumers a meaningful way to control the way their personal information is shared. Consumers would benefit more from the GLB Act Privacy Rule if there were standards for simplified disclosures that are easily understood by most consumers, not just most consumers with a legal or business background. As it stands right now, the requirement that privacy policies provide "clear and conspicuous notice to customers that accurately reflects [an institution's] policies and practices" leaves substantial room for legalese and technical nuances that many consumers may not be familiar with.

Additionally, an "opt in" provision, which restricts a financial institution from sharing an individual's personal information unless he or she has affirmatively consented, would be more meaningful than the current "opt out" requirements. Several states, including California, Connecticut and New Mexico, have enacted laws imposing "opt in" information sharing requirements on financial institutions.[35] The GLB Act does not preempt states from imposing more stringent privacy protections than those it requires. [36]

Another option that likely offers consumers even more protection than an "opt in" requirement would be a restriction barring all information sharing, other than disclosures in response to a court order or subpoena, or sharing that is directly related to business needs such as bill processing and statement printing. However, both an "opt-in" requirement and a strict restriction on sharing would likely meet great resistance from financial institutions that depend on marketing to generate new profits. However, if the GLB Act privacy provisions are intended to provide meaningful protection for personal information, then more robust provisions are necessary despite industry resistance.

Without granting consumers more meaningful control over their personal information, Congress must find ways to effectively control information sharing on behalf of consumers. Conceivably, federal lawmakers could, as some states already have, increase consumer protection by requiring all financial institutions to obtain individuals' consent prior to sharing their personal information with third parties. Congress could even take this a step further and require all companies to obtain consent before they sell to or share with a third party any

[35] CAL. FIN. CODE §§ 4050-4060 (West 2008); CONN. GEN. STAT. ANN. § 38a-988 (West 2008); N.M. ADMIN. CODE ANN. § 13-1-3 (West 2008).

[36] 15 U.S.C. § 6807(b) (2006).

consumer personal information, unless the sharing is directly related to the company's own business needs or marketing activities. The law could contain an exception, such as the GLB Act, expressly allowing a company to share personal information to facilitate necessary business services such as statement printing and payment processing. Also, to reduce the inhibition of such a provision on a company's own marketing activities, the law may permit a company to share personal information with a third party that will use the information only to market the company's own products or services.

In light of the vast number of sources of personal information, requiring all businesses to obtain consent before sharing personal information may be difficult to implement. Further, it may be overly burdensome to some records holders. However, the burden would be reduced by including exceptions for a company's business and marketing needs. Essentially, such a law would limit companies from profiting from the sale of individuals' personal information without individuals' consent. It would also protect consumers from having their personal information shared in a manner that goes beyond what they likely anticipated when they first disclosed their information to a private company.

Fragmented Federal Privacy Protections

In the United States, there is no single law that regulates all uses of personal information.[37] Congress has criminalized identity theft. However, addressing identity theft purely in the context of criminal law, by punishing the fraud, is not adequate by itself. There are not enough law enforcement resources to investigate and prosecute the estimated 8-10 million identity thefts

[37] GOV'T ACCOUNTABILITY OFFICE, PERSONALLY IDENTIFIABLE INFORMATION, GAO-08-343 (2008).

each year. Congress also has passed information privacy laws that apply to the privacy practices of particular sectors of the economy or particular industries but none that apply universally.

As it stands currently, the patchwork system of information privacy protection in the United States does not adequately address the widespread availability and disclosure of personal information among private and public entities. Some U.S. industries are more heavily regulated than others, while some businesses or industries are largely unregulated. There is no clear, universal definition of what constitutes sensitive personal information, no broad mandate for the protection of this information, and no minimum restriction on the sharing of personal information. Currently, federal information privacy protections essentially make the privacy of some personal information a priority based upon the type of record keeper, not the type of information itself. This is a flawed approach. Rather, information privacy laws should recognize the most sensitive types of personal information and regulate the use of that information no matter the source.

A set of generally applicable information privacy and security standards would at the very least provide a minimum threshold for protection. This baseline could serve as a springboard for additional, more targeted, regulation and could also work in conjunction with the current industry-specific laws. Prescribing universal information privacy and security standards would help to fill in existing gaps because the standards would apply to entities and industries not currently regulated by any specific information privacy law. Such general information privacy protections could also be supplemented as needed to respond to nuances regarding emerging technologies or industry-specific privacy concerns. Additionally, a general minimum threshold for information privacy need not supplant current industry-specific information privacy laws and regulatory frameworks that impose equivalent or more stringent privacy standards.

Research Question 3: Legislative Proposals to Identity Theft

To get a better idea of how Congress may legislatively attack identity theft in the future, Chapter 5 of this thesis examined the most recent identity theft bills considered by Congress. From 1998 through 2008, more than 200 identity-theft related bills were introduced in Congress. In 2007 and 2008 alone, during 110th Congress, nearly sixty identity theft bills were introduced but only one, a criminal statute, was passed. An additional eight identity-theft related bills passed one of the houses but failed to move through the other. During the current, 111th Congress, eight identity theft bills were introduced between the start of the current session on January 6, 2009 and February 20, 2009, the day this search was conducted.

The bills currently pending before Congress share similarities with those introduced but not fully passed during the previous session of Congress. The most common themes among these bills include further restrictions on the use of SSNs by public and private entities, mandatory consumer notification of suspected fraud, and the imposition of additional reporting requirements, such as mandatory identity fraud reporting by financial institutions. Data breach notification is mostly absent amongst the themes of these bills. There have been several breach notification statutes introduced in Congress, but none have managed to garner enough support to pass both the House and Senate. This may indicate a lack of congressional will to impose breach notification requirements.

Further, the absence of breach notification requirements in the first identity theft bills introduced in the current, 111th Congress may indicate that the tone of identity theft discussion has been set and it does not include consideration of breach notification requirements. However, it is still too early in the session to make any definitive assumptions. Notably, the 2007 version of the Identity Theft Enforcement and Restitution Act passed by the Senate contained provisions requiring breach notification. However, those provisions were left out of the final 2008 version

of the bill that ultimately passed both houses. Another provision of the 2007 version that was not included in the final 2008 bill would have prohibited businesses from soliciting SSNs except where necessary for business purposes and no alternative identifier would suffice.

Congress may be unlikely to pass legislation significantly restricting the use of SSNs, requiring the development of alternative methods of identification, or universally prohibiting specific private uses of personal information. Ultimately, Congress may be hesitant to pass any new regulations that would potentially impose greater burdens on private businesses.

However, a new Congress has just convened. In addition, there is a new political climate in Washington D.C. with the Democrats in control of the White House and both Houses of Congress and the current economic fallout from the 2009 mortgage crisis and economic recession. The shift in Washington may affect the tone of congressional discussions and political will on any number of issues, including identity theft and information privacy.

Research Question 4: Potential Solutions for Combating Identity Theft

Overall, a universally applicable and comprehensive strategy for combating identity theft is needed. Before such a strategy can be truly effective at reducing the risk of identity theft, more understanding is needed regarding the contours of the crime. This understanding can only come from an examination of identity theft from all angles—the source of stolen personal information, the failure to adequately verify identity, the amount of the fraud, the ways consumers and businesses recover from the harm, and the investigation and arrest of identity thieves. In order to achieve a better understanding, a system for reporting and analysis of comprehensive identity theft data is necessary.

Such a system would allow for the identification of common identity theft factors and of emerging factors and trends that may enable government and businesses to take a more proactive approach to mitigating identity theft. For example, it may help law enforcement identify new

technologies that are increasingly being used in identity theft or geographic patterns of fraud, drawing attention to potential sources identity theft. It may help businesses to identify common risk factors which, when present, increase the likelihood of identity theft. This may enable the development of more accurate identity verification techniques.

In light of the uncertainties that surround identity theft it is difficult to define any clear and comprehensive legislative strategy for mitigating the overall risks of identity theft. However, at a minimum, Congress needs to find a way to control the uses of SSNs in both the public and private sectors. One place to start is by assigning the FTC or a similar administrative agency the task of reviewing the multiple ways SSNs are used in the public sector, as well as in the private sector. Additional attention should be paid to how SSNs are used in conjunction with other personally identifying information, such as date of birth or drivers license number, to establish the identity of new customers or applicants. With a better understanding of how SSNs are used, the designated agency could establish rules defining appropriate minimum standards for the use of SSNs by public entities and by private entities. These standards should govern the ways SSNs are collected, stored, shared and verified, as well as limit the use of SSNs as the primary identifying characteristic of individuals.

Additionally, Congress needs to take the initiative to create a standard reporting mechanism or mechanisms for identity theft complaint and investigation information. Such a system for reporting should account for all major sources of identity theft information—consumers, private entities and government bodies. In order for this system to be effective private and public entities should be required to report aggregate, non-personal data on identity theft, including the amount of fraud, type of account, how the fraud was initiated, the

demographic characteristics of the stolen identities, and the length of time before the fraud was discovered.

In addition, Congress should require businesses that routinely collect and maintain personal information to report any breach of personal information, including the number of records compromised, the number of individuals affected, the types of information disclosed, the circumstances of the breach, the steps to could have been taken to avoid the breach, and the steps that were taken to mitigate the harm.[38] This information would be useful for a number of different reasons.

The knowledge that a business would have to report breaches to the government may encourage the implementation of more secure information security practices. Further, if Congress enacts universal information security standards then businesses could be held accountable for violating these standards. Additionally, the data could be analyzed in conjunction with identity theft and fraud data, in order to better understand the interplay of data breaches and identity theft. These results could also be used to identify needed additional information security practices and to rationally define appropriate breach notification requirements. Congressional action is necessary to ensure that all businesses report this information. Absent a congressional mandate, administrative agencies may be able to use their existing authority to promulgate reporting rules. However, those rules would only apply to the specific entities within the jurisdiction of the promulgating agencies.

[38] Congress may want to exempt from the reporting requirements some small businesses or businesses that maintain personal information on relatively few individuals.

Depending on the severity of a data breach and the potential for resulting fraud, businesses and public agencies should be required in some instances to notify consumers whose information has been breached. The arguments against breach notification have pointed out that there is no proven significant connection between data breaches and identity theft. Thus, the argument goes, there is no reason to alarm consumers and waste money notifying them when there is little likelihood of harm. However, these arguments inaccurately assume that since there is no direct proof that data breaches significantly contribute to identity theft, there is no significant relationship between the two. This is faulty logic.

Just as there is no conclusive evidence that data breaches lead to a significant number of identity thefts, there is likewise no evidence that these breaches do not cause significant harm to consumers. Identity theft survey data indicates that the source of stolen information in the majority of identity thefts is unknown. However, it is certain that data breaches do cause at least some identity thefts. Rather than brushing aside concerns over data breaches, perhaps it is better to err on the side of caution and assume that, since some breaches do cause identity theft, all breaches are potentially harmful to consumers. Then, rather than arguing over whether or not to require breach notification at all, the debate could shift towards focusing on ways to minimize the incidences of breaches and the costs of notification to businesses.[39]

For example, businesses could publicly post general breach notifications on a centralized Web site and set up a toll-free number where consumers could get automated information about whether their records where involved in the breach. With a system such as this, businesses may

[39]To avoid placing an undue burden on small businesses, Congress may want to limit the applicability of breach notification requirements based on certain factors such as the size of the business, number of employees, or the amount of personal information maintained.

only be required to mail notification to individual consumers where there is a high degree of risk for fraud. One example of a high degree of risk may include the remote hacking of a company's information system and subsequent theft of personal information. In this type of targeted breach, there is proof the information was actually obtained by a criminal and evidence that the criminal likely intends to misuse the information. On the other hand, the reported loss of a laptop computer that contains only encrypted data, including personal information such as name, address and date of birth, may not pose a severe fraud risk. The chances that the information can be unencrypted and misused are low and there is no indication that anyone specifically intends to misuse it.

Conclusion

Establishing effective control over the protection and use of personal information is difficult when the sources of this information are so widespread. Restricting the future sharing and collecting of personal information and improving information security may improve privacy protections for personal information. However, these solutions together are inadequate because the sources of personal information are already so prevalent. More secure and accurate ways of to verify identity are necessary. The universal use of SSNs as the dominant method that both public and private entities use to verify identity is one of the primary reasons consumers are so susceptible to identity theft. The SSN was not intended for use as a universal identifier.

The SSN originated as a way to identity individuals who contribute financially to the Social Security system and, thus, qualify for Social Security retirement benefits. Now, rather than simply tying individuals to the records that relate to their entitlement to public retirement benefits, the SSN links individuals to nearly all of their personal and financial records. At the same time, the SSN is used as a means to verify that an individual is who he or she claims to be. Thus, the SSN is used to prove identity and to identify individual records.

The history of widespread use of SSNs in the public and private sectors began before the advent of the Information Age. Record keepers were not yet conscious of the potential danger of such use in the "Information Age," where society revolves around the creation, distribution, processing, storing, and accessing of information. Nor had record keepers likely realized the full ramifications of computers and the digital revolution on the collection and storage of personal information. It is clear now that the widespread reliance on SSNs is untenable, especially in light of the fact that records containing SSNs now reside electronically in many different locations, leaving them vulnerable to accidental disclosure or theft.

Besides the massive use of SSNs, another that has likely contributed to the rise in identity theft is the increased use of electronic communications and electronic methods for conducting business. It is likely more difficult and more risky for an identity thief to impersonate someone in person. In person, the thief will likely be asked to show some picture identification and also faces the possibility that the fraud will be discovered by someone who is physically present, which increases the risk that the thief can be identified and arrested. Electronic methods of communications and transactions enable an identity thief to conduct fraudulent transactions from a safer distance where the burden of identification may be lower. However, these electronic methods are not to blame for the fact that thieves are so often able to fraudulently use the identities of others—the breakdown occurs because there is no secure or accurate way to verify that people are who they say they are.

Effectively curbing identity theft will require the development of new means for verifying identity and better information security protections. Developing secure standards for identity verification does not mean that a new single, universal identifier is necessary. It means developing an identification method that does not rely so heavily on any one individual attribute

for identification. With the heavy reliance on electronic communication and online business transactions, it would be easy to fraudulently use and exploit any such single means of identification.[40]

Some authors have suggested the use of biometrics and other similar technologies. These are beyond the scope of this thesis. However, future studies should consider the pros and cons of such identification methods and analyze what approaches seem most tenable. The purpose of this research was to discern the overarching deficiencies with the current federal regulatory scheme, identity difficulties inherent to combating identity theft, and suggest some potential legislative solutions that may improve identity theft protections.

[40] *See* Lynn M. LoPucki, *Symposium: Enforcing Privacy Rights: Remedying Privacy Wrongs—Did Privacy Cause Identity Theft?* 54 HAST. L.J. 1277, 1287-91 (2003) (discussing the problems with current methods of identitfication that rely heavily on the use of name, address, SSN and date of birth to identify individuals).

LIST OF REFERENCES

Statutes

18 U.S.C. § 1961 (2006).

42 U.S.C. § 405 (2000).

Administrative Procedure Act, 5 U.S.C. §§ 551-559 (2006).

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2006).

E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 tit. III (2002) (codified in scattered sections of 44 U.S.C.A. (West 2008)).

Electronic Fund Transfer Act, Pub. L. No. 95-360, 92 Stat. 3278 (1978) (codified as amended in scattered sections of 15 U.S.C. (2006)).

Fair and Accurate Credit Transctions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003) (amended at 15 U.S.C. §§ 1681-1681x (2006)).

Fair Credit Billing Act, Pub. L. No. 93-495, 88 Stat. 1500 (1974) (codified as amended in scattered sections of 15 U.S.C. (2006)).

Fair Credit Reporting Act, 15 U.S.C. § 1681-1681x (2006).

Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692-1692p (2006).

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2006).

Freedom of Information Act, 5 U.S.C. § 552 (2006).

Gramm-Leach-Bliley Act tit. V, 15 U.S.C. §§ 6821-6827 (2006).

Identity Theft Assumption and Deterrence Act of 1998, Pub. L. No, 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C. § 1028 (2006)).

Identity Theft Penalty Enhancement Act, Pub. L. No. 108-275, 118 Stat. 831(2004) (codified in relevant part at 18 U.S.C. § 1028A) (2006)).

Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, tit. II, §§ 201-09, 122 Stat. 3560, (2008) (codified in scattered sections of 18 U.S.C. (2006)).

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2006).

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

Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2006).

Cases

Dep't of State v. Wash. Post Co., 456 U.S. 595 (1982).

FTC v. 30 Minute Mortgage, Inc, 03 civ. 60021, FTC File No. 022-3224 (S.D. Fla. Nov. 26, 2003).

FTC v. C.J., 03 civ. 5275, FTC File No. 03-5275 (C.D. Cal. July 25, 2003).

FTC v. Garrett, No. H-01 civ. 1255, FTC File No. 12-3067 (S.D. Tex March 8, 2002).

FTC v. Hill, No. H-03 civ. 5537, FTC File No. 032-3102 (S.D. Tex Dec. 18, 2003).

U.S. v. Am. United Mortgage Co., No. 07C civ. 7064, FTC File No. 062-3103 (N.D. Ill. Dec. 18, 2007).

U.S. v. ChoicePoint, No. 1:06 civ. 198, FTC File No. 052-3069 (N.D. Ga. Feb. 15, 2006).

U.S. v. Hill, H-04 cr. 4-ALL (S.D. Tex. Feb. 9, 2004).

U.S. v. Performance Capital Mgmt., 2:01 civ. 1047, FTC File No. 982-3542 (C.D. Cal. Feb. 6, 2001).

FTC v. Rapp, No. 99-WM civ. 783, FTC File No. 982-3542 (Dist. Colo. June 22, 2000).

Federal Administrative and Executive Materials

Agency Rules

12 C.F.R. § 30 (2009).

12 C.F.R. § 41 (2009).

12 C.F.R. §§ 208, 225 (2009).

12 C.F.R. § 222 (2009).

12 C.F.R. § 334 (2009).

12 C.F.R. § 364 (2009).

12 C.F.R. §§ 568, 570 (2009).

12 C.F.R. § 570 (2009).

12 C.F.R. § 571 (2009).

12 C.F.R. § 717 (2009).

16 C.F.R. § 313 (2009).

16 C.F.R. § 314 (2009).

16 C.F.R. § 681 (2009)

16 C.F.R. § 682 (2009).

17 C.F.R. § 248 (2009)

31 C.F.R. § 103 (2009).

45 C.F.R. § 160 (2009).

45 C.F.R. § 162 (2009).

45 C.F.R. § 164 (2009).

Administrative Adjudications

CardSystems Solutions, Inc., 2005 F.T.C. LEXIS 176, FTC File No. 052-3148 (Sep. 5, 2006).

Gateway Learning, Corp., 138 F.T.C. 443 (2004).

Microsoft Corp., 134 F.T.C. 709 (2002).

Executive Orders

Exec. Order No. 13402, 71 Fed. Reg. 27945 (May 10, 2006).

Legislative Materials

Unenacted Federal Bills

H.R. 122, 111th Cong. (2009).

H.R. 123, 111th Cong. (2009).

H.R. 133, 111th Cong. (2009).

H.R. 137, 111th Cong. (2009).

H.R. 220, 111th Cong. (2009).

H.R. 266, 111th Cong. (2009).

H.R. 1525, 110th Cong (2007).

H.R. 1677, 110th Cong. (2007).

H.R. 1684,110th Cong. (2007).

H.R. 3046, 110th Cong. (2007)

H.R. 4791, 110th Cong. (2007).

H.R. 5719, 110th Cong. (2008).

H.R. 6600, 110th Cong. (2008).

S. 141, 111th Cong. (2009).

S. 239, 110th Cong. (2007)

S. 495, 110th Cong. (2007).

S. 1178, 110th Cong. (2007).

S. 1789.109th Congress (2005).

S. 2168, 110th Cong. (2007).

Congressional Reports, Hearing and Testimony

H. Rep. 108-528, 108th Cong. (2004).

H. Rep. 108-528, 108th Cong. (2004).

S. Rep. 110-70, 110th Congress (2007).

153 Cong. Rec. S379 (daily ed. Jan. 10, 2007).

153 Cong. Rec. S14276 (daily ed. Nov. 13, 2007).

153 Cong. Rec. S12938-39 (daily ed. Oct. 16, 2007).

153 Cong. Rec. S7086 (daily ed. July 22, 2008).

Prepared Statement of the FTC: Hearing on the FTC Reauthorization Act of 2008 Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (2008), available at http://www.ftc.gov/os/testimony/P034101reauth.pdf.

Reports

Government Reports

CENTER FOR IDENTITY MANAGEMENT AND INFORMATION PROTECTION (CIMIP), IDENTITY FRAUD TRENDS AND PATTERNS: BUILDING A DATA-BASED FOUNDATION FOR PROACTIVE ENFORCEMENT (Oct. 2007), *available at*

http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf (last visited March 10, 2009).

FED. BUREAU OF INVESTIGATION, FIN. CRIMES REP. TO THE PUB.: FISCAL YEAR 2006 (Oct. 1 2005–Sept. 30, 2006) (2006), *available at* http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm (last accessed March 10, 2009).

FTC, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA FOR JANUARY – DECEMBER 2007 (Feb. 2008), *available at* http://www.ftc.gov/sentinel/ reports/sentinel-annual-reports/sentinel-cy2007.pdf (last visited March 10, 2009).

FTC, 2006 IDENTITY THEFT SURVEY (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinal ReportIDTheft2006.pdf (last visited March 10, 2009).

FTC, 2003 IDENTITY THEFT SURVEY (2004), *available at* http://www.ftc.gov/os/2007/11/SynovateFinal ReportIDTheft2006.pdf (last visited March 10, 2009).

FTC, OFFICE OF THE INSPECTOR GENERAL, A BRIEF OVERVIEW OF THE FTC'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (July 2008), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm (last visited March 10, 2009).

GOV'T ACCOUNTABILITY OFFICE, IDENTITY THEFT: SOME OUTREACH EFFORTS TO PROMOTE AWARENESS OF NEW CONSUMER RIGHTS ARE UNDERWAY, GAO-05-710 (2005).

GOV'T ACCOUNTABILITY OFFICE, FEDERAL ACTIONS COULD FURTHER DECREASE AVAILABILITY IN PUBLIC RECORDS, THOUGH OTHER VULNERABILITIES REMAIN, GAO-07-752 (2007).

GOV'T ACCOUNTABILITY OFFICE, DESPITE REPORTED PROGRESS, FEDERAL AGENCIES NEED TO ADDRESS PERSISTENT WEAKNESSES, GAO-07-837 (2007).

GOV'T ACCOUNTABILITY OFFICE, PERSONALLY IDENTIFIABLE INFORMATION, GAO-08-343 (2008).

GRAEME R. NEWMAN AND MEGAN MCNALLY, REPORT PREPARED FOR THE U.S. DEPT. OF JUSTICE, IDENTITY THEFT LITERATURE REVIEW (2005), *available at* http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf (last visited March 10, 2009).

PRESIDENT'S IDENTITY THEFT TASKFORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf (last visited March 10, 2009).

PRESIDENT'S IDENTITY THEFT TASKFORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, vol. II supp. (2007), *available at* http://www.idtheft.gov/reports/VolumeII.pdf (last visited March 10, 2009).

PRESIDENT'S IDENTITY THEFT TASKFORCE, TASKFORCE REPORT (2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf (last visited March 10, 2009).

JULIA S. CHENEY, PAYMENT CARDS CENTER, IDENTITY THEFT: A PERNICIOUS AND COSTLY FRAUD (2003), *available at* http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2003/IdentityTheft_122003.pdf (last visited March 10, 2009).

U.S. CENSUS BUREAU, 2003 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY REPORT (released June 2005), *available at http://www.census.gov/prod/2005pubs/ict-03.pdf* (last visited March 10, 2009).

U.S. CENSUS BUREAU, 2004 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY REPORT (released March 2006), *available at* http://www.census.gov/prod/2006pubs/ict-04.pdf (last visited March 10, 2009).

U.S. CENSUS BUREAU, 2005 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY REPORT (released April 2007), *available at* http://www.census.gov/prod/2007pubs/ict-05.pdf (last visited March 10, 2009).

U.S. CENSUS BUREAU, 2006 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY (released March 2008), *available at* http://www.census.gov/csd/ict/xls/2006/Full%20Report.htm (last visited March 10, 2009).

U.S. CENSUS BUREAU, 2007 INFORMATION-AND-COMMUNICATION-TECHNOLOGY SURVEY (released Feb. 25, 2009), *available at* http://www.census.gov/csd/ict/ (last visited March 10, 2009).

U.S. CENSUS BUREAU, 2007 SERVICE ANNUAL SURVEY (released March 2009), *available at* http://www.census.gov/econ/www/servmenu.html (last visited March 10, 2009).

U.S. CENSUS BUREAU, E-STATS REPORT (May 2007), *available at* http://www.census.gov/eos/www/2005/2005reportfinal.pdf (last visited March 10, 2009).

U.S. DEP'T OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973) , *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited March 10, 2009).

Private Industry Reports

JAVELIN STRATEGY AND RESEARCH, 2004 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2004), available at http://www.javelinstrategy.com/ research/2 (last visited March 10, 2009).

JAVELIN STRATEGY AND RESEARCH, 2005 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2005), available at http://www.javelinstrategy.com/ research/2 (last visited March 10, 2009).

JAVELIN STRATEGY AND RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2008), available at http://www.javelinstrategy.com/research/2 (last visited March 10, 2009).

JAVELIN STRATEGY AND RESEARCH, 2007 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2007), available at http://www.javelinstrategy.com/ research/2 (last visited March 10, 2009).

JAVELIN STRATEGY AND RESEARCH, 2008 IDENTITY FRAUD SURVEY REPORT (Consumer Version) (Feb. 2008), available at http://www.javelinstrategy.com/ research/2 (last visited March 10, 2009).

PEW INTERNET AND AMERICAN LIFE PROJECT, HOME BROADBAND ADOPTION (2008), *available at* http://pewinternet.org/pdfs/PIP_Broadband_2008.pdf (last visited March 10, 2009).

PEW INTERNET AND AMERICAN LIFE PROJECT, INTERNET USAGE OVER TIME (current through Dec. 31, 2008), *available at* http://www.pewinternet.org/trends/UsageOverTime.xls (last visited March 10, 2009).

PEW INTERNET AND AMERICAN LIFE PROJECT, MOBILE ACCESS TO DATA AND INFORMATION (2008), *available at* http://www.pewinternet.org/topics.asp?c=4 (last visited March 10, 2009).

THE WORLD PRIVACY FORUM, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU (2006), *available at* http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (last visited March 10, 2009).

Books

DANIEL J. SOLOVE, MARC ROTENBURG AND PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (2d ed. Aspen Pub., New York 2006).

DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (NYU Press, New York 2004).

FRED H. CATE, PRIVACY IN PERSPECTIVE (AEI Press, LaVergne, TN 2005)

RICHARD A. POSNER, THE ECONOMICS OF JUSTICE (Harv. Coll., Cambridge, Mass.1981).

RICHARD POSNER, ECONOMIC ANALYSIS OF LAW (7th ed. Aspen Pub., New York 2007).

ROBERT O'HARROW, JR., NO PLACE TO HIDE (Free Press, New York 2006).

PHISHING AND COUNTERMEASURES (Markus Jakobsson and Steven Myers eds., Wiley-Interscience, Hoboken, N.J. 2007).

Law Review and Journal Articles

Brendan S. Amant, Note, *The Misplaced Role of Identity Theft in Triggering Public Notice*, 44 HARV. J. ON LEGIS. 505 (2007).

Chris Barnstable-Brown, *Developments in Banking and Financial Law*, 26 ANN. REV. BANKING AND FIN. LAW 38 (2007).

J. Howard Beales, III and Timothy J. Muris, *Symposium: Surveillance: Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109 (2008).

Reesa Benkoff, *Developments in Banking and Financial Law: 2005: Combating Identity Theft*, 25 ANN. REV. OF BANKING AND FIN. L. 127 (2006).

Susan W. Brenner and Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. AND POL'Y 211 (2006).

Melissa F. Brown, *Family Court Records: A Treasure Trove for Identity Thieves*, 55 S. CAR. L. REV. 777 (2004).

Andrew Capalbo, *Developments in Banking and Financial Law: 2004: III. Consumer Credit: B. Consumer Privacy*, 24 ANN. REV. BANKING AND FIN. L. 42 (2005).

Mike Cook, *The Lowdown on Fraud Rings*, 10 COLLECTIONS AND CREDIT RISK 20 (2005).

Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. BALT. L. REV. 1 (2006).

Barbara Crutchfield George, Patricia Lynch and Susan F. Marsnik, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735 (2001).

Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 VAL. U.L. REV. 1061 (2007)

Francis J. Facciolo, Unauthorized Payment Transactions: Who Should Bear the Losses, 83 Chi.-Kent L. Rev. 605 (2008).

Christine Easter, *Auditing for Privacy*, 1 J.L. AND POL'Y FOR INFO. SOC. 879 (2006).

David A. Freidman, Reinventing Consumer Protection, 57 DePaul L. Rev. 45, 48-56 (2007).

A. Michael Froomkin, Creating a Viral Federal Privacy Standard, 47 B.C.L. Rev. 55, 76 (2007).

Martin E. Halstuck and Bill F. Chamberlin, *The Freedom of Information Act 1966-2006: A Retrospective on the Rise of Privacy Protection over the Public Interest in Knowing What the Government's Up To*, 11 COMM. L. AND POL'Y 511 (2006).

Martin E. Halstuk, *Shielding Private Lives From Prying Eyes: The Escalating Conflict Between Constitutional Privacy and the Accountability Principle of Democracy*, 1 COMMLAW CONSPECTUS 71 (2003).

Young Han, *Developments in Banking and Financial Law: 2003: VI. Developments in Consumer Credit*, 23 ANN. REV. BANKING AND FIN. L. 72 (2004).

Dennis Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1 (2006).

Chris J. Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. AND TECH. 97 (2007).

Michael E. Jones, *Privacy on the Internet and in Organizational Database: Data Breaches: Recent Developments in the Public and Private Sectors*, 3 INFO. SOC'Y J.L. AND PUB. POL'Y 555 (2008).

Brian N. Larson and Genelle I. Belmas, *Second Class for the Second Time: How the Commercial Speech Doctrine Stigmatizes Commercial Use of Aggregated Public Records*, 58 S. CAROLINA L. REV. 935 (2007).

Stan Karas, *Loving Big Brother*, 15 ALB. L.J. SCI. AND TECH. 607 (2005).

Stan Karas, *Privacy, Identity, Database*, 52 AM. U.L. REV. 393 (2002).

David Koenigsberg, *Developments in Banking and Financial Law: 2005: XII. Security with Online Banking*, 25 ANN. REV. BANKING AND FIN. L. 118 (2006).

David Lish, Comment, *Would the Real David Lish Please Stand Up: A Proposed Solution to Identity Theft*, 38 ARIZ. L.J. 319 (2006).

Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89 (2001).

Lynn M. LoPucki, Symposium: *Enforcing Privacy Rights: Remedying Privacy Wrongs—Did Privacy Cause Identity Theft?* 54 HAST. L.J. 1277 (2003).

Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140 (2006).

Andrea M. Matwyshyn, *Symposium: Toward a General Theory of Law and Technology: Commerce, Development, Identity*, 8 MINN. J.L. SCI. AND TECH. 515 (2007).

Andrea M. Matwyshyn, Technoconsen(t)sus, 85 WASH. U. L. REV. 529 (2007).

J. Ryan McCarthy and Anita Pancholi, *Developments in Banking and Financial Law: 2003: Privacy*, 23 ANN. REV. BANKING AND FIN. L. 123 (2004).

James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1 (2005).

James P. Nehf, *Recognizing the Societal Value in Informational Privacy*, 78 WASH. L. REV. 1, 81 (2003).

Catherine Pastrikos, Comment, *Identity Theft Statutes: Which Will Protect Americans the Most?*, 67 ALB. L. REV. 1137 (2004).

Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. AND TECH. L. REV. 27 (2007).

Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978).

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992)

Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999).

Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999).

Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995).

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

Paul M. Schwartz, *Symposium: Enforcing Privacy Rights: Remedying Privacy Wrongs: New Models*, 54 HASTINGS L.J. 1183 (2003).

Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137 (2002).

Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 563 DUKE L.J. 967 (2003).

Daniel J. Solove and Chris J. Hoofnagle, *A Model Regime of Privacy Protection*, 2006 UNIV. ILL. L. REV. 357 (2006).

Peter P. Swire, *Financial Privacy and the Theory of High Tech Government Surveillance*, 77 WASH. U.L.Q. 461 (1999).

Harry Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2 (2004).

Tamela J. White and Charlotte A. Hoffman, *The Privacy Standards under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 W. VA L. REV. 709 (2004).

Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345 (2005).

J. Stephen Zielezienski and Catherine I. Paolino, *Insurance Privacy After Gramm-Leach-Bliley-Old Concerns, New Protections, Future Challenges*, 8 CONN. INS. L.J. 315 (2001-2002).

Terrance J. Keenan, *The FACT Act of 2003: Securing Personal Information in an Age of Identity Theft*, 2 SHIDLER J.L. COM. AND TECH. 5 (2005).

Newspapers, Magazines and Miscellaneous Articles

Martin H. Bosworth, *FTC Findings Undercut Industry Claims that Identity Theft Is Declining*, ConsumerAffairs.com, Feb. 9, 2007, http://www.consumeraffairs.com/ news04/2007/02/ ftc_top10_folo.html (last visited March 10, 2009).

Fred H. Cate, Center for Information Policy Leadership, *Information Security Breaches* (2008), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf (last visited March 10, 2009).

Fred H. Cate, Center For Information Policy Leadership, *Information Security Breaches and the Threat to Consumers* (2005), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265 /1280/Information_ Security_Breaches.pdf (last visited March 10, 2009).

Eric Goldman, *The Privacy Hoax*, FORBES Oct. 14, 2002.

Thomas M. Lenard and Paul H. Rubin, *An Economic Analysis of Notification Requirements for Data Security Breaches*, PROGRESS ON POINT, July 2005.

Arshad Mohammed, *Record Fine for Data Breach*, WASH. POST, Jan. 27, 2006, at D1.

Jonathon Stempel, *US Identity Fraud $45.3 billion in 2007, but Declining*, REUTERS, Feb. 11, 2008, *available at* http://www.reuters.com/article/rbssFinancialServicesAndRealEstateNews/idUSN1161861220080211 (last visited March 10, 2009).

Press Releases

Better Business Bureau (BBB), Press Release, New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think (Jan. 31, 2006), *available at* http://www.bbbonline.org/IDtheft/safetyQuiz.asp (last visited March 10, 2009).

Press Release, Better Business Bureau, New Research Shows That Identity Theft Is More Prevalent Offline with Paper than Online (Jan. 26, 2005), *available at* http://www.bbb.org/ALERTS/article.asp?ID=565 (last visited March 10, 2009).

Press Release, U.S. Dep't of Commerce, Bureau of Economic Analysis, 2005 Growth Led by Services Producing Industries (Dec. 11, 2006).

Press Release, U.S. Dep't of Commerce, Bureau of Economic Analysis, Financial and Insurance Industries Led Slowdown in 2007, *available at* http://www.bea.gov/newsreleases/industry/gdpindustry/2008/pdf/gdpind07_rev.pdf (last visited March 10, 2009).

Press Release, U.S. Dep't of Commerce, Bureau of Economic Analysis, Private Services-Producing Sector Continued to Lead Growth in 2006, *available at* http://www.bea.gov/newsreleases/industry/gdpindustry /2008/gdpind06_rev.htm (last visited March 10, 2009

Press Release, FBI, Protecting Your Identity (Aug. 21, 2006), *available at* http://www.fbi.gov/page2/dec06/scams 122906.htm (last visited March 10, 2009).

Press Release, FTC, Agencies Propose Rules on Identity Theft Red Flags and Notices of Address Discrepancy (July 18, 2006), *available at* http://www.ftc.gov/opa/2006/07/idtheftredflagjoint.shtm (last visited March 10, 2009).

Press Release, FTC, As Part of "Operation Detect Pretext" FTC Sues to Halt "Pretexting" (April 18, 2001), available at http://www.ftc.gov/opa/2001/04/pretext.shtm (last visited March 10, 2009).

Press Release, FTC, CardSystems Solutions Settles FTC Charges: Tens of Millions of Consumer Credit and Debit Card Numbers Compromised (Feb. 23, 2006), *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm (last visited March 10, 2009).

Press Release, FTC, ChoicePoint Settles Data Security Breach Charges: to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited March 10, 2009).

Press Release, FTC, Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams(Nov. 13, 2002), available at http://www.ftc.gov/opa/2002/11/netforce.shtm.

Press Release, FTC, FTC Issues Final Rule on Free Annual Credit Reports (June 4, 2004), *available at* http://www.ftc.gov/opa/2004/06/freeannual.shtm (last visited March 10, 2009).

Press Release, FTC, FTC Justice Dep't Halt Identity Theft Scam (March 22, 2004), available at http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm (last visited March 10, 2009).

Press Release, FTC, Nation's Big Three Consumer Reporting Agencies Agree To Pay $2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act (Jan. 13, 2000), *available at* http://www.ftc.gov/opa/2000/01/busysignal.shtm (last visited March 10, 2009).

Press Release, FTC, "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft, http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm (last visited March 10, 2009).

Section 5 of FTC Act, codified at 15 U.S.C. § 45 (2006).

Internet Sources

Center for Identity Management and Information Privacy, http://www.utica.edu/academic/institutes/cimip/ (last visited March 10, 2009).

DOJ.gov (U.S. Dep't of Justice), Fraud, http://www.usdoj.gov/criminal/fraud/websites/idtheft.html (last visited March 10, 2009).

HHS.gov (Dep't of Health and Human Services), Centers for Medicare and Medicaid Svcs., "Security Standards," http://www.cms.hhs.gov/SecurityStandard/ (last visited March 10, 2009).

HHS.gov (Dep't of Health and Human Services), Office for Civil Rights, "Health Information Privacy," http://www.hhs.gov/ocr/privacy/index.html (last visited March 10, 2009).

Elec. Privacy Info. Ctr., http://epic.org/privacy/medical/#stateLaw (last visited March 10, 2009).

FTC.gov, Consumer Protection Bureau, http://www.ftc.gov/bcp/about.shtm (last visited March 10, 2009).

FTC.gov, Division of Privacy and Identity Protection, http://www.ftc.gov/bcp/bcppip.shtm (last visited March 10, 2009).

FTC.gov, Identity Theft Site, http://www.ftc.gov/bcp/edu/microsites/idtheft (last visited March 20, 2009).

FTC.gov, Privacy Initiatives, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited March 10, 2009).

Identity Theft Resource Center, Breach Report 2008 (Jan. 2, 2009), http://www.idtheftcenter.org/BreachPDF/ITRC_Breach_Report_2008_final.pdf (last visited March 10, 2009).

IDTheft.gov, President's Identity Theft Taskforce, http://www.idtheft.gov/ (last visited March 10, 2009).

Library of Congress, THOMAS Advanced Bill Summary and Status Search, http://thomas.loc.gov/bss/ (last visited March 10, 2009).

Merriam-Webster Dictionary and Thesaurus (online edition), phishing, http://merriam-webster.com/dictionary/phishing (last visited March 10, 2009).

Merriam-Webster, Dictionary and Thesaurus (online edition), hacking, http://merriam-webster.com/dictionary/hacking (last visited March 10, 2009).

Privacy Rights Clearinghouse Web site, Chronology of Data Breaches—2005-2008, http://www.privacyrights.org/ar/ChronDataBreaches.htm. (last visited March 10, 2009).

BIOGRAPHICAL SKETCH

Kate Lucente grew up in Orange Park, Florida. She attended the University of North Florida, where she earned a Bachelor of Science in Mass Communication, summa cum laude. Kate worked for several years in Jacksonville, Florida before beginning her graduate studies at the University of Florida. At the University of Florida, Kate was part of the media law joint degree program. She graduated in May 2009 and received a Juris Doctor from the College of Law and a Master of Arts in Mass Communication from the College of Journalism and Communications. After graduation, Kate will join the Tampa, Florida office of DLA Piper as a litigation associate.