

Data Protection, Breach Notification, and the Interplay between State and Federal Law: The Experiments Need More Time

Flora J. Garcia *

INTRODUCTION	694
I. EXISTING LAWS AND RULES	695
A. <i>WHAT IS PRIVACY?</i>	695
B. <i>FEDERAL PRIVACY LAWS</i>	698
C. <i>PRIVACY IN ONLINE ACTIVITY</i>	699
D. <i>ENFORCEMENT BY EVERYONE</i>	701
E. <i>IN THE STATES</i>	702
1. California	703
2. Florida	705
3. Other State Laws.....	707
F. <i>CONGRESS TO THE RESCUE?</i>	710
II. BREACHES	713
A. <i>NEGLIGENCE: DATA BROKERS HAVE A DUTY OF CARE</i>	714
B. <i>CRIME: CHOICEPOINT AND ACXIOM</i>	716
1. ChoicePoint.....	716
2. The Crimes behind ChoicePoint	718
3. Acxiom.....	719
C. <i>LOW STANDARDS: OTHER LAX SECURITY PRACTICES</i>	722
D. <i>LOSS OF CONTROL: LOST AND STOLEN</i>	722

* J.D. candidate, Fordham University School of Law, 2007. M.A., Journalism and Mass Communications, The University of North Carolina at Chapel Hill, 1996; B.S., Computer Science and Economics, Duke University, 1987.

694	<i>FORDHAM INTELL. PROP. MEDIA & ENT. L.J.</i>	Vol. XVII
	<i>E. TWO ADDITIONAL CONSIDERATIONS</i>	723
	1. Is Harm Necessary?	723
	2. Mixed Messages from Washington	723
	III. THE TOOLS ARE MANY	725
	IV. CONCLUSION.....	726

INTRODUCTION

Eileen Goldberg was just one among 35,000 California residents to get a letter from data broker ChoicePoint telling her that her personal information had been stolen from the company.¹ But perhaps distinguishing her from most of the other recipients, Goldberg's son, Michael, works for a Los Angeles class action law firm, and Goldberg claims the dubious honor of being the first person to file an action against ChoicePoint in the data breach case.² In this class action, filed just days after she was notified and contrary to what generally has been allowed in identity theft litigation in the past, the attorneys are seeking to include both plaintiffs whose data was compromised and those whose information appears not to have been used.³ Goldberg is a member of the latter group, and her action seeks new standards for ChoicePoint and the data broker business as a whole.⁴

Like Goldberg's story, crimes involving the theft of personal information receive a great deal of media attention. Almost daily, there is a breach of some system where personal information, customer records, credit card numbers, or debit card numbers have fallen either into the wrong hands or out of the right hands.

This note attempts to classify the existing laws and rules that have been applied to unauthorized data movements by looking at

¹ Verne Kopytoff, *35,000 in State To Receive Warning Personal Information Stolen in October, Georgia Firm Says*, S.F. CHRON., Feb. 19, 2005, at A3; Patti Bond, *ChoicePoint: Plaintiffs Ready To Try New Angles*, ATLANTA J. CONST., Apr. 8, 2005, at F1.

² Bond, *supra* note 1.

³ *Id.*

⁴ *Id.*

the breadth of approaches. Part I will look at the existing laws and rules, focusing on California and Florida law, as examples of two different approaches. Part II will look at data breaches, suggesting that they can be categorized into four types (negligence, crime, low standards, and loss of control). Part III will conclude, relying on the incidents and information coming before it, that it is not yet time for a federal law on data protection, but instead that the states and the courts need time to tease out the elements that will best protect personal information. Part III will also assert that, while it is easy to see data protection as a legal and political issue, companies must assume responsibility for the protection of their customers' and clients' data if the internet economy and internet access to the traditional economy are to survive.

I. EXISTING LAWS AND RULES

A. *What Is Privacy?*

For the electronic economy to continue to grow, consumers and businesses clamor for clearly defined and responsibly executed use of personal data and associated activities. But what exactly comprises privacy and what information—held by whom—should be treated with respect for its “privacy” is a murky issue.⁵ For the sake of this Note, privacy will be defined generally as those attributes which constitute “personally identifiable information,”⁶

⁵ See, e.g., Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); see also Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

⁶ Personally identifiable information is a definition still in motion. The European Union Data Protection Directive defines “personal data” as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 art. 2(a), at 38.

The California statutes define “personal information” as:

an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

including (but not limited to) an individual's name, address, phone numbers, place of employment, credit card numbers, social security number, health records, transactional records, or any other identifying element with which another individual could act as though he were the original person. These actions could be simple and innocent, such as causing the delivery of marketing email, or nefarious and extreme, such as the range of activities that constitute identity theft.⁷ This information may be collected

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

CAL. CIV. CODE § 1798.29(e)-(f) (2006).

Florida law defines "Personal identification information" as

any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code;
4. Medical records;
5. Telecommunication identifying information or access device; or
6. Other number or information that can be used to access a person's financial resources.

FLA. STAT. § 817.568.1(f) (2005).

⁷ Some of the literature combines discussion of the breach of information and the theft of an identity, but this piece will focus on the data breach and the subsequent activity with that, regardless of what comprises the activity. For a helpful list of identity theft actions that resulted in criminal prosecution, see Lori J. Parker, Annotation, *Validity, Construction, and Application of State Statutes Relating to Offense of Identity Theft*, 125 A.L.R.5TH 537 (2005).

overtly or not in the course of business transactions, by the government, or by non-profit organizations.⁸

The right to privacy has long confused and confounded average Americans, who often presume a Constitutional right to privacy that doesn't explicitly exist.⁹ While most scholars accept that there is some sort of derived right to some sort of privacy, "the right to privacy has been poorly articulated and only vaguely theorized."¹⁰ In contrast, in many European countries national privacy laws were generally in place by the early 1990's,¹¹ with some dating back to the 1970's,¹² and a European Union Directive has been in force for more than a decade, setting minimum levels of national legislation.¹³ Additionally, the European Union has a Directive on Electronic Commerce that acts as the "legal framework" for e-commerce among member countries.¹⁴ The United States, on the other hand, relies on a "sectoral . . . mix of legislation, regulation,

⁸ Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 255–56 (2005). These "entities . . . assemble, update, manage, and use masses of computerized information relating to individuals." *Id.* at 255. Johnson further defines the data as including "names, relationships (e.g., family members and employers), contact information (e.g., phone numbers, residences, and virtual addresses), personal histories (e.g., birth dates, medical data, physical characteristics, and educational records), official identifiers (e.g., social security, driver's license, and passport numbers), and financial records (e.g., bank, credit card, frequent flyer, and investment account numbers)." *Id.* at 256.

⁹ See generally Oliver Ireland & Rachel Howell, *The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy*, 29 N.C. J. INT'L L. & COM. REG. 671, 671–74, 688–89 (2004) (tracing through the case law and outlines the major legislative elements that comprise the United States' privacy laws); see also PAUL M. SCHWARTZ & JOEL R. REIDENBERG, *DATA PRIVACY LAW* 29–90 (1996) (discussing the Constitutional Law approach).

¹⁰ Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1155 (2005).

¹¹ PETER P. SWIRE & ROBERT E. LITAN, *NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE* 23 (1998).

¹² HARRY HENDERSON, *PRIVACY IN THE INFORMATION AGE* 36 (1999) (noting that France, Germany, and Great Britain all enacted privacy regulations in the 1970's).

¹³ Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

¹⁴ Directive on Electronic Commerce, 2000 O.J. (L 178) 1. See, e.g., the European Commission's Electronic Commerce portal, available at http://europa.eu.int/comm/internal_market/e-commerce/index_en.htm (last visited Jan. 12, 2007).

and self regulation”¹⁵ in privacy regulation that is “riddled with gaps and weak spots.”¹⁶

B. Federal Privacy Laws

In the United States, legislation exists to address the use of credit reports in the form of the Fair Credit Reporting Act,¹⁷ to limit the personal information that state motor vehicle agencies can release about licensees in the Driver’s Privacy Protection Act,¹⁸ to control the information held on individuals by government agencies and how it may be disclosed in the Privacy Act of 1974,¹⁹ and to govern the disclosure of medical information in the Health Insurance Portability and Accountability Act.²⁰ The federal Computer Fraud and Abuse Act (CFAA) serves as the primary means by which unauthorized access to computer systems, including data access and theft cases, are prosecuted.²¹ Access device fraud²² and wire fraud²³ are similarly covered by federal laws. The Identity Theft Penalty Enhancement Act,²⁴ enacted in July 2004, stiffens the penalty for use of another’s identification during the commission of any of a list of more than a hundred felonies, including wire fraud, misuse of a Social Security number,

¹⁵ See U.S. Dep’t of Commerce, Safe Harbor Overview, available at http://www.export.gov/safeharbor/sh_overview.html (last visited Jan. 12, 2007). “The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin.” *Id.*; see also U.S. Dep’t of Commerce, Safe Harbor Documents, available at http://www.export.gov/safeharbor/sh_documents.html (last visited Jan. 12, 2007).

¹⁶ Daniel J. Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357 (2006) [hereinafter Solove & Hoofnagle, *Model Regime*].

¹⁷ 15 U.S.C.A. § 1681 (2006).

¹⁸ 18 U.S.C. § 2721 (2000).

¹⁹ 5 U.S.C.A. § 552a (2006).

²⁰ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified at 42 U.S.C. § 210 (2006)).

²¹ 18 U.S.C.A. § 1030 (2006).

²² 18 U.S.C.A. § 1029 (2006).

²³ 18 U.S.C.A. § 1343 (2006).

²⁴ 18 U.S.C.A. § 1028A(a)(1), (c) (2006). For an overview, see MADELEINE SCHACHTER, INFORMATIONAL AND DECISIONAL PRIVACY, PART II 199–518 (CAROLINA ACADEMIC PRESS 2003).

or passport fraud.²⁵ Other laws address similar narrowly focused issues.²⁶ But there are also wide gaps where information is not protected, and no single overriding consumer-targeted law exists that protects the information stored by companies and the government from abuse, or gives those whose information is misused or abused a personal right of action.²⁷ And that lack of a safety net is affecting the behavior of American consumers, by some estimates keeping as many as a third of those over the age of fourteen from making purchases through the internet.²⁸

C. Privacy in Online Activity

The consumer advocacy group the Privacy Rights Clearinghouse warns consumers that “[o]ften the level of privacy you can expect from an online activity will be clear from the nature of that activity. Sometimes, however, an activity that appears to be private may not be. *There are virtually no online activities or services that guarantee absolute privacy.*”²⁹ This message to consumers is reiterated every day in news headlines, highlighting the intersection between privacy and data security, and attacks on the latter that result in the loss of privacy in the former. Informational privacy has been defined as “the claim of individuals, groups, and institutions ‘to determine for themselves when, how, and to what extent information about them is communicated to others.’”³⁰ Understanding the increasing

²⁵ Sean B. Hoar, *Trends In Cybercrime: The Dark Side of the Internet*, 20-FALL CRIM. JUST. 4, 8 (2005).

²⁶ INTERNATIONAL GUIDE TO PRIVACY 15–80 (Jody R. Westby ed., 2004). See, generally, Ireland & Howell, *supra* note 9, at 674–88. There is extensive literature tracing and distinguishing the existing federal laws. See, e.g., MADELEINE SCHACHTER, *supra* note 24.

²⁷ See 18 U.S.C.A. § 1030 (2006); 18 U.S.C.A. § 1029 (2006), 18 U.S.C.A. § 1343 (2006), 18 U.S.C.A. § 1028(a)(1), (c) (2006).

²⁸ *The Online Fear Factor: Phishing and Keylogging and Fraud. Oh, My!*, EMARKETER, Mar. 14, 2006, available at <http://www.emarketer.com/Article.aspx?1003865>.

²⁹ Privacy Rights Clearinghouse, *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*, <http://www.privacyrights.org/fs/fs18-cyb.htm> (last visited Jan. 12, 2006) (emphasis in original).

³⁰ RICHARD A. GLENN, THE RIGHT TO PRIVACY: RIGHTS AND LIBERTIES UNDER THE LAW 205 (ABC-CLIO 2003) (citing ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Atheneum 1967)).

commoditization of this information, another scholar says that “information privacy is concerned with the use, transfer, and processing of the personal data generated in daily life.”³¹

Data protection and privacy are concepts conjoined both in theory and in practical application.³² The interrelatedness is that:

Security involves the protection of information, applications and operating systems, networks, and hardware and supporting equipment. If networks can be breached, information can be accessed; if applications or operating systems can be manipulated, data can be sabotaged or compromised; if information controls can be broken, then information can be stolen, disclosed, or compromised. In part, security is about protecting information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.³³

The ChoicePoint breach, disclosed in February 2005,³⁴ was a tipping point in the discussion of privacy and the revelation of data breaches, perhaps because it was of such great magnitude or perhaps because it involved criminals barely posing as legitimate data purchasers.³⁵ Since February 14, 2005, the date of the ChoicePoint disclosure, more than 100 million records containing the personal information of U.S. residents have been “compromised.”³⁶ Nearly 19 million U.S. households had some theft of personal information in 2006, in an estimated 303 incidents.³⁷ Additionally, ChoicePoint alerted the public to the massive and growing data broker business, and to the associated data transfers about consumers and their behavior which these

³¹ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004).

³² INTERNATIONAL GUIDE TO PRIVACY, *supra* note 26, at 136.

³³ *Id.* at 136.

³⁴ The Privacy Rights Clearinghouse Keeps a Tally of the Breaches Since ChoicePoint, available at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

³⁵ *See infra* Part II.

³⁶ The Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (last visited Feb. 2, 2007).

³⁷ The Identity Theft Resource Center, *2006 Disclosure of U.S. Data Incidents*, <http://www.idtheftcenter.org/breaches.pdf> (last visited Feb. 2, 2007).

companies seek and store.³⁸ One of the Acxiom profiler tools is estimated to have collected information from at least 15 million sources, covering 95 percent of American households; Experian claims to cover 98 percent of households, with potentially more than 1000 data points of information on each household.³⁹ And not only major businesses have access to their lists of households, as the price points for such data are low, as inexpensive as \$65 per 1000 names.⁴⁰

Surveys of Americans and of online consumers emphasize their concerns about the use of their information.⁴¹ “Information sharing and collection have been going on for a long time, but I think consumers are finally starting to get some awareness and they do not like it,” a Federal Trade Commission attorney presciently told a privacy panel at the University of Maine in the summer of 2001.⁴² The notion that, even without explicit laws regarding their data, responsible companies should treat information with care is steadily emerging, indeed, “[t]here are instances where there are no laws or regulations regarding the privacy or security of certain information; however, there is a public perception that disclosure of this type of data is not acceptable.”⁴³

D. Enforcement by Everyone

Data breaches and subsequent data theft or illegitimate use are covered by a haphazard series of state laws, as well as enforcement actions by Attorneys General and federal administrative agencies, especially the Federal Trade Commission. But the recent story of data security breaches in the United States is a bit of a chicken-and-egg situation. Many of the large-scale breaches which have

³⁸ See *infra* Part II.

³⁹ Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65–66 (2003).

⁴⁰ Richards, *supra* note 10, at 1157–58.

⁴¹ See Rita Heimes, *Internet Privacy Law, Policy, and Practice: State, Federal, and International Perspectives*, 54 ME. L. REV. 95 (2002).

⁴² *Id.* at 103 (reporting a panel discussion that took place June 7–8, 2001 and quoting Laura Mazzarella, attorney in the Division of Financial Practices of the Federal Trade Commission’s Bureau of Consumer Protection).

⁴³ See INTERNATIONAL GUIDE TO PRIVACY, *supra* note 26, at 156.

come to the attention of the press and the public—including the ChoicePoint incident—may be credited to legislation out of California requiring the notification of California residents whose personal information is breached.⁴⁴ Of course, breaches large and small occurred before the California legislation went into effect, and it is likely that some companies have made the decision to take the business risk of violating the California law—or more subtly deciding an incident did not cause the notification requirement to kick in—than risk the questions from those whose information was revealed who live outside of California, from regulators, stockholders; the dip in stock prices; the loss of customers and clients; and the surrounding publicity.⁴⁵ Estimates do suggest that the number of security breaches is increasing; security breaches are estimated to have occurred at between 80 and 90 percent of Fortune 500 companies and government agencies.⁴⁶

E. In the States

California was the first state to pass significant online breach notification legislation, and, though the law has been criticized for ambiguous drafting and other elements considered disadvantageous (especially to non-California-based companies), it is nevertheless setting the standard by which subsequent state legislation is being drafted.⁴⁷ The California data breach notification law was only one of several significant pieces of online- or privacy-oriented consumer protection to come out of that state's legislature recently,⁴⁸ and was the reaction to the

⁴⁴ See Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals with Id Theft: The Promise and the Problems*, BUS. L. TODAY, May/June 2004, at 37.

⁴⁵ See *id.*

⁴⁶ Alexander Frid & Jeffrey M. Rawitz, *Jones Day Commentaries: Security Breach Notification Requirements: Guidelines and Securities Law Considerations* (2006), available at http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S3225 (last visited Jan. 12, 2007).

⁴⁷ See CAL. CIV. CODE §§ 1798.29, 1798.82 (2006). For criticisms, see Paetkau & Torabian-Bashardoust, *supra* note 44.

⁴⁸ The breadth of California legislation is dizzying, covering the transfer of information to direct marketers, the publication of cell phone numbers in a directory, the use of Social Security numbers on paychecks, the downloading of spyware, using medical information about individuals to market to them, the use of data from GPS systems in rental cars, among others. Though some of the other California legislation does touch on data

hacking of a website that could have exposed all of the state's employees' Social Security numbers.⁴⁹ The hacker attack, which involved data about more than 225,000 employees, was discovered in early May.⁵⁰ However, the individuals whose data was compromised—and who included state legislators—were not notified for several weeks.⁵¹ California, which shares the dubious distinction with Washington, D.C., as the two places where the most identity theft crimes take place,⁵² is traditionally very protective of consumers, as well as the home of cutting-edge technology legislation.⁵³ In a nod to the fact that not all data is held in electronic format, the legislature has considered expanding the statute to include non-electronic data.⁵⁴

1. California

The California law, the Security Breach Information Act, was drafted, passed, and signed by Governor Gray Davis within four months.⁵⁵ The law, which went into effect July 1, 2003, defines the personal information at issue as a person's first name (or first initial) and last name in combination with either the person's Social Security number; driver's license number or California

privacy and information security, this piece focuses on the issue of breaches, and as such is concerned only with CAL. CIV. CODE §§ 1798.29 and 1798.82. For the other legislation, see David Bender, *Privacy Developments-2005*, 11th Annual Institute on Intellectual Property Law, 842 PLI/PAT 9 (2005) [hereinafter Bender, *Privacy Developments*]; Barbara L. Delaney et al., *California Privacy and Security Legislation Affects Entire Nation*, 3 INTELL. PROP. & TECH. L.J. 21 (2005); Chad C. Coombs & Keenen Milner, *New California Identity Theft Legislation*, L.A. LAWYER 21 (2004); Paetkau & Torabian-Bashardoust, *supra* note 44.

⁴⁹ See Robert Lemos, 'Perfect Storm' for New Privacy Laws?, CNETNEWS.COM, Mar. 1, 2005, available at http://news.com.com/Perfect+storm+for+new+privacy+laws/2100-1029_3-5593225.html.

⁵⁰ See *id.*

⁵¹ See *id.*

⁵² Coombs & Milner, *supra* note 48, at 21.

⁵³ See generally Delaney et al., *supra* note 48.

⁵⁴ Kenneth M. Dreifach, *Data Privacy, Web Security, and Attorney General Enforcement*, 6th Annual Institute on Privacy Law: Data Protection—The Convergence of Privacy & Security, 828 PLI/PAT 401, 420.

⁵⁵ Lemos, *supra* note 49. For more of the history of the passage of the California, see Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 14–39 (2003).

Identification Card number; account number; credit or debit card number, in combination with any code that would permit access to a financial account and that isn't available to the general public from government records.⁵⁶ It is not necessary that both elements be unencrypted; either an unencrypted name or data would trigger the statute.⁵⁷ The definition of a breach is one of the elements that is controversial—the “unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person[.]”⁵⁸ without regard for whether the information was actually used. The California law applies to both private and governmental entities.⁵⁹ It additionally allows for a private civil action by anyone harmed by a breach, and the law places no limits on other claims under unfair business practices or misrepresentation (regarding the privacy policies in place, for example).⁶⁰

The California law also specifies how a company must alert customers of the breach, and, in one of the most criticized aspects of the law, an ambiguously drafted statement of how quickly the notification must take place.⁶¹ The disclosure must take place within “most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement[.]”⁶² Notice must be written; or electronic in accordance with 15 U.S.C. § 7001 (concerning electronic records and signatures); or may be a sort of substitute notice, if the cost of notice exceeds \$250,000 or that the number of people who must be notified is more than 500,000 or if their contact information is incomplete.⁶³ Substitute notice requires email for those the entity has email for; “[c]onspicuous posting of the notice on the agency’s Web site page, if the agency maintains one”; and “[n]otification to major

⁵⁶ CAL. CIV. CODE § 1798.29(e)–(f) (2006).

⁵⁷ *Id.* § 1798.29(e).

⁵⁸ CAL. CIV. CODE § 1798.82(a) (2006).

⁵⁹ *Id.* § 1798.29 (applying to any person or business); *id.* § 1798.82 (applying to any California state agency); *see also* Dreifach, *supra* note 54, at 419.

⁶⁰ Cheryl A. Falvey et al., *Disclosure of Security Breaches Required by New California Privacy Legislation*, METRO. CORP. COUNS., Aug. 2003, at 5.

⁶¹ CAL. CIV. CODE § 1798.29(a) (2006).

⁶² *Id.*

⁶³ *Id.* § 1798.29(g).

statewide media.”⁶⁴ If the breaching entity has an “information security policy” that states how and how quickly it will notify customers of a breach, and that policy is not in conflict with the California law, following that policy will suffice as complying with the timely notification aspects of the statute.⁶⁵

2. Florida

In a tale that is indicative of the conflict of openness of records and the call for increasing privacy, Florida government officials find themselves struggling to follow two seemingly contradictory pieces of legislation—one which requires county recorders to make available online a wide variety of public records, and another (set to be enforced as of January 1, 2008, a deadline that has been extended twice⁶⁶) that limits the personal information placed online.⁶⁷ The old law meant that Social Security numbers, birth dates, driver’s license information, passport numbers, green card information, images of signatures, and bank account numbers of current and former Florida residents were to be put online if they were part of a public record, making the owners of the information extremely vulnerable to identity theft; the new law mandates the removal of “Social Security numbers, bank account numbers, and credit and debit card numbers” from online public records.⁶⁸ The issue initially rose in Broward County in the spring of 2006, but the data in question has been online since 1999, according to that county’s director of records, who claims that the Broward exposure is repeated around the country as local governments followed policies to allow internet access to public records.⁶⁹

Florida has another law that addresses the data security of individuals under the criminal code, and is a useful contrast to the

⁶⁴ *Id.* § 1798.29(g)(3).

⁶⁵ *Id.* § 1798.29(h).

⁶⁶ Monica Hatcher, *Public Records Easy Targets for ID Thieves*, MIAMI HERALD, Aug. 27, 2006, at A1.

⁶⁷ Jaikumar Vijayan, *Update: Fla. Residents’ Data Exposure a Statewide Issue*, COMPUTERWORLD, Apr. 11, 2006, <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,110389,00.html>.

⁶⁸ *Id.*

⁶⁹ *Id.*

California law.⁷⁰ Passed after the ChoicePoint breach, the amendments to the “Criminal Use of Personal Identification Information” statute went into effect July 1, 2005,⁷¹ and prescribe criminal penalties for misusing others’ information,⁷² including that of dead people.⁷³ The Florida statute focuses on the criminal aspect of data breaches, with the misuse quickly becoming a felony.⁷⁴

Florida requires that the victim “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person,” be notified “without unreasonable delay . . . [usually] no later than 45 days following the determination of the breach.”⁷⁵ A company’s failure to notify may invoke a fine of up to \$500,000 per breach,⁷⁶ but the statute exempts governmental agencies unless they have contracted with a third-party to provide “governmental services,” in which case the third-party can be liable for the fine without the ability to bill back to the governmental agency.⁷⁷ For third parties holding data for businesses, breaches must be reported within ten days, or penalties start to kick in.⁷⁸ In Florida, “breach” means “unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information.”⁷⁹ Victim notification provisions are very similar to those in the California law,⁸⁰ with law enforcement⁸¹ and data protection policy carve-outs.⁸² But unlike California, if the data of more than 1000 people is involved in a breach, the company must notify “all consumer reporting agencies that compile and maintain

⁷⁰ Compare FLA. STAT. § 817.568 (2005), with CAL. CIV. CODE § 1798.29(e).

⁷¹ H.R. 481, 2005 Leg., 107th Reg. Sess. (Fl. 2005).

⁷² See, e.g., FLA. STAT. § 817.568(2) (2005).

⁷³ FLA. STAT. § 817.568(8)(a) (2005).

⁷⁴ See, e.g., FLA. STAT. ANN. § 817.568(2).

⁷⁵ FLA. STAT. § 817.5681(1)(a) (2005).

⁷⁶ FLA. STAT. § 817.5681(1)(b) (2005).

⁷⁷ See FLA. STAT. § 817.5681(1)(d).

⁷⁸ FLA. STAT. § 817.5681(2)(a).

⁷⁹ FLA. STAT. § 817.5681(4).

⁸⁰ Compare FLA. STAT. § 817.5681(6), with CAL. CIV. CODE § 1798.29(g) (2006).

⁸¹ Compare FLA. STAT. § 817.5681(3), with CAL. CIV. CODE § 1798.29(c) (2006).

⁸² Compare FLA. STAT. § 817.5681(9), with CAL. CIV. CODE § 1798.29(h) (2006).

files on consumers on a nationwide basis.”⁸³ There is also the addition of a clause that “notification is not required if, after an appropriate *investigation or after consultation with relevant federal, state, and local agencies* responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed.”⁸⁴

3. Other State Laws

The California and Florida laws are now just two among the many laws in an increasing list. As of July 2006, state security breach laws were in effect in at least thirty-three states: Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia (covers data brokers only), Hawaii, Idaho, Illinois, Indiana (covers state agencies only), Kansas (took effect Jan. 1, 2007), Louisiana, Maine (applies to information brokers only), Minnesota (law does not apply to financial institutions or HIPAA-covered institutions), Montana, Nebraska, Nevada, New Hampshire (took effect Jan. 1, 2007), New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma (covers state agencies only), Pennsylvania, Rhode Island (does not include HIPAA-covered institutions), Tennessee, Texas, Utah (took effect Jan. 1, 2007), Washington, and Wisconsin.⁸⁵ An additional protection for the individual is the ability to act on the information that one’s identity could be endangered. By summer 2006, according to the Public Interest Research Group, twenty-five states had legislation that allows or would be in force to allow consumers to place security freezes on their credit reports.⁸⁶ Five of those states require that the consumer be a victim of identity theft (Hawaii, Kansas, South Dakota, Texas and Washington, with Washington including

⁸³ FLA. STAT. § 817.5681(12).

⁸⁴ FLA. STAT. § 817.5681(10)(a) (emphasis added). “Such a determination must be documented in writing and the documentation must be maintained for 5 years.” *Id.*

⁸⁵ See *State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, <http://pirg.org/consumer/credit/statelaws.htm> (last visited Feb. 11, 2007) (maintaining a relatively up-to-date list of the status of state legislation on security breach notification and freeze laws and links to most of the state legislation).

⁸⁶ *Id.*

consumers who have received notice of a breach).⁸⁷ The other twenty states are California, Colorado, Connecticut, Delaware, Florida, Illinois, Kentucky, Louisiana, Maine, Minnesota, Nevada, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Rhode Island, Utah, Vermont and Wisconsin.⁸⁸ This is an increase over the twelve states that had laws in place that let consumers restrict access to credit reports as of January 2006, and up from four states with security freeze laws in place as of January 2005.⁸⁹

Factors that differentiate the state laws include: whether the breach victim must be notified in all cases or only in the case of risk of some level or of actual harm;⁹⁰ if a credit-reporting agency must also be notified, and if so at what threshold of records;⁹¹ what constitutes personal information covered by the law (and whether it must be electronic in format);⁹² whether there is an individual right of action or if the state Attorney General's office or another governmental entity must act;⁹³ who must comply with the law (for instance, must governmental agencies comply at the same level as private enterprise, does the storage with a third party change the application of the breach notification, who is the target of the notification, etc.);⁹⁴ whether the law addresses civil or criminal repercussions;⁹⁵ what opt-outs for federally covered information exist (such as the Health Information Portability and Accountability Act (HIPAA) or the Graham-Leach-Bliley Act (GLBA));⁹⁶ if there is an associated ability to freeze access to

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ *See, e.g.*, FLA. STAT. § 817.5681(12).

⁹² DOUG MARKIEWICZ, VIGILANTMINDS, STATE SECURITY BREACH LEGISLATION 4-5 (2006), http://www.vigilantminds.com/files/vigilantminds_state_security_breach_legislation_whitepaper.pdf (last visited Jan. 10, 2007).

⁹³ *See, e.g.*, FLA. STAT. § 817.5681(11).

⁹⁴ *See, e.g.*, FLA. STAT. § 817.5681(10)(c).

⁹⁵ *Compare* FLA. STAT. § 817.568 (LexisNexis 2005) (providing criminal penalties), *with* FLA. STAT. § 817.5681 (providing administrative fines).

⁹⁶ *See State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, <http://pirg.org/consumer/credit/statelaws.htm> (last visited Feb. 11, 2007); *see also* Kaustuv M. Das, *Data Breach Notification Laws: The Changing Landscape in Early*

credit reports (this is often found in separate statute, but also has several variants, such as whether the individual must have had their identity stolen before the freeze can take place or if the freeze may be prophylactic);⁹⁷ how much and what sorts of effort must be made to notify those whose information is breached;⁹⁸ and how quickly that notification must take place.⁹⁹ Additionally, some of the legislation interacts with old state statutes on unfair competition.¹⁰⁰ It is also unclear how state laws will interact with the Fair Credit Reporting Act and parts of the GLBA.¹⁰¹

The requirement of some level of risk of use of the information is not present in the California law, meaning that the breach without any level of harm or risk of harm is in and of itself actionable, and this is one of the elements that makes it one of the toughest state laws.¹⁰² Levels of risk of use of the data required for the statutes to kick in vary among the states, with no requirement at all of any consideration of harm, to “reasonable” or even “significant” risk and harm, injury, or loss all being among the issues considered.¹⁰³ Notification speed is generally vague, with the exception of Florida and Ohio, which require notification within forty-five days and New York, which specifies that state agencies must notify potential victims within 120 days.¹⁰⁴

The definition of personal information¹⁰⁵ also varies widely (mother’s maiden name, for instance, is personal information

2006, DAVIS WRIGHT TREMAINE ADVISORY BULLETIN, Mar. 2006, available at http://www.dwt.com/practc/privacy/bulletins/03-06_DataBreach.htm.

⁹⁷ See *id.*

⁹⁸ See MARKIEWICZ, *supra* note 92, at 5–6.

⁹⁹ *Id.* at 6–7, Table 1 (comparing some of these and other attributes of the state laws).

¹⁰⁰ See Das, *supra* note 96.

¹⁰¹ See Solove & Hoofnagle, *Model Regime*, *supra* note 16, at 380. “Most privacy protections in America have been created by state legislatures.” *Id.* at 381. Solove and Hoofnagle suggest that federal privacy legislation should focus on “‘floor preemption,’ thereby allowing states to innovate more comprehensive protections for individual rights.” *Id.*

¹⁰² See Patti Waldmeir, *Federal data security law reaches turning point in Congress*, FT.COM, Apr. 13, 2006, available at <http://www.ft.com/cms/s/49315c58-ca6b-11da-852f-0000779e2340.html>.

¹⁰³ MARKIEWICZ, *supra* note 92, at Table 1; see also Das, *supra* note 100.

¹⁰⁴ MARKIEWICZ, *supra* note 92, at Table 1; see also Das, *supra* note 100.

¹⁰⁵ See *supra* note 6 and accompanying text.

according to laws in North Carolina and North Dakota¹⁰⁶), as does the requirements for the information's encryption, with some state laws including a "encrypted data safe harbor" for data that is safely encrypted.¹⁰⁷ In California, the statute comes into play only when the data is not encrypted, but other statutes require notification if the encryption is broken or the encryption key compromised.¹⁰⁸

Who owns enforcement and administration varies, too; the Florida Department of Legal Affairs collects fines and institutes proceedings for the civil penalties, while the criminal penalties are handled by that state's criminal division.¹⁰⁹

F. Congress to the Rescue?

After ChoicePoint, it appeared that Congress might act fast to pass federal data breach notification legislation, but the topic has been mired by a variety of different approaches—reflecting the variety of approaches by the states.¹¹⁰ Legislation has been proposed and publicized by high-profile lawmakers, among them California Democratic Sen. Dianne Feinstein, Vermont Democratic Sen. Patrick Leahy, and Pennsylvania Republican Sen. Arlen Specter.¹¹¹ Feinstein's bill is very similar to the California law, and interacts with existing state laws by serving as a floor, allowing the states to go above her proposed legislation, and explicitly allows for the Federal Trade Commission to impose civil remedies.¹¹²

At least eighteen bills have been introduced in House and Senate committees, but the issues raised by proposed legislation are difficult, and influential lobbies have vested interests in the outcomes (banking and financial concerns among them).¹¹³ For example, allowing consumers to freeze access to their credit reports is proving controversial. In March 2006, the House

¹⁰⁶ MARKIEWICZ, *supra* note 92, at Tbl. 1.

¹⁰⁷ *Id.*

¹⁰⁸ CAL. CIV. CODE § 1798.29(a) (2006); MARKIEWICZ, *supra* note 92, at tbl.1 n.8.

¹⁰⁹ FLA. STAT. § 817.5681(11) (2005).

¹¹⁰ *See* Das, *supra* note 100.

¹¹¹ *See* Lemos, *supra* note 49.

¹¹² *See* Skinner, *supra* note 55, at 62.

¹¹³ *See* Waldmeir, *supra* note 102; Das, *supra* note 100.

Financial Services Committee passed a bill with a credit freeze provision; several members who voted for the bill in committee said they would need to revisit that aspect if it went before a full House vote.¹¹⁴ On the federal level, the already-complicated elements considered by the state legislation above take on even more dimensions. Other controversial issues include how a federal law would interact with the existing federal laws, chief among them the Graham-Leach-Bliley Act (GLBA).¹¹⁵

In what may be the best chance for federal legislation, in February 2007, Leahy and Sen. Bernie Sanders, an Independent from Vermont, introduced The Personal Data Privacy and Security Act of 2007, a bill similar to one Specter and Leahy sponsored in 2005.¹¹⁶ The first version was considered by the Senate Judiciary Committee, but “languished on the Senate calendar for more than a year.”¹¹⁷ The 2007 bill as proposed has notice provisions, provides for criminal recourse for improper access to “sensitive personally identifiable information” (by amending the computer fraud statute, 18 U.S.C. § 1030 (a)(2)), and allows consumers to request from data brokers the information on file, and to correct any inaccuracies.¹¹⁸

The proposed bill has carve-outs for information covered by GLBA and HIPAA, for law enforcement need, for fraud-prevention technologies, and for marketing data.¹¹⁹ Companies holding information on more than 100,000 Americans would be required to have data privacy and security programs.¹²⁰ Notice is required when the risk of harm is “significant,” and there are criminal penalties for intentionally concealing a breach that would

¹¹⁴ See Stacy Kaper & Rob Blackwell, *Data Bill Moves Along, And So Does Freeze Fight*, AMERICAN BANKER, Mar. 17, 2006, at 1.

¹¹⁵ See Das, *supra* note 96.

¹¹⁶ Statement Of Senator Patrick Leahy, Chairman, Committee On The Judiciary, On The Introduction Of The Leahy-Specter Personal Data Privacy And Security Act Of 2007, Feb. 6, 2007, available at <http://leahy.senate.gov/press/200702/020607.html> (last visited Feb. 14, 2007).

¹¹⁷ *Id.*

¹¹⁸ The Personal Data Privacy and Security Act of 2007, available at <http://www.epic.org/privacy/pdsa2005.pdf> (last visited Feb. 14, 2007).

¹¹⁹ *Id.*

¹²⁰ *Id.*

require notice. In an interesting and gentle nod to data brokers, the bill asserts that “[d]ata brokers have assumed a significant role in providing information, authentication, and screening services, and related data collection and analyses for commercial, nonprofit, and government operations.”¹²¹

The bill limits “[s]ensitive personally identifiable information” to “electronic or digital form.”¹²² “Sensitive personally identifiable information” is defined as first name or first initial and last name with any one of “Social Security number, driver’s license number, passport number, or alien registration number” or with two of “home address or telephone number; mother’s maiden name, if identified as such; month, day, and year of birth.”¹²³ Additionally, “biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation,” any account number and associated code or password that can be used to obtain anything of value, or a financial account number and any code needed to get funds or credit also constitute “[s]ensitive personally identifiable information.”¹²⁴

Another option to use federal law to address the issues of privacy would be to strengthen existing legislation, such as addressing some of the opt-outs in the GLBA.¹²⁵ Possible opt-outs that could be limited include the exemptions from notification about information sharing that results from customer requests, or account maintenance, or when the sharing is among the financial institution’s affiliates or partners with whom it has agreements in place.¹²⁶ Including data brokers such as Acxiom, Experian and ChoicePoint under the purview of the GLBA is another option, as the data broker industry is largely unregulated.

Commentators and privacy experts alike worry that notification may have the opposite effect from that intended: the desensitization of consumers. “[O]ver-notification anaesthetizes people because they feel, this happens all the time, and I didn’t get

¹²¹ *Id.* § 2, Findings.

¹²² *Id.*

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ Ireland & Howell, *supra* note 9, at 681–82.

¹²⁶ *Id.*

hurt by it,” said a senior executive at data security firm RSA Security, which is advocating federal legislation.¹²⁷ Acxiom’s chief privacy officer, Jennifer Barrett, who supports a notification bill based on a risk of identity theft, shares the concern.¹²⁸ “It’s called a cry wolf syndrome,” she said in 2005. “Cry wolf too many times and people won’t listen.”¹²⁹

II. BREACHES

A look at some of the major security breaches from the past few years serves to highlight both the existing remedies that are being utilized and the room for improvement and experimentation. This discussion is by no means exhaustive, and suffers from inconsistent news reporting on criminal trials and a lack of access to lower court decisions and actual charges brought. Companies and institutions—especially publicly traded ones, or ones reliant on the public’s trust—who have experienced a breach and are working with law enforcement have, despite the growing number of data breach notification laws, incentives to reduce the attention on the breach, the questions it raises about their data policies, and the extent to which customer, client, or student information has been exposed. This section will categorize personal information data breaches, offering illustrations of each category: negligence, crime, low standards, and loss of control. An attempt to establish a taxonomy of breaches is important in assuring that emerging legislative, administrative, and industry rules are properly covering the breadth of the issues. Additionally, it is important to note that in many cases there is a duality of the approach to punish both the data attacker and the company that allowed the attack, as illustrated in the Amy Boyer and ChoicePoint cases.

¹²⁷ Waldmeir, *supra* note 102.

¹²⁸ Chip Taulbee, *Acxiom Lets Congress Know Opinion of Privacy Proposals*, ARK. BUS., Apr. 25, 2005, available at 2005 WLNR 8154023 [hereinafter Taulbee, *Acxiom Lets Congress Know*].

¹²⁹ *Id.*

A. Negligence: Data Brokers Have a Duty of Care

Highlighting much of the consumer discomfort about what information data brokers hold, how they hold it, and where they got it from is a 1999 case from New Hampshire.¹³⁰ Liam Youens was obsessed with a former high school classmate, Amy Boyer, and kept a log on a website of his efforts to find her so he could kill her.¹³¹ He knew her address, but not where she worked, so he turned to the information broker Docusearch.com.¹³² “It’s actually [sic] obscene [sic] what you can find out about a person on the internet,” he wrote on his website.¹³³ Docusearch had subcontractors working for the company, and provided one of them, Michele Gambino, with Boyer’s Social Security number and more. Gambino called Boyer or her mother, and, posing as an insurance company employee with a refund for overpayment, got Boyer’s work address from her.¹³⁴ This practice is called “pretexting,” and some forms of it were made illegal by the GLBA.¹³⁵ For Boyer, it was too late; on October 15, Youens drove by as she was getting in her car to leave work and shot eleven bullets into her head and upper body before turning the gun on himself.¹³⁶ Docusearch charged Youens \$45 for Boyer’s Social Security number, and \$109 for her work address.¹³⁷ After Boyer’s murder, a New Hampshire Senator introduced “Amy Boyer’s Law,” which would limit the use of Social Security numbers.¹³⁸ Ironically, privacy advocates and industries attacked the legislation, which did not become law.¹³⁹

¹³⁰ *Remsburg v. Docusearch, Inc.*, 2002 U.S. Dist. LEXIS 7952 (D.N.H. Apr. 25, 2002).

¹³¹ *Securing Electronic Personal Data Before the S. Comm. on the Judiciary*, 109th Cong. (2005) (statement of Robert Douglas, CEO of PrivacyToday.com).

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.* See also Electronic Privacy Information Center, *The Amy Boyer Case*, <http://epic.org/privacy/boyer/> (last visited Jan. 10, 2007) (providing a background of the case and the relevant claims) [hereinafter *The Amy Boyer Case*].

¹³⁵ See 15 U.S.C. § 6821 (2006). See also *The Amy Boyer Case*, *supra* note 134.

¹³⁶ Testimony of Robert Douglas, *supra* note 131.

¹³⁷ *The Amy Boyer Case*, *supra* note 134.

¹³⁸ Lemos, *supra* note 49.

¹³⁹ *Id.*

The Boyer case is not the only situation in which data brokers have given out information to stalkers resulting in tragic consequences; actress Theresa Saldana was stabbed and slashed in March 1992 by a stalker who got her home address from a private investigator who called Saldana's mother impersonating Martin Scorsese's assistant, and claiming to be looking for Saldana to discuss a role.¹⁴⁰

In 1989, actress Rebecca Schaeffer was murdered by a stalker who got her home address from a private investigator using the California motor vehicles database.¹⁴¹ The Schaeffer case is credited with sparking the passage of the Drivers' Privacy Protection Act.¹⁴² Prior to the passage of that law, states had made millions of dollars auctioning off their motor vehicle and driver's license records. Colorado earned about \$4.4 million, Florida's price was \$33 million, and New York made \$17 million in a year.¹⁴³

The Boyer case, however, was different from the Schaeffer incident in that Amy Boyer's mother, on behalf of her estate, sued Docusearch and the subcontractor Gambino. The New Hampshire Supreme Court said in February 2003 that data brokers and private investigators have a legal duty to exercise reasonable care if the information they sell about a person creates a risk, and that stalking and identity theft constitute foreseeable harms that would give rise to this duty.¹⁴⁴ "This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information[.]" the court said.¹⁴⁵

In what EPIC called "a significant expansion of privacy protection" exceeding Gramm-Leach-Bliley's provisions,¹⁴⁶ the New Hampshire Supreme Court said that the state's Consumer

¹⁴⁰ Testimony of Robert Douglas, *supra* note 131.

¹⁴¹ *Id.* (noting that the Shaeffer murder led to the passage of the Drivers Privacy Protection Act).

¹⁴² Solove & Hoofnagle, *Model Regime*, *supra* note 16, at 376.

¹⁴³ Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1150 (2002).

¹⁴⁴ *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1004-05, 1007 (N.H. 2003).

¹⁴⁵ *See id.* at 1008.

¹⁴⁶ EPIC Litigation Docket, available at <http://www.epic.org/privacy/litigation/> (last visited Jan. 7, 2007).

Protection Act allows a private cause of action by the individual who was deceived against a private investigator or information broker for damages caused by the sale of information obtained by a pretextual phone call.¹⁴⁷ The court also said that getting an individual's Social Security number from a credit reporting agency without the person's knowledge or permission and selling it to a client may also provide a cause of action for damages.¹⁴⁸

B. Crime: ChoicePoint and Acxiom

1. ChoicePoint

Choicepoint is perhaps the world's biggest data broker, holding 19 billion records in its databases, many of which have come from smaller data brokers that it has bought during its first seven years in business.¹⁴⁹ In its second significant breach, but the first to receive massive media attention, the commercial data aggregator ChoicePoint reported that 50 business clients to whom it had been selling data were not who they claimed but instead fraudulent entities set up entirely to collect data, and that the data the businesses received had been used in about 50 cases of identity theft.¹⁵⁰ The first breach, in 2002, involved about \$1 million of fraud "in the form of identity theft."¹⁵¹ In the later breach, early reports put the number of consumers affected at 145,000, but the Federal Trade Commission said that the number reached more than 160,000.¹⁵² A 2003 California law requiring the notification of

¹⁴⁷ See *Remsburg*, 816 A.2d at 1005, 1010–11.

¹⁴⁸ See *id.* at 1004–05.

¹⁴⁹ Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1 [hereinafter Zeller, *Breach Points Up Flaws*]. See also Bender, *Privacy developments*, *supra* note 48, at n.15. This data includes "current and previous address, credit data, employment history, motor vehicle data, police data, assets, insurance claims, and professional license data."

¹⁵⁰ Bender, *Privacy Developments*, *supra* note 48; Tom Zeller Jr., *U.S. Settles with Company on Leak of Consumers' Data*, N.Y. TIMES, Jan. 27, 2006, at C3 [hereinafter Zeller, *U.S. Settles*]. A ChoicePoint official disagreed with the claims of 800 identity thefts, saying the number he was aware of was sixteen. *Id.*

¹⁵¹ Bender, *Privacy Developments*, *supra* note 48.

¹⁵² Zeller, *U.S. Settles*, *supra* note 150. An additional 17,000 people were notified in November 2005 that their data was included. Solove & Hoofnagle, *Model Regime*, *supra*

breaches by companies holding information on California residents is credited with bringing the breach to light.¹⁵³ Initially, the company at first notified only the 35,000 California residents whose data might have been compromised; when questions arose about other state residents, the company was forced to reveal the breadth of the issue.¹⁵⁴

The ChoicePoint breach also brought to the public's attention the data broker industry, and "invited a national debate."¹⁵⁵ Indicative of the growing broker business, ChoicePoint numbers among its clients "insurance agencies and corporate employee screeners, check-cashing companies, media outlets . . . , private investigators, law enforcement officials and even the United States government" as well as offering inexpensive public records information to everyone.¹⁵⁶ The data is used for background checks for employers, tenant and drug screenings, checking for mortgage fraud, and searching for shareholders.¹⁵⁷

The FTC fined the Alpharetta, Georgia, based ChoicePoint \$10 million and required the company to set aside a \$5 million fund for consumer compensation.¹⁵⁸ The FTC complaint said that ChoicePoint failed to notice "obvious red flags" in applications from the fraudulent businesses.¹⁵⁹ Because the data included highly regulated credit history data, the company was potentially in violation of the Fair Credit Reporting Act, though the FTC settlement is not an acknowledgement of any wrongdoing.¹⁶⁰

Other class-action suits have been filed in addition to the Goldberg class-action suit mentioned above. In at least two of them, the would-be plaintiffs claim that ChoicePoint, which spun off from Equifax, was indeed a consumer reporting agency, and

note 16, at 358 n.1 (citing Michael Hiltzik, *Big Data Broker Eyes DMV Records*, L.A. TIMES, Dec. 1, 2005, at C1).

¹⁵³ Amanda Bronstad, *ChoicePoint Case Highlights Evolution of Identity Theft*, L.A. BUS. J., Sept. 19, 2005, at 6.

¹⁵⁴ Zeller, *Breach Points Up Flaws*, *supra* note 149.

¹⁵⁵ See generally, Solove & Hoofnagle, *Model Regime*, *supra* note 16, at 368.

¹⁵⁶ Zeller, *Breach Points Up Flaws*, *supra* note 149.

¹⁵⁷ Bronstad, *supra* note 153.

¹⁵⁸ Zeller, *U.S. Settles*, *supra* note 150.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

hence should be governed by the federal and state laws that apply to that industry, especially the ones that require a company to be certain of the other entities to which it is selling data.¹⁶¹

2. The Crimes behind ChoicePoint

What took place in the ChoicePoint case was a modern version of the classic dumpster diving schemes, where thieves would look through garbage for information with which to open new credit lines. Starting in March 2000, the brother-sister duo of Adedayo and Bibiana Benson opened a series of accounts with ChoicePoint, and used those accounts to get thousands of identifying numbers from ChoicePoint.¹⁶² The Bensons, as well as at least one other man, obtained credit data from ChoicePoint, after opening accounts using forged business documents.¹⁶³

The Bensons then opened credit and bank accounts, including cell phone accounts, using the names of the people ChoicePoint had released to them.¹⁶⁴ They also resold the data to others.¹⁶⁵ Bibiana was charged in 2002, and her brother in late 2004; the cases ended in March 2005, and both are serving federal prison sentences of more than four years each.¹⁶⁶ The other man, Olatunji Oluwatosin, was charged in August 2005 of operating similar schemes and was sentenced to ten years in prison and \$6.5 million in restitution.¹⁶⁷ Oluwatosin pleaded guilty to “conspiracy to commit computer access fraud and grand theft.”¹⁶⁸

ChoicePoint has been criticized for the delay in revealing the breach, as well as the fact that the company was giving data out based merely on the applicant having a business license; the company claims it has changed this practice and now has agents

¹⁶¹ Bond, *supra* note 2.

¹⁶² Bronstad, *supra* note 153.

¹⁶³ *Id.*

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

¹⁶⁶ *Id.*

¹⁶⁷ *Business Briefs: Identity Theft Results in a 10-Year Sentence*, N.Y. TIMES, Feb 11, 2006, at C2.

¹⁶⁸ *Id.* There is mention of at least one more defendant in the case, an “Encino man,” but he is not named in news reports. *See* Bronstad, *supra* note 153.

visit businesses before the company reveals “sensitive personally identifiable information.”¹⁶⁹

There is an additional irony in this particular breach: ChoicePoint is only one among several commercial data brokers who work with the government and law enforcement agencies to aggregate data.¹⁷⁰ But ChoicePoint’s breach raises many questions about the sorts of information and how much access government entities have to data stored at these brokers.¹⁷¹

These issues, which include the security of the access to the databases, the protocols in place for the government employees who have access to the information—estimated to include tens of thousands of federal law enforcement agents¹⁷²—and the breadth of the information itself, have been the subject of Electronic Privacy Information Center requests under the Freedom of Information Act (FOIA).¹⁷³ The FOIA requests include ChoicePoint, but also cover LexisNexis, Experian, Dun & Bradstreet, and Database Technologies Online.¹⁷⁴ The requests have revealed that security measures in place tend to favor the protection of the agencies, not the individuals whose information the databases are housing.¹⁷⁵

3. Acxiom

At Acxiom, one hacker led authorities to another, much more nefarious one. Federal authorities said that Daniel Baas of Milford, Ohio, was just “hacking for kicks” when he intruded into the company’s systems and took millions of records on individuals,

¹⁶⁹ Bronstad, *supra* note 153.

¹⁷⁰ See Chris Jay Hoofnagle, *Big Brother’s Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT’L L. & COM. REG. 595, 599 (2004) [hereinafter Hoofnagle, *Big Brother’s Little Helpers*].

¹⁷¹ See *id.* at 599–618.

¹⁷² *Id.* at 607.

¹⁷³ See *id.* at 595–600. See also <http://www.epic.org/privacy/choicepoint/> (last visited Jan. 8, 2007) for the documents which have been released and for the status of the pending requests.

¹⁷⁴ Hoofnagle, *Big Brother’s Little Helpers*, *supra* note 170, at 599.

¹⁷⁵ *Id.* at 610.

which he stored on disks he kept at his home.¹⁷⁶ Baas was working as a systems administrator for one of Acxiom's clients, Cincinnati's Market Intelligence Group, when he downloaded about 300 passwords, including an administrative one, and accessed data from other Acxiom customers from December 2002 to January 2003.¹⁷⁷ In March 2005, Baas started serving a forty-five month federal prison sentence for the intrusions, which were estimated to cost Acxiom \$5.8 million.¹⁷⁸

But in the discovery for their prosecution of Baas, investigators found a trail left by Scott Levine, whose theft of more than one billion records eclipsed Baas' activities.¹⁷⁹ From about January through July 2003, Levine got access to an Acxiom server by using what the Department of Justice called "sophisticated decryption software" to illegally obtain passwords.¹⁸⁰

Levine who is alternatively described as an "online advertiser"¹⁸¹ and the owner of a "corporation engaged in the business of distributing advertisements over the Internet to email addresses[,]"¹⁸² had a previous run-in with the Securities and Exchange Commission, which alleged he sold unregistered securities targeted at Florida's senior citizens.¹⁸³ At the time of the Acxiom breach, Levine was the owner of Boca Raton, Florida-based Snipermail.com, a bulk emailer.¹⁸⁴ One news report said that his initial access came from a client Snipermail and Acxiom had in common who gave his company the FTP password.¹⁸⁵

¹⁷⁶ *Acxiom Case Sends Message (Commentary)*, ARK. BUS., Feb. 27, 2006 [hereinafter *Acxiom Case Sends Message*]; Chip Taulbee, *Trial To Rehash Acxiom's, Hackers Past*, ARK. BUS., July 11, 2005, available at 2005 WLNR 12588914 [hereinafter Taulbee, *Trial To Rehash*].

¹⁷⁷ Taulbee, *Trial To Rehash*, *supra* note 176.

¹⁷⁸ *Acxiom Case Sends Message*, *supra* note 176; Taulbee, *Acxiom Lets Congress Know*, *supra* note 128.

¹⁷⁹ *Acxiom Case Sends Message*, *supra* note 176. See also Press Release, Dep't of Just., Former Officer of Internet Company Sentenced in Case of Massive Data Theft from Acxiom Corporation (Feb. 22, 2006), 06-088, available at 2006 WL 416250 [hereinafter Press Release, Dep't of Just.].

¹⁸⁰ Press Release, Dep't of Just., *supra* note 179.

¹⁸¹ *Acxiom Case Sends Message*, *supra* note 176.

¹⁸² Press Release, Dep't of Just., *supra* note 179.

¹⁸³ Taulbee, *Trial To Rehash*, *supra* note 176.

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

Using that password, he and other Snipermail employees were able to access other files from other Acxiom clients, and then ran programs to decrypt other usernames and passwords.¹⁸⁶ In the end, Levine and Snipermail stole more than eight gigabytes of information, some of which was resold to other Snipermail client “spammers[,]” making his entry a peer among the larger known intrusions.¹⁸⁷

Levine’s download and subsequent resale of those records led to his conviction in an August 2005 jury trial on “120 counts of unauthorized access of a protected computer, two counts of access device fraud, and one count of obstruction of justice,” for which he was sentenced to ninety-six months in federal prison.¹⁸⁸ Acxiom estimated that the Levine intrusion cost the company at least \$7 million.¹⁸⁹ Acxiom’s data security methodologies were also criticized widely after the breach and the stock price suffered.¹⁹⁰

In 2005 testimony in front of a Congressional committee considering federal privacy regulation, Acxiom’s privacy officer said that none of the files accessed in either breach resulted in identity theft.¹⁹¹ The Acxiom official line supports a federal privacy legislation that prevents state action on the issue, but only one that limits notification to situations where there is a real chance that identity theft will ensue.¹⁹²

The *Wall Street Journal* reported that Acxiom’s initial interpretation of the California breach notification law made the company responsible only for notification of its clients—the retailers for whom it manages databases—and not the California consumers.¹⁹³ The company’s logic, which was criticized by privacy advocates, was that the data belonged to the retailers.¹⁹⁴

¹⁸⁶ *Id.*

¹⁸⁷ *Id.*

¹⁸⁸ Press Release, Dep’t of Just., *supra* note 179.

¹⁸⁹ See Taulbee, *Acxiom Lets Congress Know*, *supra* note 128.

¹⁹⁰ See Taulbee, *Trial To Rehash*, *supra* note 176.

¹⁹¹ See Taulbee, *Acxiom Lets Congress Know*, *supra* note 128.

¹⁹² *See id.*

¹⁹³ Dionne Searcey, *Information Security; Consumer Alert: In 2003, California Passed Its Security Breach Notice Law; Its Effect Has Extended Well Beyond the State*, WALL ST. J., July 18, 2005, at R6.

¹⁹⁴ *See id.*

C. Low Standards: Other Lax Security Practices

The Federal Trade Commission has filed at least nine actions against companies whose security practices resulted in compromised customer data. At least one of them was a complaint about the company's information security policies; many of the others, including complaints against Gateway Learning Corp. (2004), Eli Lilly (2002), Microsoft (2002), and Guess? (2003), were based on allegations that the company did not do what the privacy policy promised that it was doing to protect customer information.¹⁹⁵

Eliot Spitzer, New York's Attorney General at the time, reached an agreement with the online arm of lingerie retailer Victoria's Secret, where the retailer agreed to a fine of \$50,000 for exposing the orders, names, and addresses of more than 560 customers.¹⁹⁶ "The consumer protection laws of the 1930's have become the privacy law of the 21st century," Spitzer told the *New York Times*.¹⁹⁷

D. Loss of Control: Lost and Stolen

Stolen laptops comprise another—and seemingly endlessly reported—category of data breaches. Wells Fargo, Motorola, MCI, a large number of universities, blood banks, and medical centers have reported losses.¹⁹⁸ Backup tapes went missing from Time Warner, the Bank of America, and Ameritrade, among others.¹⁹⁹ The scorecard is not comforting and does not reflect learning from prior events. The University of Colorado had four instances of lost tapes in 2005; Michigan State University had three.²⁰⁰

¹⁹⁵ See Dreifach, *supra* note 54, at 417.

¹⁹⁶ See John Schwartz, *Victoria's Secret Reaches a Data Privacy Settlement*, N.Y. TIMES, Oct. 21, 2003, at C14.

¹⁹⁷ *Id.*

¹⁹⁸ See Bender, *Privacy Developments*, *supra* note 48, at 15.

¹⁹⁹ *See id.*

²⁰⁰ See *Identity Theft Resource Center Reports 104 Security Breaches Since January 1st Is Anyone Hearing An Alarm Bell Yet?*, PR NEWSWIRE, Sept. 6, 2005.

E. Two Additional Considerations

1. Is Harm Necessary?

Harm is a troublesome element in looking at the privacy legislation put forth by the states.²⁰¹ At least one commentator says that the role of harm—or the requirement of particular types or levels of harm—is far from settled in private claims regarding privacy violations.²⁰² As an example, he cites the case of a local pharmacy that was sold to the CVS chain, which required as a condition of the sale that pharmacy records be transferred and that customers not be notified until after the sale.²⁰³ As a result, a class-action suit was filed against the pharmacies.²⁰⁴ The plaintiff, an AIDS patient, claimed he used the independent pharmacy for almost twenty years precisely because he expected his information to be handled confidentially. The court said that, although “actual injury” is required by the New York General Business law in play, that injury did not need to be “pecuniary,” apparently accepting the plaintiff’s assertion that the loss of the right to privacy was an adequate harm, one that was lost as a result of the intentional practices of CVS.²⁰⁵

2. Mixed Messages from Washington

Meanwhile, at the same time that Congress and state lawmakers are seeking to protect consumers with more legislation at both levels, other governmental actors are moving in the opposite direction. In two stark examples of the amount and variety of information held on consumers, changes to IRS and Health Insurance Portability and Accountability Act (HIPAA) enforcement appear to be on the horizon. The IRS has quietly revealed that it is considering allowing tax preparers to sell

²⁰¹ See *supra* Part I.E.

²⁰² Dreifach, *supra* note 54, at 416.

²⁰³ *Id.* (discussing *Anonymous v. CVS Corp.*, 188 Misc. 2d 616 (N.Y. Sup. Ct. 2001)).

²⁰⁴ *CVS*, 188 Misc. 2d at 616.

²⁰⁵ *Id.* at 624. “To plead a claim for violation of General Business Law § 349, a plaintiff must allege that (1) defendant’s acts have broad impact on consumers at large; (2) defendant is engaged in deceptive practices; and (3) this practice has injured plaintiff[.]” *Id.*

information gathered from tax returns.²⁰⁶ In response, however, forty-six Attorneys General from the states and the District of Columbia have submitted formal opposition to the change, instead suggesting a ban on the sharing of taxpayer information.²⁰⁷ In the summer of 2005, HIPAA rule-making changes were announced that reduced the criminal liability of individual employees in doctor's offices.²⁰⁸ In March 2006, the House Financial Services Committee passed the Financial Data Protection Act, which, if enacted, would reduce the level of consumer protection in state laws.²⁰⁹

²⁰⁶ Jeff Gelles, *IRS Plans to Allow Preparers To Sell Data*, PHILA. INQUIRER, Mar. 21, 2006, at A01, available at 2006 WLNR 4628551.

²⁰⁷ *Federal, State Officials Object to Proposed IRS Rules*, EPIC ALERT, Vol. 13.07, Apr. 6, 2006, available at http://www.epic.org/alert/EPIC_Alert_13.07.html. EPIC has been critical of the IRS and its security, as is a broader Government Accountability Office report released in April 2006 that gave many federal agencies poor reports. *Id.* Security problems include:

IRS's physical security controls (restricting physical access to computer facilities and resources); software patch management; and electronic access controls such as passwords, user rights and file permissions. The IRS also has had considerable trouble with its contractors improperly accessing and collecting sensitive taxpayer data. In one case, an IRS contractor spent several months collecting political party affiliation data on taxpayers in 20 states, in violation of the law. *Id.*

²⁰⁸ See Amy Snow Landa, *HIPAA Memo Could Affect Doctors' Criminal Liability*, AMERICAN MEDICAL NEWS, Jul. 18, 2005, available at <http://www.ama-assn.org/amednews/2005/07/18/gvsb0718.htm> (referencing to Memorandum from Timothy J. Coleman, Senior Counsel to the Deputy Attorney General to Alex M. Aza II, General Counsel, Department of Health and Human Services, *Re: Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6*, June 1, 2005, available at http://www.worldprivacyforum.org/pdf/hipaa_opinion_06_01_2005.pdf); see also David V. Marshall, *Justice Department Limits Prosecution Under HIPAA*, Davis Wright Tremaine LLP Advisory Bulletin, http://www.dwt.com/practc/hc_ecom/bulletins/06-29-05_ProsecutionLimits.htm, (referencing Memorandum from Timothy J. Coleman, Senior Counsel to the Deputy Attorney General to Alex M. Aza II, General Counsel, Department of Health and Human Services, *Re: Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6*, June 1, 2005, available at http://www.worldprivacyforum.org/pdf/hipaa_opinion_06_01_2005.pdf).

²⁰⁹ *House Committee Approves Bill to Weaken Data Breach Laws*, EPIC ALERT, Vol. 13.06, Mar. 24, 2006, available at http://www.epic.org/alert/EPIC_Alert_13.06.html. H.R. 3997 is just one of the data security bills under consideration, some stronger and some weaker than the state laws.

III. THE TOOLS ARE MANY

The examples mentioned above invoke tort and due care considerations; state consumer protection legislation; administrative actions by the FTC; class action lawsuits, including one where no tangible harm has been suffered; computer fraud statutes; grand theft charges; the Freedom of Information Act; unauthorized access statutes; access device fraud; and obstruction of justice charges. These are all real tools used by prosecutors and other governmental agents, privacy advocates, consumer groups, and individuals whose data has been compromised. These tools are separately imperfect, but together comprise a net that needs further investigation and testing before an overarching federal law can provide safety for consumer information.

Additional theoretical approaches are mentioned in the literature. Tort theories that can be available to victims include trespass to chattels, conversion, and intrusion.²¹⁰ Several commentators support a response based in a tort of privacy.²¹¹ There is an increasing movement toward the recognition of a duty to protect information, with scholars suggesting the utilization of a variety of existing remedies in tort law and in traditional business law for those who fail to exercise proper care, in addition to the existing federal and state laws.²¹² One commentator says that if we do not already expect two new duties from companies, they soon will be expected to fulfill even more explicitly duties “to provide reasonable security for their corporate data and information systems; and . . . to disclose security breaches to those who may be adversely affected by such breaches.”²¹³ Another commentator warns of liability for directors whose companies fail to ensure customer and employee privacy as a possible violation of the

²¹⁰ *Johnson, supra* note 8, at 259.

²¹¹ *See generally* McClurg, *supra* note 39 (suggesting that the privacy tort of appropriation should be available as a remedy in situations of “invasive consumer data profiling”).

²¹² *See generally* Johnson, *supra* note 8; McClurg, *supra* note 39.

²¹³ Thomas J. Smedinghoff, *The New Law of Information Security: What Companies Need To Do Now*, 22 NO. 11 COMPUTER & INTERNET LAW. 9, 9 (2005).

business judgment rule and the subsequent basis for shareholders' derivative suits.²¹⁴

IV. CONCLUSION

To avoid nefarious and extreme legislation, companies need to make it regularly occurring business practices to take care of their customer data. For instance, though the California law covers only breaches involving unencrypted data; an advisory article suggests that companies would then be wise “to encrypt the personal information of its customers (or employees)” in order to avoid most of the explicit liability in the law.²¹⁵ “Companies might also wish to consider installing firewalls and other software applications to guard their computer databases—particularly those containing ‘personal information’ of consumers or employees[.]” the piece goes on, offering advice that seems a sub-floor of what would constitute good business practices.²¹⁶ Just like offline data would be stored in locked file cabinets to safeguard it, businesses, schools, and government agencies need to realize that the trust of their customers, students, and employees can very easily be eroded by a lack of protection. Data protection is not just one way to follow the law, it makes for good business.²¹⁷

In seeking to be made whole or to punish individuals for malicious use of others' data, myriad tools are available to both individual consumers as well as governmental enforcement entities. State laws are beginning to address the remedies at the roots of the malady, the laissez-faire attitudes of some companies and agencies about data security and protection, and a marketplace with many different approaches is a robust test of what the best remedies will be at this still-nascent point in the development of electronic data storage. It is far too premature to determine the best methods for ensuring the protection of consumer data, and the states should be allowed to continue to experiment to generate new ideas, testing the range of state laws against the ongoing breaches.

²¹⁴ INTERNATIONAL GUIDE TO PRIVACY, *supra* note 26, at 142–43.

²¹⁵ Paetkau & Torabian-Bashardoust, *supra* note 44, at 41.

²¹⁶ *Id.*

²¹⁷ *Id.*

The cost of a breach in business lost and in goodwill tarnished is far greater than the costs of compliance with the various laws, which simply encourage good data practices and responsible treatment of consumers.

Justice Brandeis said that “[i]t is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”²¹⁸ That is certainly mandated by the issue of privacy protection.

²¹⁸ *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).