2006

A Model Regime of Privacy Protection

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

A MODEL REGIME OF PRIVACY PROTECTION

*Daniel J. Solove**
*Chris Jay Hoofnagle***

A series of major security breaches at companies with sensitive personal information has sparked significant attention to the problems with privacy protection in the United States. Currently, the privacy protections in the United States are riddled with gaps and weak spots. Although most industrialized nations have comprehensive data protection laws, the United States has maintained a sectoral approach where certain industries are covered and others are not. In particular, emerging companies known as "commercial data brokers" have frequently slipped through the cracks of U.S. privacy law. In this article, the authors propose a Model Privacy Regime to address the problems in the privacy protection in the United States, with a particular focus on commercial data brokers. Since the United States is unlikely to shift radically from its sectoral approach to a comprehensive data protection regime, the Model Regime aims to patch up the holes in existing privacy regulation and improve and extend it. In other words, the goal of the Model Regime is to build upon the existing foundation of U.S. privacy law, not to propose an alternative foundation. The authors believe that the sectoral approach in the United States can be improved by applying the Fair Information Practices—principles that require the entities that collect personal data to extend certain rights to data subjects. The Fair Information Practices are very general principles, and they are often spoken about in a rather abstract manner. In contrast, the Model Regime demonstrates specific ways that they can be incorporated into privacy regulation in the United States.

* Associate Professor of Law, George Washington University Law School. Professor Solove has discussed many of the problems and solutions herein in his book, *The Digital Person: Technology and Privacy in the Information Age* (2004).

** Director, Electronic Privacy Information Center West Coast Office. Chris Hoofnagle has discussed many of the problems and solutions herein in his articles, *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 (2004), *available at* http://ssrn.com/abstract=582302; and *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, Jan. 5, 2005, http://ssrn.com/abstract=679581. Marc Rotenberg of the Electronic Privacy Information Center and Beth Givens of the Privacy Rights Clearinghouse have provided substantial comments which are incorporated in an earlier iteration.

I. INTRODUCTION

Privacy protection in the United States has often been criticized, but critics have too infrequently suggested specific proposals for reform. Recently, there has been significant legislative interest at both the federal and state levels in addressing the privacy of personal information. This was sparked when ChoicePoint, one of the largest data brokers in the United States with records on almost every adult American citizen, declared that it sold data on about 145,000 people to fraudulent businesses set up by identity thieves.[1] Other companies announced security breaches, including LexisNexis, from which personal information belonging to about 310,000 people was improperly accessed.[2] Senator Schumer criticized Westlaw for making available to certain subscribers personal information including Social Security Numbers (SSNs).[3]

In the aftermath of the ChoicePoint debacle and other major information security breaches, both of us have been asked by Congressional legislative staffers, state legislative policymakers, journalists, academics, and others about what specifically should be done to better regulate information privacy. In response to this question, we believe that it is imperative to have a discussion of concrete legislative solutions to privacy problems.

What appears below is our attempt at such an endeavor. Privacy experts have long suggested that information collection be consistent with Fair Information Practices. This Model Regime incorporates many of those practices and applies them specifically to the context of commercial data brokers such as ChoicePoint. We hope that this will provide useful guidance to legislators and policymakers in crafting laws and regulations. We also intend this to be a work-in-progress in which we collaborate with others. We have welcomed input from other academics, policymakers, journalists, and experts, as well as from the industries and businesses that will be subject to the regulations we propose. We have incorporated criticisms and constructive suggestions, and we will continue to update this Model Regime to include the comments we find most helpful and illuminating.

1. Joseph Menn, *Did the ChoicePoint End Run Backfire?*, L.A. TIMES, Mar. 13, 2005, at C1; Bob Sullivan, *Database Giant Gives Access to Fake Firms: ChoicePoint Warns More than 30,000 They May Be at Risk*, MSNBC, Feb. 14, 2005, http://www.msnbc.msn.com/id/6969799/. In November 2005, ChoicePoint informed an additional 17,000 individuals that their personal data may also have been compromised, bringing the total number to 162,000. Michael Hiltzik, *Big Data Broker Eyes DMV Records*, L.A. TIMES, Dec. 1, 2005, at C1.

2. David Colker, *LexisNexis Breach Is Larger: The company reveals that personal data files on as many as 310,000 people were accessed*, L.A. TIMES, Apr. 13, 2005, at C1.

3. Ken Fireman, *Identity Theft Made Easy, Schumer Warns*, NEWSDAY, Feb. 25, 2005, at A02.

II. U.S. PRIVACY LAW AND THE DATABASE INDUSTRY

Currently, the collection and use of personal data by businesses and government is spinning out of control. An entire industry devoted primarily to processing and disseminating personal information has arisen, and this industry is not well-regulated. Many companies brokering in data have found ways to avoid being regulated by the Fair Credit Reporting Act (FCRA),[4] a landmark law passed in 1970 to regulate consumer reporting agencies. Increasingly, the government is relying on data-broker companies to supply personal data for intelligence and law enforcement purposes. As a result, the government is navigating around the protections of the Privacy Act of 1974,[5] a law passed to regulate the collection and use of data by government agencies. The FCRA and Privacy Act form the basic framework that regulates a large portion of the flow of personal data, but this framework is riddled with exceptions and shunted with limitations. We propose a Model Regime of Privacy Protection to address these problems.

A. The Fair Credit Reporting Act

The database industry has its roots in the rise of consumer reporting agencies—companies that gather and sell personal information on individuals for business purposes. The consumer reporting industry began over a century ago. The first major consumer reporting agency, Retail Credit Co., was founded in 1899, and over the years, it grew in size and began selling reports about individuals to insurers and employers.[6]

By the 1960s, significant controversy surrounded the credit reporting agencies. There were questionable practices in the industry, including requirements that investigators fill quotas of negative information on data subjects.[7] To do this, some investigators fabricated negative information; others included incomplete information.[8] Additionally, the investigators were collecting "lifestyle" information on data subjects, including their sexual orientation, marital situation, drinking habits, and cleanliness.[9] The credit-reporting agencies were maintaining outdated information and, in some cases, providing the file to law enforcement and to unauthorized persons. Individuals had no right to see what was in their files. Public exposure of the industry resulted in an extensive con-

4. 15 U.S.C. § 1681 (2000).

5. 5 U.S.C. § 552a (2000).

6. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 316 (2000).

7. *See id*. at 316–21.

8. *Id*. at 316–18.

9. *Id*. at 316–19.

gressional inquiry and ultimately led to the passage of the FCRA in 1970.[10]

The FCRA was the first federal law to regulate private-sector use and disclosure of personal information. At the most basic level, the FCRA requires consumer reporting agencies to maintain procedures to ensure "maximum possible accuracy."[11] The law regulates the collection, maintenance, and dissemination of "consumer reports."[12] Consumer reports can only be used for a series of enumerated purposes, such as for determining eligibility for credit or engaging in employment background checks.[13] Consumer reporting agencies must allow people access to their records and must provide a telephone number for people to call to voice a complaint.[14] Consumer reporting agencies must investigate any mistakes that people point out in their files.[15] Any user of a credit report taking adverse action on a person based on a consumer report must notify the person about this fact.[16] When employers (both prospective and current) want to examine a person's credit report, they must first obtain the person's consent.[17] If the employer takes any adverse action based on the report, the employer must inform the person and provide instructions to obtain a copy of the report.[18] Under the FCRA, law enforcement has a number of avenues to access consumer reports, some of which require an annual accounting to Congress. Full consumer reports can be accessed by court order, by grand jury subpoena, or by request of a child support enforcement agency.[19] The Act allows the Federal Bureau of Investigation (FBI) access to individuals' account information and identifying information for counterintelligence purposes upon written request.[20]

B. The Privacy Act

The Privacy Act of 1974 was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights.[21] As technology advanced through the 1960s and 70s, it became easier for agencies to cross-reference individuals' personal data. Citizens and legislators began to contemplate the ways that this in-

10. 15 U.S.C. § 1601 (2000).
11. *Id.* § 1681e(b).
12. *Id.* § 1681.
13. *Id.* § 1681b.
14. *Id.* § 1681g.
15. *Id.* § 1681i.
16. *Id.* § 1681m(a).
17. *Id.* § 1681b(b).
18. *Id.*
19. *Id.* § 1681b.
20. *Id.* § 1681u.
21. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 71–82 (1995).

formation, if compiled, could be abused. In 1973, the Department of Health, Education, and Welfare (HEW) issued a report recommending that Congress enact legislation adopting a Code of Fair Information Practices for record systems containing personal data.[22] This Code consisted of the following principles:

- There must be no personal data record-keeping system whose very existence is secret.[23]
- There must be a way for an individual to find out what information about him is in a record and how it is used.[24]
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.[25]
- There must be a way for an individual to correct or amend a record of identifiable information about him.[26]
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precaution to prevent misuse of the data.[27]

The HEW Report also raised concerns about the use of the SSN, which was fast becoming a "standard universal identifier" that would link all of the records kept on a person by all agencies. The HEW Report recommended that the use of SSNs should be strictly curbed.[28]

The Privacy Act grew out of the HEW Report. The Act requires government agencies to show people any records kept on them.[29] It requires agencies to follow the Fair Information Practices when gathering and handling personal data.[30] Agencies must provide people with access and correction rights, limit data-collection to that necessary to fulfill a specified government function, and destroy data after a certain period of time. The Privacy Act places restrictions on how agencies can share an individual's data with other people and agencies.[31] Finally, the Act permits individuals to sue government agencies for violations.[32] The FCRA and Privacy Act have thus provided a basic framework of privacy protec-

22. SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEPT. OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *available at* http://epic.org/privacy/hew1973report (follow "Summary and Recommendations" hyperlink).

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. 5 U.S.C. § 552a(d) (2000).

30. *Id.* § 552a(e); *see also* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1.

31. 5 U.S.C. § 552a(b).

32. *Id.* § 552a(g).

tion, with the FCRA addressing the key private sector uses of personal data and the Privacy Act addressing public sector uses.

C. The Database Industry

A number of companies have arisen apart from the consumer reporting agencies or have spun off of the consumer reporting agencies. These companies' primary business is gathering, analyzing, and disseminating personal data. One such company is ChoicePoint, Inc., based in Alpharetta, Georgia, which spun off from consumer reporting agency Equifax in 1997.[33] ChoicePoint sells information and data services to insurers, businesses, government agencies, and direct marketers.[34] In 2004, the company reported total revenue of nearly $1 billion.[35]

In its short history, ChoicePoint has managed to attain a large share of the commercial data broker market with strategic purchases of other businesses. In 2000, ChoicePoint purchased DBT Online, Inc., a successful commercial data broker that provides "AutoTrackXP," a favored law enforcement-oriented service.[36] In all, ChoicePoint has acquired over fifty database companies.[37] ChoicePoint has thousands of clients and sells services to 7,000 federal, state, and local law enforcement agencies.[38]

There are many similar types of companies. Acxiom, for example, is "a billion-dollar player in the data industry, with details about nearly every adult in the United States."[39] Acxiom provides information to marketers for profiling consumers, manages credit records, sells data for background checks, and provides data to government agencies:

> It's not just names, ages, addresses, and telephone numbers. The computers in [Acxiom's] rooms also hold billions of records about marital status and families and the ages of children. They track individuals' estimated incomes, the value of their homes, the make and price of their cars. They maintain unlisted phone numbers and details about people's occupations, religions, and ethnicities. They

33. ChoicePoint Inc., General Form for Registration of Securities Pursuant to Section 12(b) or 12(g) of the Securities Exchange Act of 1934 (Form 10) (June 6, 1997), *available at* http://www.sec.gov/Archives/edgar/data/1040596/0000950144-97-006666.txt.

34. *See* EPIC ChoicePoint Page, http://www.epic.org/privacy/choicepoint/ (last visited Sept. 13, 2005).

35. ChoicePoint Inc., Annual Report (Form 10-K), at 5 (Mar. 15, 2005), *available at* http://www.sec.gov/Archives/edgar/data/1040596/000095014405002577/g93507e10vk.htm#102.

36. ChoicePoint Inc., Annual Report (Form 10-K), at 3 (Mar. 26, 2003), *available at* http://www.sec.gov/Archives/edgar/data/1040596/000095014401500429/g68168e10-k.txt.

37. ROBERT O'HARROW, JR., NO PLACE TO HIDE 130 (2005).

38. *Testimony of Derek Smith: Before the Subcomm. On Commerce, Trade and Consumer Protection of the H. Energy and Commerce Comm.*, 109th Cong. (2005) (testimony of Derek Smith, Chairman and Chief Executive Officer, ChoicePoint Inc.), *available at* http://energycommerce.house.gov/108/Hearings/03152005hearing1455/Smith.pdf.

39. O'HARROW, *supra* note 37, at 34.

> sometimes know what some people read, what they order over the phone and online, and where they go on vacation.[40]

LexisNexis is a corporation owned by the United Kingdom-based Reed Elsevier that offers access to numerous databases and information retrieval services.[41] Through services such as its featured search tool "SmartLinx," LexisNexis offers access to SSNs, addresses, licenses, real estate holdings, bankruptcies, liens, marital status, and other personal information.[42]

ChoicePoint, Acxiom, and LexisNexis are three of the larger data brokers. There are many other companies that comprise this industry. The database industry provides data to companies for marketing, to the government for law enforcement purposes, to private investigators for investigating individuals, to creditors for credit checks, and to employers for background checks.

The government increasingly has been contracting with data brokers. For example, ChoicePoint has multimillion dollar contracts with at least thirty-five federal agencies, including the Internal Revenue Service (IRS) and the FBI.[43] The United States Marshals Service uses LexisNexis for "location of witnesses, suspects, informants, criminals, parolees in criminal investigations, location of witnesses, [and] parties in civil actions."[44] LexisNexis's Person Tracker Plus Social Security number is a private library "designed to meet the needs of law enforcement."[45] It provides information probably derived from credit headers, including name, SSN, current address, two prior addresses, aliases, birth date, and telephone number.[46] After 9/11, Acxiom positioned itself as "an anti-terrorism company" by actively pursuing ways to manage personal information for the government.[47] Charles Morgan, Acxiom's CEO, stated after 9/11 that "we developed a sense among the leadership at Acxiom that for this country to be a safer place [the government] had to be able to work with information better."[48]

The government is becoming increasingly interested in data-mining technologies. Data mining involves searching through repositories of data to find out new information by combining existing data or to make

40. *Id.* at 36.

41. LexisNexis Company History, http://www.lexis-nexis.com/presscenter/mediakit/history.asp (last visited Mar. 27, 2004).

42. LexisNexis SmartLinx, http://www.lexis-nexis.com/smartlinx/ (last visited Mar. 27, 2004).

43. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169 (2004).

44. Exhibit B, Lexis-Nexis Select Limited Distribution Authorized Use List 6 (1998), *available at* http://epic.org/privacy/choicepoint/cpusms7.30.02a.pdf.

45. Lexis-Nexis Fax Bulletin 39, *available at* http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

46. *Id*.

47. O'HARROW, *supra* note 37, at 60.

48. *Id.* at 58.

predictions about future behavior based on patterns in the data.[49] One of the government's most notable attempts to engage in data-mining research was the Total Information Awareness program, run by John Poindexter in the Department of Defense (DOD), which received considerable media attention in late 2002.[50] The idea was to gather various records about individuals from businesses and then analyze it for patterns of terrorist behavior. Due to sharp criticism, the Senate denied funding to the program in 2003.[51]

However, government data-mining programs did not die with Total Information Awareness. According to the Report of the Technology and Privacy Advisory Committee (TAPAC), appointed by Secretary of Defense Donald Rumsfeld, Total Information Awareness is "not unique in its potential for data mining. TAPAC is aware of many other programs in use or under development both within DOD and elsewhere in the government that make similar uses of personal information concerning U.S. persons to detect and deter terrorist activities."[52] In light of the intense criticism that Total Information Awareness generated, government agencies have moved data mining projects underground. Increasingly, such data analysis is being outsourced to database companies. ChoicePoint vice president James Zimbardi declared: "We do act as an intelligence agency, gathering data, applying analytics."[53]

D. The Limits of U.S. Privacy Law

The FCRA and the Privacy Act do not adequately address the activities of the database industry. The FCRA applies to "any consumer reporting agency" that furnishes a "consumer report."[54] The definition of "consumer reporting agency" is any person who "regularly engages" in collecting information about consumers "for the purpose of furnishing consumer reports to third parties."[55] This definition turns on the meaning of "consumer report," which is the key term that defines the scope of the FCRA. Unfortunately, the FCRA has a poorly drafted definition of "consumer report" that has allowed some to unduly narrow the FCRA coverage. The FCRA conditions the definition of "consumer report" on how the information is used. That is, a "consumer report" is any communication bearing on a consumer's character or general reputation *which is used or collected for* credit evaluation, employment screening,

49. SOLOVE, *supra* note 43, at 41.
50. *Id.* at 168–69.
51. *Id.* at 169.
52. TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM vii–viii, 45–49 (2004) (footnote omitted).
53. Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth of Personal Data*, WASH. POST, Jan. 20, 2005, at A1.
54. 15 U.S.C. § 1681b (2000).
55. *Id.* § 1681a(f).

insurance underwriting, or licensing.[56] Although the FCRA was passed to limit the uses of personal information in evaluating people, a literal reading of its definition of "consumer report" makes the law inapplicable if information is used for an unauthorized purpose beyond those enumerated in the FCRA. One could argue, for instance, that a criminal using credit information for fraud has not triggered the FCRA because fraud is not an authorized use. These problems in the definition of "consumer report" have allowed data brokers to avoid being regulated by the FCRA.

The FBI uses similar reasoning to evade protections of the FCRA. In a memo justifying the agency's reliance on services provided by commercial data broker ChoicePoint, the agency reasoned: "In this instance, none of the information which the FBI would seek to review has been collected by ChoicePoint for any of the [FCRA] purposes."[57] The FBI further concludes that ChoicePoint is not a consumer reporting agency: "Because ChoicePoint does not collect 'public record information' for any of the highlighted purposes [under the FCRA], ChoicePoint is not acting as a 'consumer reporting agency' for the purposes of the FCRA, and the collected information therefore does not constitute a 'consumer report.'"[58]

In the absence of statutory regulation, data brokers have adopted self-regulatory rules known as the Individual Reference Services Group (IRSG) Principles.[59] The Principles set forth a weak framework of protections, allowing companies to sell nonpublic personal information "without restriction" to "qualified subscribers," which includes law enforcement agencies.[60] Qualified subscribers need only state a valid purpose for obtaining the information and agree to limit redissemination of information.[61] Under IRSG Principles, individuals can only opt-out of the sale of personal information to the "general public," but ChoicePoint

56. *Id.* § 1681a(d) (emphasis added); *see also id.* § 1681b(a)(3)(A)–(E). For an account of other limitations of the FCRA, see Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 210–13 (1992).

57. OFFICE OF THE GEN. COUNSEL, NAT'L SEC. LAW UNIT, GUIDANCE REGARDING THE USE OF CHOICEPOINT FOR FOREIGN INTELLIGENCE COLLECTION OR FOREIGN COUNTERTERRORISM INVESTIGATIONS 12–13 (2001), *available at* http://epic.org/privacy/choicepoint/cpfbia.pdf.

58. *Id.* at 13 (footnote omitted). A strong argument can be made that these interpretations are flawed. The provisions of the FCRA governing law enforcement access make it clear that Congress intended procedural safeguards against disclosure of credit information, regardless of its intended use. As noted in the review of federal privacy law and access to commercial information done by the Center for Democracy & Technology, some courts have ruled that when information is collected for consumer reporting purposes, it remains a consumer report, despite the fact that it may be employed for non-FCRA purposes. James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1477 (2004).

59. *See* FEDERAL TRADE COMMISSION, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (1997), http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

60. INDIVIDUAL REFERENCE SERVICES GROUP, IRSG PRINCIPLES, http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc2.htm#A%20The%20IRSG%20Principles (last visited Sept. 13, 2005).

61. *Id.*

does not consider its customers to be members of the general public.[62] The IRSG Principles were carefully crafted in order to ensure maximum flexibility by commercial data brokers. They have failed to set forth a reasonable degree of protection for individuals, and in fact, it was while data brokers were operating under these principles that the major privacy breaches occurred.

The FCRA also fails to provide sufficient protection against identity theft, a crime that is rising at an alarming rate. Identity theft involves the use of a victim's personal information to improperly access accounts, obtain credit in the victim's name, or otherwise engage in transactions by masquerading as the victim. In 2003, the Federal Trade Commission (FTC) estimated that "almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the past year."[63] The FCRA, unfortunately, does little to prevent identity theft or to minimize its impact on victims once it occurs. Under the Fair and Accurate Credit Transactions Act (FACTA) of 2003, which amended FCRA, individuals can now obtain a free credit report once a year from each of the three major consumer reporting agencies (Equifax, Trans Union, and Experian) online.[64] Individuals can also place a fraud "alert" on their records if they are victimized by identity theft, but such alert "is often as simple as a mere entry in the '100-word statement' box in credit files that's made available to consumers who disagree with an entry made in their credit file."[65] Moreover, the alert does not stop activity in a person's file. Instead, it acts as a warning to a retailer that it should exercise more care in granting credit. A savvy identity thief could continue committing more fraud even with the alert present. Indeed, Linda and Jay Foley of the Identity Theft Resource Center found that consumer reporting agencies ignored fraud alerts in a significant number of cases.[66]

The Privacy Act also suffers from many problems that limit its effectiveness. It only applies to the federal government and to private companies that are administering a system of records for the government.[67] Thus, when the information originates from the government and is transferred to a private company, then Privacy Act requirements apply to the contractor.[68] However, a database of information that originates at a data broker would not trigger the requirements of the Privacy Act. Beyond data brokers, consumer reporting agencies are specifically ex-

62. Letter from Gina Moore, ChoicePoint, Inc. to Chris Hoofnagle, Director, Electronic Privacy Information Center 1 (Feb. 21, 2003), *available at* http://epic.org/privacy/choicepoint/cp_nooptout.pdf.

63. FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 4 (Sept. 2003), *available at* www.ftc.gov/os/2003/09/synovatereport.pdf. For an excellent account of the rise of identity theft, see BOB SULLIVAN, YOUR EVIL TWIN: BEHIND THE IDENTITY THEFT EPIDEMIC (2004).

64. 15 U.S.C. § 1681j (2000).

65. SULLIVAN, *supra* note 63, at 85.

66. IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2004 16 (Sept. 2004), *available at* http://www.idtheftcenter.org/aftermath2004.pdf.

67. 5 U.S.C. § 552a(m) (2000).

68. *Id.*; *see, e.g.*, Modification M001, http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf.

empted from being considered a federal contractor for systems of records.[69]

This limitation to the Privacy Act is critical—it allows data brokers to amass huge databases that the government is legally prohibited from creating. Then, when the government needs the information, it can request it from the data broker. At that point, the personal information would be subject to the Privacy Act, but law enforcement and intelligence agencies have special exemptions under the Privacy Act that limit access, accuracy, and correction rights.[70] For example, law enforcement agencies "may promulgate rules . . . to exempt any system of records [involving information about criminal investigation or criminal history] within the agency from [most] part[s] of [the Privacy Act]."[71]

The Privacy Act's attempt to rein in the use of SSNs has been a failure. One of the primary reasons is that the Privacy Act fails to restrict the use of SSNs by businesses or other private sector entities. Such a restriction was proposed during the creation of the Privacy Act, but Congress failed to include it.[72] Today, SSNs are routinely used by businesses and other entities, often as a password to gain access to accounts.

Another limitation is that the Privacy Act only applies to federal, not state or local, government agencies. Moreover, the Privacy Act has a number of major exceptions, including one that exempts agencies when they disclose information for "any routine use" that is "compatible" with the purpose for which the agency gathered the data.[73] As Robert Gellman has observed: "This vague formula has not created much of a substantive barrier to external disclosure of personal information. . . . Later legislation, political pressures, and bureaucratic convenience tended to overwhelm the law's weak limitations."[74]

In sum, the database industry is increasingly straining the regulatory regime for information privacy established in the early 1970s. The existing regime has struggled to address the rise of new data-trafficking companies apart from consumer reporting agencies, the burgeoning cooperation of businesses with the government for intelligence and law enforcement operations, and the increase in the uses of personal data. While privacy laws passed after the 1970s apply to specific kinds of records such as video rental records and cable television records, most of these laws fail to cover the database industry.[75] The Model Regime we

69. 5 U.S.C. § 552a(m)(2) (2000).
70. *Id.* § 552a(k).
71. *Id.* § 552a(j).
72. SMITH, *supra* note 6, at 297.
73. 5 U.S.C. § 552a(b)(3).
74. Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 198 (Philip E. Agre & Marc Rotenberg eds., 1997).
75. Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000) (cable records); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (2000) (Internet Web sites gathering data

propose in the pages that follow is designed to address the gaps and limitations in existing law.

III. THE MODEL REGIME

A. Notice, Consent, Control, and Access

1. Universal Notice

a. Problem

There is no general knowledge about the companies using personal information. In order to grant consent, gain access, or otherwise exercise one's rights with regard to personal information maintained by data brokers, consumer reporting agencies, and other institutions, people must know what institutions are collecting their data. Providing such rights without knowledge of the companies will be meaningless. For example, in the ChoicePoint security scandal, most people had no idea that ChoicePoint existed, let alone that it was collecting and selling their personal data. Moreover, as the ChoicePoint security scandal demonstrates, data brokers routinely sell personal information with little oversight about who may receive the data and how it will be used. The problems of such a system were emphatically illustrated in *Remsburg v. Docusearch*,[76] where a data broker was employed by a stalker to locate and murder Amy Boyer. ChoicePoint has invited a national debate and discussion about data brokers, but such a discussion cannot meaningfully take place unless people are informed about what information companies have and what they do with that information.

b. Legislative Mandate

To ensure meaningful access, opt-out, and other rights, there must be a way to provide people with notice about all of the companies collecting their information.

c. Specific Solution

Any company primarily engaged in interstate collection, maintenance, and/or sale of personally identifiable information shall register with the FTC. Such registration shall include the nature of personal information collected, the name and contact information for the data controller, as well as a clear and concrete description of the uses to which the information is put. Data brokers shall also disclose the types of busi-

about children under 13); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710–2711 (video records).

76. 149 N.H. 148, 152–53 (2003).

nesses and entities to whom they disclose personal information, as well as what safeguards they have in place for vetting those entities that receive the data. This information shall be publicly disclosed by the FTC on a Web site and in printed materials.

2. Meaningful Informed Consent

a. Problem

Many data transfers and uses by companies occur without the meaningful informed consent of consumers. The current regime of allowing consumers to opt-out of data sharing, as embodied in the Gramm-Leach-Bliley Act,[77] is ineffective. The incentives are such that companies benefit if they make opting out as cumbersome as possible and do not adequately inform people about the uses of their data. As a result, very few people opt-out, and those who try find the process difficult and time-consuming.

b. Legislative Mandate

There must be a way to ensure that consumers can exercise meaningful informed consent about the uses and dissemination of their personal information.

c. Specific Solution

Companies that collect personal information should be required to first obtain an individual's consent before using it for an unrelated secondary use, except for reasonable investigation of fraud. To the extent that companies endeavor to use personal information for secondary uses without first obtaining individual consent, such uses shall be specifically authorized by statute or regulation. For all new uses of personal information, companies must either be authorized by statute to engage in such a use or seek the consent of the individual to whom the information pertains. When a company engages in any new use authorized by statute, it shall disclose such expansion in use immediately to the FTC, and the change shall be displayed clearly on the FTC Web site so that individuals are aware of the change.

77. 15 U.S.C. § 6802(b) (2000).

3. One-Step Exercise of Rights

a. Problem

There are hundreds, possibly thousands, of companies that collect and trade in personal information. To the extent that the law provides people with rights of access, opt-in, opt-out, limitation of use and transfer, and so on, these rights must currently be exercised one-at-a-time at each individual company. For example, under the Gramm-Leach-Bliley Act, people have a right to opt-out of the transfer of their data to third parties for marketing purposes.[78] Many people have dealings with a multitude of financial institutions, and opting out of each one can be onerous and time-consuming. When data brokers are brought into the fold, the exercise of such rights becomes exponentially more difficult. Imagine the time it would take to opt-out with hundreds of different companies. This example merely involves opt-out; there are many other rights that people exercise as well, and exercising all such rights with the multitude of companies individually will prove nearly impossible and time-prohibitive.

b. Legislative Mandate

To ensure the meaningful exercise of rights with regard to personal information, there must be a centralized system for exercising these rights in an efficient and easy manner.

c. Specific Solution

In conjunction with universal notice, the FTC shall develop a centralized mechanism for people to exercise their rights with respect to their personal information. Such a mechanism would mimic the Do Not Call Web site, which allows individuals to opt-out of telemarketing and verify their enrollment by visiting a single Web site. Similarly, individuals should be able to enroll in a centralized do-not-share registry. Other rights, to address security risks, including access and correction, will have to be administered by the individual companies maintaining personal data. The centralized mechanism will simply provide a pointer to instructions on how to exercise these rights with the companies maintaining the data.

Those seeking to access any personal information collected on the centralized mechanism for purposes other than those for which the mechanism was created must first obtain a court order. Only specifically enumerated and approved purposes will be authorized. As for law enforcement access to the data, officials will be required to demonstrate

78. *Id.*

probable cause and obtain only as much information as necessary to meet the needs articulated in the showing of probable cause.

4. Individual Credit Management

a. Problem

As the ChoicePoint snafu illustrates, individuals are not in control of the basic information that is used for credit identification authentication. Numerous individuals and companies can access a person's credit information without that person's knowledge. Identity thieves take advantage of this system when they can seek loans or credit cards with creditors, who check the victim's credit without informing the victim. Such credit checks are often the beginning step in an identity theft. Because these checks can occur without the victim's knowledge or consent, the identity thief can readily obtain credit in the victim's name surreptitiously. Many identity thefts would be stopped at their incipiency if only the victim had known about the access to the victim's credit records and could have blocked such access. Moreover, the problem exacerbates identity thefts after they are underway because victims are unaware that they have been victimized until months or years later.

b. Legislative Mandate

To ensure effective individual management of consumer reporting, there must be a way for individuals to know when entities attempt to access their credit records and to have the ability to block such access.

c. Specific Solution

First, notice shall be issued whenever any new person or entity makes an inquiry on or accesses the consumer report of another. The individual can choose to receive such notice by mail, telephone, or email. Second, unless individuals choose otherwise, credit records shall be "frozen," whereupon they can only be accessed by others after the individual has preapproved the release of such records. Third, to guarantee maximum possible accuracy of consumer reports, individuals should be entitled to free credit monitoring if they choose.

5. Access to and Accuracy of Personal Information

a. Problem

ChoicePoint and other data brokers collect detailed dossiers of personal information on practically every American citizen. Most people have not even heard of these companies. Even if they do know about these companies, people have no way of knowing what information is

maintained about them, why it is being kept, how long it is being maintained, to whom it is being disseminated, and how it is being used. The records maintained by these companies can have inaccuracies. This would not matter much if the information were never used for anything important. However, the data is being used in ways that directly affect individuals—by the government for law enforcement purposes and by private investigators for investigation.

b. Legislative Mandate

There must be a way for individuals to ensure that their personal information, that is maintained by various data brokers, is maintained accurately and is not kept for an unreasonable amount of time.

c. Specific Solution

Individuals shall, in a centralized manner, be able to access their information and an accounting of disclosures from data brokers at no cost. Data brokers must limit the amount of time they maintain personal information to a reasonable period. As with consumer reporting agencies under the FCRA, a procedure shall be developed for individuals to correct inaccuracies in their records.

B. Security of Personal Information

6. Secure Identification

a. Problem

Businesses and financial institutions currently grant access to people's records when the accessor merely supplies a SSN, date of birth, mother's maiden name, or other forms of personal information that is either available in public records or sold by data brokers. This makes the repositories of individuals' personal data and their accounts woefully insecure, as identity thieves can readily obtain the information needed to gain access and usurp control. As the ChoicePoint security scandal illustrates, SSNs and other personal information about hundreds of thousands of people can readily fall into the hands of identity thieves.

b. Legislative Mandate

There must be a way to prevent readily available pieces of personal information from being used as passwords to gain access to people's records and accounts.

c. Specific Solution

Companies shall develop methods of identification which (1) are not based on publicly available personal information or data that can readily be purchased from a data broker, and (2) can be easily changed if they fall into the wrong hands. Whereas an individual's SSN cannot be changed without significant hassle, and date of birth and mother's maiden name cannot be changed, identifiers such as passwords can be changed with ease. Furthermore, they are not universal, and thus a thief with a password cannot access all of a victim's accounts—only those with that password. Biometric identifiers present problems because they are impossible to change. If they fall into the wrong hands, they could prove devastating for victims as well as present ongoing risks to national security. Therefore, passwords are a cheap and effective way to limit identity theft and minimize the problems victims face in clearing up the damage caused by identity theft.

7. Disclosure of Security Breaches

a. Problem

When companies suffer security breaches that result in personal information being leaked or falling into the hands of unauthorized third parties, the people to whom the personal information pertains are made more vulnerable to fraud and identity theft. They often are unaware of this and are unable to take steps, such as monitoring their consumer reports, to protect themselves. This was dramatically illustrated by the ChoicePoint security breach, which apparently was the second time the company had sold personal information to criminals. The first incident occurred in 2002 and only recently came to public light in the context of the second breach, which had to be disclosed under California's information security breach disclosure requirements.[79] ChoicePoint is not the only commercial data broker that has disclosed records to others improperly—in 2002 and 2003 two individuals were able to crack commercial data broker Acxiom's databases, leading to the release of twenty million customer records, some of which contained SSNs.[80]

b. Legislative Mandate

There must be a way for individuals to learn about security breaches that result in the leakage or improper access of their personal data.

79. CAL. CIV. CODE § 1798.29 (West 2005).
80. O'HARROW, *supra* note 37, at 71–72.

c. Specific Solution

Companies shall be placed under an affirmative obligation to provide direct notice to the individuals whose data has been leaked or improperly accessed. Such a statute could be modeled on California's information security breach law.[81] Individuals should also receive a copy of the dossier or information given to the unauthorized party.

C. Business Access to and Use of Personal Information

8. Social Security Number Use Limitation

a. Problem

Numerous businesses and organizations demand that a person provide a SSN and then use that number as a password for access to accounts and data. Many schools and other organizations use SSNs on identification cards, thus ensuring that when a wallet is lost or stolen, one's SSN is exposed. The use of SSNs is so extensive that simple transactions, such as signing up for cell phone service, often require disclosing one's SSN.

b. Legislative Mandate

There must be a way to reduce the use of SSNs by private sector businesses.

c. Specific Solution

Unless specifically authorized by statute or regulation, businesses and other privacy sector entities shall be barred from using SSNs for identification purposes. A useful starting point is the framework of protections for the SSN embodied in California law. The law provides a panoply of protections for the identifier, including listing prohibitions on the publication of the SSN, embedding the SSN in an identification document, and limiting the appearance of the identifier in family court records.[82]

9. Access and Use Restrictions for Public Records

a. Problem

Public records were once scattered about the country, and finding out information on individuals involved trekking to or calling a series of

81. CAL. CIV. CODE § 1798.29.
82. *Id.* §§ 1785.11.1, 1785.11.6, 1786.60, 1798.85–.86; CAL. FAM. CODE § 2024.5 (West 2004).

different local offices. Today, massive database companies sweep up the data in public record systems and use it to construct dossiers on individuals for marketers, private investigators, and the government. This is what ChoicePoint does. These uses of public records turn the justification for public records on its head. Public records are essential for effective oversight of government activities, but commercial data brokers have perverted this principled purpose, and public records have now become a tool of businesses and the government to watch individuals.

b. Legislative Mandate

There must be a way to regulate access and use of public records that maximizes exposure of government activities and minimizes the disclosure of personal information about individuals.

c. Specific Solution

Access to personal information in public records shall be restricted for certain purposes. For example, accessing public records to obtain data for commercial solicitation should be prohibited. Other purposes shall be permitted: monitoring the government, conducting research, carrying on educational purposes, tracing property ownership, and other traditional noncommercial purposes. Data brokers obtaining such data should be required to promise via contract, in return for receiving such data, to be subject to reasonable use restrictions on that data and to demand that those to whom the data is transferred also restrict uses and transfers. Such regulation would have allowed for greater control over ChoicePoint's use of personal data, since it obtained a significant amount of its information from public records. Additionally, federal, state, and local agencies that maintain public record systems must make substantial efforts to limit the disclosure of SSNs, phone numbers, addresses, and dates of birth.

10. Curbing Excessive Uses of Background Checks

a. Problem

Background checks are cheaper now than ever before, which leads to a situation where individuals are being screened for even menial jobs. We risk altering our society to one where the individual can never escape a youthful indiscretion or a years-old arrest, even for a minor infraction. Pre-employment screens are frequently being used by employers even for jobs that do not involve participating in security-related functions, handling large sums of money, or supervising children or the elderly.

b. Legislative Mandate

There must be a way to limit the use of background checks to those jobs where there is a reasonable and justifiable need.

c. Specific Solution

Background checks should only be performed in contexts where fiduciary relationships are involved, where a large amount of money is handled, where employment involves care taking, or any of the national defense and security related jobs enumerated by the Employee Polygraph Protection Act of 1988.[83] Whether background checks are performed by employers or by companies hired to do the screening, the employee or prospective employee shall receive a copy of the actual investigation.

11. Private Investigators

a. Problem

Private investigators routinely access personal information about individuals from data brokers. Private investigators often operate without the extensive regulation that public law enforcement officials must heed. In some states, they are not subject to licensure; in others they are subject only to a pro forma process. As a result, they can be a source of great abuses. The Rebecca Schaeffer incident that sparked the passage of the Drivers' Privacy Protection Act demonstrates the problem. A private investigator obtained actress Rebecca Schaeffer's home address from a state DMV office.[84] The investigator was working for a stalker who used the information to go to Schaeffer's home and murder her.[85] More recently, Amy Boyer was murdered by a stalker who had hired private investigators to locate her.[86]

b. Legislative Mandate

There must be a system that ensures greater accountability in the private investigator profession.

83. 29 U.S.C. § 2006 (2000) (listing jobs involving national defense and security).

84. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1191 (2002).

85. *Id.*

86. *See* Remsburg v. Docusearch, 149 N.H. 148, 152–53 (2003).

c. Specific Solution

Each state should be required to establish minimum standards for licensure and oversight of the private investigator industry. Such standards should address the use of pretexting (pretending to be another person in order to gain access to someone's account or to gain information), establish a duty of care to those who are investigated, and prohibit the use of invasive practices, such as sorting through individuals' trash, employing electronic listening devices, etc.

D. Government Access to and Use of Personal Data

12. Limiting Government Access to Business and Financial Records

a. Problem

Increasingly, the government is gathering personal information from businesses and financial institutions. Companies such as ChoicePoint have multimillion dollar contracts with government agencies to supply them with personal information. The Fourth Amendment is often inapplicable because in a series of cases, including *United States v. Miller*[87] and *Smith v. Maryland,*[88] the Court has held that whenever a third party possesses personal information, there is no reasonable expectation of privacy. In the Information Age, it is impossible to live without extensive information about one's life existing in the hands of various third parties: phone companies, cable companies, Internet service providers, merchants, booksellers, employers, landlords, and so on. Thus, the government can increasingly obtain detailed information about people without ever entering their homes.

b. Legislative Mandate

There must be a way to engage in electronic commerce and routine transactions without losing one's expectation of privacy in personal data.

c. Specific Solution

Whenever the government attempts to access personal information from third parties that maintain record systems of personal information (databases or other records of personally identifiable information on more than one individual), the government should be required to obtain a special court order that requires probable cause and particularized suspicion that the information sought involves evidence of a crime. Excep-

87. 425 U.S. 435, 444 (1976).
88. 442 U.S. 735, 743–44 (1979).

tions should exist for reasonable law enforcement needs, including emergency circumstances.

13. Government Data Mining

a. Problem

The government is increasingly researching, planning, and initiating data-mining endeavors. Data mining entails combining and analyzing various records of personal information for suspicious patterns of behavior.[89] This was envisioned on a grand scale with the Total Information Awareness project. Due to a public outcry, Congress nixed the program from the public budget. But a recent Government Accountability Office (GAO) report, as well as the Technology and Privacy Advisory Committee report, demonstrates that a number of government data-mining programs are underway.[90] Data mining threatens to undermine a longstanding Fourth Amendment principle, which holds that dragnet searches—those without prior particularized suspicion—are impermissible.[91] Because there are serious inaccuracies in dossiers created by commercial data brokers, innocent people may be swept into these dragnets. Furthermore, the profiles and algorithms used to determine suspicious patterns of behavior are often kept secret, thus impeding public accountability or judicial oversight, and providing no way to determine the extent of use of certain factors such as race, religion, and First Amendment activity.

b. Legislative Mandate

There must be a way to ensure that government data mining does not permit law enforcement to engage in dragnet searches for prospective crimes. Where data mining is employed, it should occur in as open a manner as possible and have adequate judicial oversight and public accountability.

c. Specific Solution

Subject to judicial oversight and normal search warrant requirements, prospective subject-based data mining should be permitted. Subject-based data mining involves analyzing records where a specific individual or individuals are identified and there is particularized suspicion

89. U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 4 (2004).

90. *Id.* at 2–3; *see* TECH. AND PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM ix (2004), *available at* www.cdt.org/security/usapatriot/20040300tapac.pdf.

91. *Id.* at 22.

that they are involved in criminal activity.[92] Pattern-based data mining presents greater difficulties. Prospective pattern-based data mining involves analyzing record systems for various suspicious patterns of activity and then investigating those individuals who meet the particular pattern or profile.[93] Pattern-based data mining should be generally prohibited, as it involves a dragnet search. However, with appropriate judicial supervision, and with a way to preserve the principle of particularized suspicion, pattern-based data mining should be permitted in cases where there are specific and articulable facts that a particular crime will or has occurred, that a particular limited type of record system (not a broad dossier) has information that is necessary to the investigation (no alternatives are available), and where the inquiry into the record system is limited. Data-mining profiles must be approved by a court prior to their use and must be revealed to the public once the investigation is over. Moreover, as is currently done with wiretapping, government agencies engaging in data mining shall produce annual public reports to Congress describing the frequency and nature of their data mining activities.

14. Control of Government Maintenance of Personal Information

a. Problem

The Privacy Act of 1974 is riddled with loopholes. Despite a requirement that government agencies disclose new record systems, they can readily avert other substantive requirements simply by declaring that they want to exempt these records. For instance, in 2003, the Justice Department administratively discharged the FBI of its statutory duty to ensure the accuracy and completeness of over 39 million criminal records it maintains in its National Crime Information Center (NCIC) database.[94] That database provides over 80,000 law enforcement agencies with access to data on wanted persons, missing persons, gang members, as well as information about stolen cars, boats, and other information. Aside from agencies exempting themselves from the requirements of the Privacy Act, agencies have also employed the "routine use" exemption in such a broad fashion that it contravenes the intent of the Privacy Act. Another limitation of the Privacy Act is that it is very difficult for plaintiffs to obtain remedies. Plaintiffs must prove a "willful or intentional" violation of the Act,[95] which is difficult since many agency actions are negligent or reckless. Moreover, in *Doe v. Chao*,[96] the Court held that plaintiffs suing

92. *See* MARY DEROSA, DATA MINING AND DATA ANALYSIS FOR COUNTERTERRORISM 5 (2004), *available at* www.cdt.org/security/usapatriot/20040300csis.pdf.

93. *See id.* at 4–5.

94. Exemption of Federal Bureau of Investigation Systems—Limited Access, 28 C.F.R. § 16.96 (2004).

95. Privacy Act of 1974, 5 U.S.C. § 552a(g)(4) (2000).

96. 540 U.S. 614, 627 (2000).

for violations of the Privacy Act must prove actual loss in order to obtain minimum damages of $1,000 under the Privacy Act. Although many plaintiffs whose personal information is leaked by an agency suffer emotional distress, such emotional distress is not sufficient to constitute an actual loss for many courts. Accordingly, such plaintiffs are left without a remedy.

b. Legislative Mandate

There must be meaningful regulation that limits the collection of personal data, lists acceptable uses, guarantees accuracy, provides security, and restricts retention of personal information by government agencies, especially since they are acquiring more and more data about individuals.

c. Specific Solution

The Privacy Act must be updated. Over thirty years have gone by without a major reexamination of the Privacy Act, and one is sorely needed. Congress should empanel a new Privacy Protection Study Committee to examine government use of personal information comprehensively and make recommendations for legislation to update the Privacy Act. Specific changes shall include, but shall not be limited to: (1) limiting the routine use exception; (2) addressing the outsourcing of personal information processing to private-sector businesses; (3) strengthening the enforcement provisions of the Act; and (4) overturning *Doe v. Chao*[97] so that violations of the Act are remedied by minimum-damages provisions.

E. Privacy Innovation and Enforcement

15. Preserving the Innovative Role of the States

a. Problem

The recently enacted amendments to the FCRA preempted more protective state laws. As a result, states are less able to pass effective identity theft and privacy protections.

b. Legislative Mandate

The ability of states to innovate and experiment new approaches to privacy protections must be preserved.

97. *See id.*

c. Specific Solution

Most privacy protections in America have been created by state legislatures. The security breach law that resulted in ChoicePoint disclosing the recent sale of personal information to criminals was developed in California. Many of the most important protections in the FCRA originated in the states. Indeed, as Justice Brandeis once noted: "It 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."[98] Legislation crafted to address privacy problems should only employ "floor preemption," thereby allowing states to innovate more comprehensive protections for individual rights.

16. Effective Enforcement of Privacy Rights

a. Problem

Often, privacy rights are difficult to enforce. In many instances, it is difficult for victims to establish damages or causation when leaks or improper uses of their personal information result in identity theft or other harms. When a company discloses a person's data or violates its privacy policy by wrongfully transferring data to other companies or not providing adequate security, it is often difficult to prove actual damages. As a result, companies often lack sufficient accountability and sanctions when they engage in wrongdoing. About half of identity theft victims cannot tell how their personal information was even accessed, and thus do not know what parties should be pursued legally. Moreover, it is very difficult for identity theft victims to prove actual monetary damages even though they have spent considerable time fixing the harm and suffered great mental distress. With the ChoicePoint security debacle, people's personal information was sold to identity thieves. Although many did not suffer from identity theft, they still suffered harm, as they are now much more vulnerable to identity theft, have considerable mental unease, and must spend significantly more time monitoring their credit and accounts over a period that could last years.

b. Legislative Mandate

There must be a way to enforce privacy protections with meaningful sanctions, as well as meaningful redress to victims.

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

c. Specific Solution

There should be minimum liquidated damages provisions for companies that violate their privacy policies or that suffer a security breach due to negligence. Statutes must provide for individual redress. As part of an enforcement effort, individuals should be able to obtain an order to have a commercial data broker audited. In the event of leaked information, the most effective way to address the problem, in a way that avoids extensive class action litigation, is to authorize state attorneys general to fine companies and establish a fund where victims can make claims for disbursements.

IV. COMMENTARY

An earlier iteration of the Model Regime, which was released on March 10, 2005, received considerable attention. It was discussed in testimony at legislatures at the federal and state level. We received a number of very thoughtful comments and read many insightful discussions across the blogosphere.[99] The comments we received range from being very supportive of the Model Regime to being very critical. In this section, we respond to some of the comments and criticisms to the Model Regime.

A. General Comments

Eric Goldman, Assistant Professor at Marquette University School of Law, comments that the Model Regime has no cost/benefit analysis. He contends that "investments in increased privacy are like investments in security—they may end up being infrastructural investments that ultimately prove to be 'wasted' investments in terms of social welfare they create."[100] Many of the solutions proposed are not very costly. With respect to those that do impose costs on business, it must be noted that identity theft costs businesses tens of billions of dollars a year.[101] If the solutions have just a moderate effect on identity theft, they could pay for themselves.

Additionally, the business community has been loathe to recognize the costs of a lack of privacy to individuals, which includes lost time, frustration with direct marketing, and sometimes an increase in vulnerability

99. Jim Horning, Chief Scientist at McAfee Research (title listed for identification purposes only), and Rich Kulawiec helped us fix grammatical errors, and we are indebted to them for their kind efforts.

100. E-mail from Eric Goldman, Assistant Professor, Marquette University School of Law, to Daniel Solove, Associate Professor, The George Washington University Law School (Mar. 15, 2005, 06:51 PM) (on file with authors).

101. The FTC estimates that identity theft costs businesses about $33 billion each year. FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 6 (2003).

to violent crime. For instance, an anonymous commentator who works in the credit industry wrote to us that "since federal law right now does not hold them [identity theft victims] liable for fraud accounts or the misuse of their accounts, there really is no harm you are protecting against."[102] In contrast, we believe that identity theft causes significant harm to individuals. According to estimates, victims spend on average 175 hours and hundreds of dollars fixing the damage.[103] The harm is not simply measured in lost dollars; identity theft causes incalculable mental distress. Victims feel helpless, and the ongoing nature of identity theft exacerbates these feelings. Most other crimes have an ending point, in which victims can recover and begin to cope. Identity theft can last for years, even after detection, thus creating a perpetual sense of victimization that has no apparent ending. Moreover, victims are often financially crippled, and they can no longer engage in many financial transactions freely (such as obtaining loans, mortgages, etc.) until the damage to their credit is fixed. We can find little evidence that these costs to the consumer have been adequately taken into account by businesses. The Model Regime aims to force businesses to internalize some of the costs they impose on consumers. To this extent, it increases costs on businesses, but such increases are justified.

"Roy Owens" comments on Bruce Schneier's blog that defamation laws could address inaccurate information flows.[104] Defamation actions are costly to bring, and damages might be hard to prove. In egregious cases where errors result in denial of loans or wrongful arrest, plaintiffs might have a powerful case, but defamation law will not provide adequate incentives to protect against many of the smaller errors that often crop up in databases. These errors can cause harm, but not enough to support an expensive lawsuit. We also note that under the FCRA, consumer reporting agencies are shielded from defamation liability, except in cases where there was malice or willful behavior.[105] This legislative bargain gives the consumer reporting agencies flexibility to collect and report information as long as they use procedures to ensure "maximum possible accuracy."[106]

Eric Grimm, an attorney with Calligaro & Meyering, P.C., and others suggest that any regulatory regime would be compromised by the fact

102. E-mail from Anonymous, to Daniel Solove, Associate Professor, The George Washington University Law School (Apr. 4, 2005, 04:41 PM) (on file with authors).

103. Janine Benner et al., *Nowhere To Turn: Victims Speak Out on Identity Theft: A CALPRIG/Privacy Rights Clearinghouse Report* (2000), http://privacyrights.org/ar/idtheft2000.htm.

104. Posting of Roy Owens to Schneier on Security: ChoicePoint Says "Please Regulate Me," http://www.schneier.com/blog/archives/2005/03/choicepoint_say.html (Mar. 9, 2005, 04:06 PM). Bruce Schneier is the founder and CTO of Counterpane Internet Security, Inc. and author of numerous books on data security. *See* BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD (2003); BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2000).

105. 15 U.S.C. § 1681h(e).

106. *Id.* § 1681e(b).

that agencies may be captured by the companies that they regulate.[107] We do not disagree, but we do not believe that this is a reason to reject regulatory solutions. Agency capture is a risk with any regulatory action. Despite agency capture problems, few would argue that we are better off without regulatory regimes for food, drugs, the environment, auto safety, and the like. Moreover, the risk of agency capture is mitigated where state attorneys general can prosecute wrongdoing, where individuals have a private right of action, and where federal regulation is a floor, allowing states to create broader protections. All of these are central features of our Model Regime.

Matthew Miller, an attorney at Hughes & Luce LLP, blogging on Privacy Spot, praises the Model Regime.[108] Miller suggests that the Model Regime address how long data should be retained by entities.[109] Jim Horning, Chief Scientist of McAfee Research,[110] also makes a similar suggestion.[111] Many privacy laws set an upward limit on the amount of time private entities can store personal information, including the Cable Communications Policy Act,[112] the Video Privacy Protection Act,[113] and the FCRA.[114] We have incorporated this suggestion into the Model Regime.

Dennis Bailey, author of the book *The Open Society Paradox,* argues that "the free flow of data provides significant economic and social benefits and regulations that attempt to restrict it only serve to hurt the economy."[115] We agree that the collection and use of personal information can provide substantial benefits, but we disagree that any regulation of the free flow of data will necessarily impede economic development. We live in a highly regulated society. At the time of the New Deal, similar arguments were made in support of *laissez faire*. Indeed, one response to the problems of the Industrial Age (pollution, poor working conditions, etc.) was that any regulation would injure economic development. Regulation is not necessarily in tension with economic devel-

107. E-mail from Eric Grimm, Attorney, Calligaro & Meyering, P.C., to Daniel Solove, Associate Professor, The George Washington University Law School, and Chris Hoofnagle, Director, Electronic Privacy Information Center, West Coast Office (Mar. 20, 2005, 04:48 PM) (on file with authors).

108. *See* Matt Miller, *Draft of a Model Privacy Regime (Part One)* (Mar. 14, 2005), http://privacyspot.com/?q=node/view/593; Matt Miller, *Draft of a Model Privacy Regime (Part Two)* (Mar. 14, 2005), http://privacyspot.com/?q=node/view/595.

109. Matt Miller, *Draft of a Model Privacy Regime (Part Two)*, *supra* note 108.

110. Title listed for identification purposes only.

111. E-mail from Jim Horning, Chief Scientist, McAfee Research, to Daniel Solove, Associate Professor, the George Washington University Law School, and Chris Hoofnagle, Director, Electronic Privacy Information Center (Mar. 15, 2005, 04:43 PM) (on file with authors).

112. 47 U.S.C. § 551(e) (2000).

113. 18 U.S.C. § 2710(e) (2000).

114. 15 U.S.C. § 1681c (2000).

115. Dennis Bailey, *The Whole Kit and Caboodle—Solove and Hoofnagle Go for Regime Change*, Mar. 21, 2005, http://www.opensocietyparadox.com/mt/archives/000517.html; *see also* DENNIS BAILEY, THE OPEN SOCIETY PARADOX 157–58 (2004).

opment, and many regulations benefit the economy and support innovation where there have been market failures.

Moreover, the free flow of information and maximization of economic development are not the only normative ends of our society. Information regulation can serve to promote fairness or prevent a panoply of types of discrimination. For example, since the 1970s, it has been illegal under federal anti-discrimination laws to exclusively rely upon an arrest record to make hiring decisions, as minorities are more heavily targeted by law enforcement:

> Blacks and Hispanics are convicted in numbers which are disproportionate to Whites and . . . barring people from employment based on their conviction records will therefore disproportionately exclude those groups. Due to this adverse impact, an employer may not base an employment decision on the conviction record of an applicant or an employee absent business necessity.[116]

Dennis Bailey suggests in his blog that personal information should generally be public, and that regulation should only focus on the harmful uses of personal information:

> If information is being used to deprive someone of their freedoms, such as the right to vote or the ability to get a job; or used to defraud someone through identity theft then the full weight of the law should be applied. But to regulate data simply on the basis of privacy is not something I support.[117]

It is not practical to take such an approach. Limiting the public disclosure of certain data as a precaution is a first line of defense for individuals such as judges, workers at medical clinics performing abortions, and domestic violence victims. The use of criminal law alone to address identity theft has been a failure. Gartner, Inc., a research firm, estimates that far less than one percent of identity thefts result in a conviction.[118] A United States GAO Report describes in compelling detail the difficulties with criminal investigation and prosecution of identity theft cases.[119]

Jim Harper, Director of Information Policy Studies at the Cato Institute, comments that regulation "at its best proscribes a set of actions in order to prevent harm," and criticizes regulations that seek to prevent behavior not tied to "monetary loss, property loss, or mental distress that causes physical symptoms, loss of work, or destruction of family and pro-

116. Gregory v. Litton Systems, Inc., 472 F.2d 631, 632 (9th Cir. 1972); EEOC, Policy Guidance No. N-915-061, POLICY GUIDANCE ON THE CONSIDERATION OF ARREST RECORDS IN EMPLOYMENT DECISIONS UNDER TITLE VII OF THE CIVIL RIGHTS ACT OF 1964, at 4 (1990).

117. Bailey, *supra* note 115.

118. Stephen Mihm, *Dumpster-Diving for Your Identity*, N.Y. TIMES MAG., Dec. 21, 2003, at 42. The figure is less than one in seven hundred identity thefts resulting in conviction.

119. U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE HONORABLE SAM JOHNSON, HOUSE OF REPRESENTATIVES, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED 17–18 (June 2002), *available at* http://www.gao.gov/new.items/d02766.pdf.

fessional relationships."[120] Harper contends that common-law torts could address the problems much more effectively than our Model Regime of regulatory provisions.

The problem with applying common-law torts is that data privacy harms are often ill-defined and under-developed in the common law. To what extent is an individual harmed if an intruder enters her home and looks through her papers but does not steal anything and leaves without a trace? To what extent is an individual harmed whose personal data is leaked by a company such as ChoicePoint but who thus far has not been victimized in an identity theft? Perhaps the common law could better address data privacy if it had a different conception of harm. As Warren and Brandeis noted in their seminal article on privacy, the law evolved to address more than just property loss and physical harm.[121] After the Warren and Brandeis article, the law developed to recognize the more incorporeal and emotional harms associated with privacy violations.[122] But the common law has a long way to develop. It must recognize duties on the part of data brokers such as ChoicePoint. It must address issues of causation, as it is often impossible for victims to prove how their identity was stolen and which companies were responsible for the theft of their personal data. It must develop a concept of harm that does not depend upon severe emotional distress, reputational harm, or actual monetary loss, as such harms are very difficult to prove when people's data is merely leaked, when people are denied access to their information, or when people's information is improperly transferred to other entities. Common-law torts can certainly supplement a regulatory regime, but they cannot serve as an adequate replacement for it without significant development.

Michael Shankey, CEO of BRB Publications, Inc., a company that monitors government record access policies, made significant comments on the Model Regime.[123] Shankey notes that the Model Regime "would be more useful if it recognized the existence of different vendors and what they do, rather than to primarily lump them together as 'data brokers.'"[124] Shankey describes five general categories of public record vendors: (i) "proprietary database vendors," which are companies that "combine public sources of bulk data and/or online access to develop their own database product(s)" and "purchase or license records from

120. E-mail from Jim Harper, Director of Information Policy Studies, The Cato Institute, to Daniel Solove, Associate Professor, The George Washington University Law School, and Chris Hoofnagle, Director, Electronic Privacy Information Center (Mar. 21, 2005, 3:59 PM) (on file with authors).

121. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890).

122. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 392 (1960).

123. E-mail from Michael Shankey, Chief Executive Officer, BRB Publications, Inc., to Daniel Solove, Associate Professor, The George Washington University Law School, and Chris Hoofnagle, Director, Electronic Privacy Information Center (Mar. 3, 2005) (on file with authors).

124. *Id.*

other information vendors,"[125] (ii) "gateways," which are companies that "provide automated electronic gateway to Proprietary Database Vendors or to government agencies online systems,"[126] (iii) "search firms," which are companies that "furnish public record search and document retrieval services using online services and/or through a network of specialists, including their own employees or correspondents,"[127] (iv) "verification firms," which are companies that ensure information provided to employers and businesses is correct,[128] and (v) "private investigation firms," which are companies that "use public records as tools rather than as ends in themselves, in order to create an overall, comprehensive 'picture' of an individual or company for a particular purpose."[129] These distinctions are informative and should be considered when legislative packages are introduced to address the field of commercial data brokers. We also note that in some cases, commercial data brokers perform many of the different functions described by Shankey.

Although commercial data broker ChoicePoint did not comment on the Model Regime, the company did announce a series of changes to its business model in March 2005. ChoicePoint stated that it "will discontinue the sale of information products that contain sensitive consumer data, including Social Security and driver's license numbers, except where there is a specific consumer-driven transaction or benefit, or where the products support federal, state or local government and criminal justice purposes."[130] The company also has created "an independent office of Credentialing, Compliance and Privacy that will . . . oversee improvements in customer credentialing processes, the expansion of a site visit-based verification program and implementation of procedures to expedite the reporting of incidents."[131]

We think ChoicePoint's reforms are inadequate to address the privacy implications of the commercial data broker industry. First, ChoicePoint's reforms do not bind the company's competitors, and so other commercial data brokers can continue to sell SSNs and other personal information.[132] Indeed, ChoicePoint is now at a competitive disadvantage with other lesser-known data brokers, such as Tracers Information

125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.*
130. News Release, ChoicePoint, ChoicePoint to Exit Non-FCRA, Consumer-Sensitive Data Markets; Shift Business Focus to Areas Directly Benefiting Society and Consumers (Mar. 4, 2005), *available at* http://www.choicepoint.com/choicepoint/news.nsf/IDNumber/TXK2005-5381565?OpenDocument.
131. *Id*.
132. According to journalist Jonathan Krim: "So far, neither those moves nor revelations of a series of breaches at major banks and universities has curbed a multi-tiered and sometimes shadowy marketplace of selling and re-selling personal data that is vulnerable to similar fraud." Jonathan Krim, *Net Aids Access to Sensitive ID Data, Social Security Numbers Are Widely Available*, WASH. POST, Apr. 4, 2005, at A01.

Specialist Inc., Merlin, and Intellius.[133] ChoicePoint's reforms resulted in the company forgoing approximately $20 million in revenue.[134] Smaller companies have not experienced the public attention that ChoicePoint, LexisNexis, and Acxiom have received, and thus may not adopt reforms to protect consumers.

Second, ChoicePoint is still going to sell its unregulated "public records" reports to small businesses, albeit with the SSN or driver's license number "truncated."[135] Large businesses and law enforcement will still be able to obtain the full report with sensitive information. It is not clear how the SSN will be truncated. Some companies obscure the first five digits while others block the last four. Without a full redaction of the SSN, it may be possible to piece the SSN together from several sources.

Third, the public records reports sold by ChoicePoint have been shown to be highly inaccurate. According to a report by Pam Dixon of the World Privacy Forum, ChoicePoint's public information reports have a very high error rate.[136] In her sample, 90% of the reports obtained contained errors; frequently these errors were serious, such as individuals being identified by the wrong sex.[137] Dixon's initial findings are supported by anecdotal stories of other individuals who have obtained their unregulated ChoicePoint reports. Elizabeth Rosen, a victim of the ChoicePoint privacy breach, found that five of the seven pages of her report contained errors.[138] Rosen's report erroneously indicated that she was the officer of businesses in Texas, that she maintained private mail boxes in Texas and Florida," and that she owned businesses, including "Adopt-A-Classroom."[139] Privacy researcher Richard Smith obtained his ChoicePoint report and wrote that his report "contain[ed] more misinformation than correct information."[140] Deborah Pierce's National Comprehensive Report from ChoicePoint falsely indicated a "possible Texas criminal history."[141]

133. Brian Bergstein, *ChoicePoint Tries to Find Its Footing in Anti-Fraud Effort*, ASSOC. PRESS, Sept. 30, 2005.

134. Ann Carrns & Valerie Bauerlien, *ChoicePoint Curtails Business, Changes Method to Protect Data*, WALL ST. J., June 24, 2004, at A10.

135. "ChoicePoint will continue to serve most of its core markets and customers, but these actions will have an impact on the scope of products offered to some customers and the availability of information products in certain market segments, particularly small businesses. The transition will begin immediately and is expected to be substantially completed within 90 days." News Release, ChoicePoint, *supra* note 129.

136. *See* Martin H. Bosworth, *USA PATRIOT Act Rewards ChoicePoint: "Identity Verification" Exposes Consumers to Risks*, May 13, 2005, http://www.consumeraffairs.com/news04/2005/patriot01.html.

137. *Id.*

138. Bob Sullivan, *ChoicePoint Files Found Riddled With Errors: Data Broker Offers No Easy Way to Fix Mistakes, Either*, Mar. 8, 2005, http://msnbc.msn.com/id/7118767.

139. *Id.*

140. Posting of Richard Smith to Free Public, http://www.freerepublic.com/forum/a3b1251464594.htm (May 28, 2001, 06:23 PDT).

141. Sullivan, *supra* note 138.

Fourth, individuals will have access, but not correction rights, with respect to ChoicePoint's unregulated public information reports. ChoicePoint claims that it cannot correct these reports because they are generated from public records. However, this claim is deceptive—the problem is that ChoicePoint is mixing up public-record information between individuals. The public records are correct, but they are attached to people to whom they do not pertain.

Fifth, nothing binds ChoicePoint to its promise to maintain its reformed policies. In recent years, many large companies including eBay.com, Amazon.com, Drkoop.com, and Yahoo.com, changed users' privacy settings or altered privacy policies to the detriment of users.[142] ChoicePoint is legally in a better position to renege on its promises, as it does not acknowledge a direct relationship with consumers that could be the basis of a legal action. ChoicePoint's "consumers" are the businesses that buy data from the company.

Sixth, ChoicePoint is still reserving the right to sell "sensitive" personal information to businesses in a large number of contexts. ChoicePoint's release states that sensitive information will be sold to "[s]upport consumer-driven transactions where the data is needed to complete or maintain relationships . . . [p]rovide authentication or fraud prevention tools to large, accredited corporate customers where consumers have existing relationships . . . [a]ssist federal, state and local government and criminal justice agencies in their important missions."[143] These categories articulated by ChoicePoint are broad and ill-defined. What specifically falls under "consumer-driven transactions"? When is data "needed to complete or maintain relationships?" Under this standard, ChoicePoint can decide what constitutes a consumer benefit. In the past, ChoicePoint has declared that selling personal information benefits consumers in the aggregate, and thus individuals should have no right to opt-out of ChoicePoint's databases.[144] Simply put, ChoicePoint's idea of what benefits consumers differs from what consumers and consumer advocates think benefits them.

Seventh, the ChoicePoint policy allows the company to sell full reports for anti-fraud purposes. While in theory this exception seems ap-

142. Chris Jay Hoofnagle, *Consumer Privacy In the E-Commerce Marketplace*, *in* THIRD ANNUAL INSTITUTE ON PRIVACY LAW 1339, 1360 (2002), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=494883#PaperDownload.

143. News Release, ChoicePoint, *supra* note 130.

144. The privacy statement mailed to individuals who request their unregulated AutoTrackXP report reads in part:

> We feel that removing information from these products would render them less useful for important business purposes, many of which ultimately benefit consumers. ChoicePoint DOES NOT DISTRIBUTE NON-PUBLIC INFORMATION (as defined in the Principles) TO THE GENERAL PUBLIC PURSUANT TO SECTION V(C) OF THE PRINCIPLES. The general public therefore has NO direct access to or use of NON-PUBLIC INFORMATION (as defined in the Principles) from ChoicePoint whatsoever.

Letter from Gina Moore to Chris Hoofnagle, *supra* note 62, at 1.

propriate, almost any transaction can have some fraud risk. If a broad fraud exemption is maintained, it will allow the sale of reports even when the fraud risk is minimal or a proxy for wishing to collect information for some other purpose.

Finally, ChoicePoint's proposal does not at all limit sale of personal information to law enforcement. The company continues to sell personal information to 7,000 federal, state, and local law enforcement agencies.[145]

B. Comments on Specific Proposals

1. Universal Notice

Eric Goldman questions the breadth of the definition in this proposal and notes that "virtually every Internet company would be covered by the standard."[146] We disagree that the standard would cover virtually any Internet company. It would cover any company that has a primary business of selling personal information.

Jim Horning comments that in light of the digital divide, notice should be available to those who are not online.[147] Because our original proposal was based on the use of a Web site to provide such notice, we have adjusted the Universal Notice section to ensure that those who are offline also receive notice.

An anonymous commentator who works in the credit industry writes that the definition of commercial data broker should not include consumer reporting agencies because "they are well known and they have specific obligations that cover most of the concerns enumerated in your paper."[148] We agree with this assessment. The purpose of the Model Regime is primarily to expand the duties on companies that have functions falling outside the FCRA. However, some portions of the Model Regime do impose greater responsibilities on traditional consumer reporting agencies, such as proposal #4.

2. Meaningful Informed Consent

Rich Kulawiec suggests that the exemption from consent for fraud investigations is too broad; individuals should receive notice when an investigation does not result in a finding of fraud.[149] Kulawiec argues that this would prevent baseless uses of data for anti-fraud purposes and allow people to correct data that led the business to suspect fraud. We ad-

145. *Testimony of Derek Smith*, *supra* note 38.

146. E-mail from Eric Goldman to Daniel Solove, *supra* note 100.

147. ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (2002).

148. E-mail from Anonymous to Daniel Solove, *supra* note 102.

149. E-mail from Rich Kulawiec, to Daniel Solove, Associate Professor, The George Washington University Law School, and Chris Hoofnagle, Director, Electronic Privacy Information Center (Mar. 12, 2005, 12:53 PM) (on file with authors).

justed this principle to allow use without consent for "reasonable" fraud investigations. Providing notice each time a company used data to perform some anti-fraud function would be burdensome. We think requiring a condition of reasonableness for investigations will prevent arbitrary uses of personal information under the exemption.

3. One-Step Exercise of Rights

"Curt Sampson," commenting on Bruce Schneier's blog,[150] and Jim Horning[151] make a number of important points regarding the security of any centralized source created to manage privacy rights. Sampson correctly points out that such a system will have problems in identifying and authenticating individuals who seek access to it.[152] In lieu of such a system, Sampson proposes that commercial data brokers adopt an opt-in business model, where they have to contact the data subjects and establish a relationship with each.[153] We believe that such an alternative might result in a barrage of unwanted contact to individuals given the many companies that trade in people's data. Many of the identification and authentication issues Sampson raises are addressed successfully by the Federal Trade Commission (FTC) in its Do-Not-Call Telemarketing Registry. The FTC uses "automatic number identification" to verify that an individual enrolling in the system is calling from the affected number.[154]

Serious security issues are not presented by requiring the commercial data brokers to register and provide information about their activities online. The security issues arise when individuals can exercise rights at the registry. This can be addressed in several ways. With respect to the congressionally mandated central source for free consumer reports, the individual can go to a single Web site, but then be passed off to an individual consumer reporting agency for identification and authentication. A privacy registry could operate in the same way, with the individual reading about different commercial data brokers on the central registry, but then pursing the exercise of certain rights (especially access and correction) with the individual companies.

In some instances, the harms from abuse are not significant enough to outweigh the benefits of a central registry. For instance, some direct marketing groups objected to the Do-Not-Call Registry on the basis that an imposter could secretly opt-out individuals by placing them on the Do-Not-Call Registry without their consent. We think the FTC properly

150. Posting of Curt Sampson to Schneier on Security: Ideas for Privacy Reform, http://www.schneier.com/blog/archives/2005/03/ideas_for_priva.html (Mar 14, 2005, 10:56 PM).

151. E-mail from Jim Horning, Chief Scientist, McAfee Research, to Daniel Solove, Associate Professor, The George Washington University Law School, and Chris Hoofnagle, Director, Electronic Privacy Information Center (Mar. 15, 2005, 07:44 PM) (on file with authors).

152. Posting of Curt Sampson to Schneier on Security: Ideas for Privacy Reform, *supra* note 150.

153. *Id.*

154. Privacy Act Notice, 68 Fed. Reg. 37494, 37494 (June 24, 2003).

resolved this conflict by still allowing individuals to opt-out without the hassle of burdensome authentication because missing some telemarketing is an acceptable harm in exchange for ease of use. Similarly, with respect to opting out of financial services information sharing, there should not be a significant hurdle or a requirement to go to each individual company to authenticate and opt-out. Instead, the FTC could monitor enrollments in the system and investigate those who appear to have a fraudulent pattern (multiple opt-outs from the same IP address, opt-outs that come in alphabetical or numerical order, etc).

To address Curt Samson's concerns, we have adjusted the Model Regime so that certain rights can be exercised at the centralized system, but others will have to be pursued with individual companies.

"David Mohring," commenting on Bruce Schneier's blog, raises a different issue with the centralized source: it could become a honeypot for law enforcement and lawyers seeking personal information.[155] This indeed is a risk. The FTC, in creating the Do-Not-Call Registry, established a routine use allowing the agency to disclose enrollment information to law enforcement agencies.[156] To avoid a similar development with respect to any newly created system, we have altered the Model Regime to specify that government officials seeking access to personal information in the registration system should be required to obtain a search warrant with probable cause and to minimize the data acquisition to only that which is needed for a specifically identified law enforcement purpose.

Rich Kulawiec comments that the Do-Not-Call Registry has a feedback loop that our system lacks.[157] That is, if one continues to receive telemarketing after enrollment, there is a possibility that someone is violating the law. He rightly asks what mechanisms will ensure compliance with our proposed system. This is a legitimate concern, but a fully developed approach would create rights that would help individuals identify when something wrong is afoot, and strong penalties (suggested by many who commented on the Model Regime) would serve as a deterrent to prevent misuse of personal data. To further develop a feedback mechanism for individuals as data subjects, we have added a provision to the access section calling upon commercial data brokers to not only provide a copy of a report, but also an accounting of the entities to which it has been disclosed. This right exists in the FCRA context, where the individual can obtain a complete list of all entities that received a consumer report.[158] Therefore, in the access and accuracy section (proposal #5), we

155. Posting of David Mohring to Schneier on Security: Ideas for Privacy Reform, http://www.schneier.com/blog/archives/2005/03/ideas_for_priva.html (Mar. 12, 2005, 06:56 AM).

156. Privacy Act Notice, 68 Fed. Reg. at 37496.

157. E-mail from Rich Kulawiec to Daniel Solove and Chris Hoofnagle, *supra* note 149.

158. 15 U.S.C. § 1681b(b)(2) (2000).

have added a provision to enable an individual to seek such an accounting of a commercial data broker's disclosures.

4. Individual Credit Management

"No id please," commenting on Bruce Schneier's blog, notes that credit card companies have architected the current credit system that has put consumers at risk, and then turned this risk into a business opportunity to market credit monitoring.[159] This comment is correct—the information business has turned many of its problems into new profit opportunities, such as identity theft insurance, which can cover lost wages and fees associated with remedying the crime. Dennis Bailey observes: "I use CreditWatch from Experian and it gives me peace of mind. Of course [Solove and Hoofnagle] are asking the companies to give away a profitable service for free."[160] It strikes us as unfair for companies to make a profit selling a service to protect consumers from problems created by these very companies themselves.[161] Consumer reporting agencies contend that people's information would be much more safe and secure if they signed up for the agencies' credit monitoring services.[162] However, under the FCRA, consumer reporting agencies are required to maintain procedures to ensure "maximum possible accuracy," and nowhere in the statute does it authorize companies to charge a fee for such service.[163] We believe that under their FCRA duty to maintain the maximum possible accuracy, consumer reporting agencies should provide free credit monitoring to individuals.[164] Therefore, we have added to this provision free credit monitoring to individuals who desire such protection.

"Matthew B.," commenting on Bruce Schneier's blog, argues in support of the security freeze proposal.[165] He points out that it will serve as an effective identity theft "detection approach" because it will notify individuals where there may be wrongdoing.[166] Such an approach is useful

159. Posting of No id please to Schneier on Security: ChoicePoint Says "Please Regulate Me," http://www.schneier.com/blog/archives/2005/03/choicepoint_say.html (Mar. 9, 2004, 04:12 PM).

160. Bailey, *supra* note 115.

161. The Federal Trade Commission has labeled unfair a scheme where marketers sent unwanted popup messages to users of Microsoft Windows computers and then offered these users software to block the messages, thereby seeking to profit from the very harm the company caused. *See* FTC v. D Squared Solutions, LLC, No. AMD 03-CV3108 (N.D. Md. Nov. 6, 2003).

162. Complaint at Exhibit B, In the Matter of Experian (before the Federal Trade Commission) (2003), *available at* http://www.epic.org/privacy/Experian (follow "Exhibit B" hyperlink).

163. 15 U.S.C. § 1681e(b) (2000).

164. Letter from Chris Jay Hoofnagle, Director, Electronic Privacy Information Center, to the Federal Trade Commission (Sept. 16, 2003), *available at* http://epic.org/privacy/experian (arguing that a consumer reporting agency promoting its subscription credit monitoring service by capitalizing on its own failure to adequately fulfill its duty to maintain maximum possible accuracy violated the Fair Consumer reporting Act).

165. Posting of Matthew B. to Schneier on Security: Ideas for Privacy Reform, http://www.schneier.com/blog/archives/2005/03/ideas_for-priva.html (Mar. 15, 2005, 08:30 AM).

166. *Id.*

because in a typical identity theft situation, the impostor will make a number of attempts to apply for credit in the victim's name. Notice of inquiries will alert an individual to wrongdoing; the freeze will stop the actual granting of credit, assuming that the impostor cannot himself lift the freeze.

Rich Kulawiec suggests that notice of access or attempted access to personal information should not be delivered by e-mail because of security risks.[167] Our approach would give the individual a choice regarding which method of notice could be used; those concerned about e-mail security could choose notice by postal mail.

An anonymous commentator who works in the credit industry writes that "[r]equiring a notice to be sent by a . . . [consumer reporting agency] each time someone makes an inquiry or accesses your consumer report is just not practical."[168] The anonymous commentator is correct. Our original proposal would have required notice to be given each time a company does a routine review of an existing consumer's credit. The Model Regime is not concerned with routine account review, but rather with new accounts of credit and new inquiries made on the file. We have accordingly altered the Model Regime so that new persons or entities (those that do not currently have a business relationship with the consumer) that access or make an inquiry on the report will trigger a notice to the consumer.

The same commentator writes that "[a]llowing full consumer control over their credit file . . . is not practical. . . . because [of] the need to have a center available 24/7/365 to allow consumers to have access to their file."[169] This would "create a cost structure that would destroy the industry."[170] Certainly there will be costs involved with a credit freeze, but under the current information architecture, individuals have no tools to proactively shield themselves from identity theft. There are certain pressure points that can be used to address identity theft. One is limiting access to personal information, an approach that commercial data brokers have made impractical. The other approach is to limit access to the consumer report, because without it, companies will not grant credit to impostors. We think consumers should have the ability to limit access to the reports. An increasing number of states are in accord with this position.[171]

167. E-mail from Rich Kulawiec to Daniel Solove and Chris Hoofnagle, *supra* note 149.

168. E-mail from Anonymous to Daniel Solove, *supra* note 102.

169. *Id.*

170. *Id.*

171. California, Louisiana, Texas, and Vermont have credit freeze laws. *See* CAL. CIV. CODE § 1785.11.2–.11.6 (West 2005); LA. REV. STAT. ANN. § 9:3571.1 (2005); TEX. BUS. & COM. CODE ANN. § 20.01 (Vernon 2005); VT. STAT. ANN. tit. 9, § 2480a (2004).

5. Access to and Accuracy of Personal Information

Michael Shankey correctly notes that our original proposal justified access, accuracy, and correction rights by listing uses of personal information (pre-employment screening and credit granting) that are already regulated and subject to the very rights we seek.[172] Our reliance on those uses of information was misplaced, and thus we have removed those justifications. We still think that these rights are appropriate for reports sold by commercial data brokers, as law enforcement and other entities use them to make decisions affecting people's lives.

Shankey also comments that correction rights are difficult to execute because the "originating data comes from the government agencies [and] the database vendor is merely reporting what was in the record."[173] While it is true that individuals have to pursue correction rights with individual government agencies, as noted above, much of the problem stems from the fact that although the public records are correct, they are attached to the wrong individuals.

6. Secure Identification

"Anonymous," commenting on Bruce Schneier's blog, warns that legislative mandates defining security can cause problems because they stifle innovation and technological development.[174] We agree with this comment. In our Model Regime, we avoided stating specific security standards. Privacy laws that address security standards rarely define specific security measures; instead, they create a burden to maintain "reasonable procedures." These standards place a continuing burden upon data collectors to employ good practices rather than set the standards in stone. However, this does not mean that the law must avoid all specific measures. In particular, some existing security measures that have proven to be ineffective—such as the use of SSNs as passwords—should be specifically limited. There may be some security measures that have proven so effective that they should be required. Such instances should be employed sparingly, as the law should maximize flexibility and continued security innovation.

"Gary," commenting on Bruce Schneier's blog, suggests that the SSN be made public but that the law should prohibit its use as a password.[175] We agree that the SSN should not be used as a password. How-

172. E-mail from Michael Shankey to Daniel Solove and Chris Hoofnagle, *supra* note 123.

173. *Id.*

174. Posting of Anonymous to Schneier on Security: ChoicePoint Says "Please Regulate Me," http://www.schneier.com/blog/archives/2005/03/choicepoint_say.html (Mar. 9, 2005, 06:34 PM).

175. Posting of Gary to Schneier on Security: Ideas for Privacy Reform, http://www.schneier.com/blog/archives/2005/03/ideas_for_priva.html (Mar. 15, 2005, 04:45 AM). This proposal resembles in some respect Lynn LoPucki's proposal to have a public system of identification. Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 120 (2001). For an extensive critique of LoPucki's system, see Daniel J. Solove, *Identity Theft, Privacy, and the Architec-*

ever, the SSN is an individual's "account number" with the Social Security Administration, and making such a financial account number public could create opportunities for fraud and abuse.

Jim Horning and several others are critical of the employment of passwords: (i) users choose bad passwords, (ii) they tend to use the same password for many different purposes, and (iii) they forget good passwords.[176] All of these problems are valid concerns, but the current system is a password system that is among the worst that could possibly be devised. SSNs (i) are used as passwords, (ii) are far from secret, (iii) can readily be found out with minimal effort, (iv) are very difficult to change, and (v) are used on countless accounts and record systems. The Model Regime's password proposal eliminates several of these problems. First, passwords will vary with different accounts, so a thief finding out a password will not unlock everything. Second, passwords can readily be changed, so once the identity theft is detected, people can readily render the stolen password useless. Third, it will be much more difficult for the average identity thief to guess people's passwords. Thieves can of course do this, but it will make identity thefts more difficult. It is difficult to completely eliminate identity theft, but the Model Regime makes it much harder to engage in and makes it easier for victims to halt it once it happens. The problem of forgetting passwords can be addressed by having people supply answers to questions such as naming their favorite pet's name or favorite color.

We have received some interesting technological solutions for identification and authentication, but we were reluctant to adopt any without a more thorough understanding of their implications, feasibility, usability, and potential problems.[177] We are open to other approaches that provide more flexibility and security than passwords. For now, we believe that passwords are an easy measure that will have a significant impact on reducing the incidence and severity of identity theft. While such a solution is not perfect, its great virtue is that it supplies a substantial advance in effectiveness with relative simplicity.

ture of Vulnerability, 54 HASTINGS L.J. 1227, 1262–66 (2003). For LoPucki's response, see Lynn LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003).

176. E-mail from Jim Horning to Daniel Solove and Chris Hoofnagle, *supra* note 110; E-mail from Scott Minneman, Student, The George Washington University Law School, to Daniel Solove, Associate Professor, The George Washington University Law School (Mar. 11, 2005, 08:32 PM).

177. For example, Jim Horning suggested "PwdHash" as one possible approach to addressing the problem of using the same password for different services. Web Password Hashing, http://crypto.stanford.edu/PwdHash/ (last visited Apr. 3, 2005). PwdHash is an Internet Explorer plug-in "that transparently converts a user's password into a domain-specific password." Web Password Hashing, *supra.* This would reduce the risk associated with individuals using the same password at different Web sites.

7. Disclosure of Security Breaches

Eric Goldman suggests that individuals be able to control whether security breach notifications are received, and the standard for receiving notifications should be opt-in.[178] We agree that individuals should be able to opt-out of receiving notifications, should they wish. However, setting an opt-in standard will give companies an incentive to hide the option from the consumer, or charge consumers for receiving this basic information.

In discussions about a federal security breach disclosure law, there has been debate concerning when a company should be required to disclose a security breach. Some argue that disclosure should triggered only if there is a "reasonable basis of substantial consumer harm" or a "reasonable basis that the disclosure may result in a significant risk of identity theft." The problem with such thresholds, however, is that they leave the determination for "reasonable basis" to self-interested companies. With most of the security breaches that were announced in 2005, the companies insisted that the risk of identity theft was small to nonexistent. Thus, under such a threshold, hardly any companies would make the disclosure. Moreover, it is unclear what a "significant risk of identity theft" or "substantial consumer harm" means. If a company decides that it must disclose, then it is also conceding that there is a "significant risk" of harm from its breach, which is a very difficult thing for a company to concede. Instead, most companies will not want to concede that they have created a risk of harm to consumers, let alone a significant one, as this will create a public relations nightmare. Given the strong disincentive for companies to admit publicly that a security breach could cause harm to consumers, a standard involving "harm" would lead to minimal to no disclosures. Additionally, it is often hard to determine whether a disclosure will create a significant risk of identity theft or harm, so nearly all companies that suffer breaches could claim in good faith not to have to disclose. Finally, security breaches may occur for purposes beyond identity theft. Unauthorized access may be sought in order to locate a person, to engage in stalking, or to embarrass them.

8. Social Security Number Use Limitation

Many wrote to express support of this provision in particular. Several wrote that the SSN should be considered to be compromised because of its widespread use and availability. Thus, it should never be used as a password.

178. E-mail from Eric Goldman to Daniel Solove, *supra* note 100.

9. Access and Use Restrictions for Public Records

No commentary.

10. Curbing Excessive Uses of Background Checks

Jim Horning argues that the background check section is not relevant to the problems we aimed to address in the Model Regime.[179] However, the growth of the commercial data broker industry has been in large part due to employers performing background checks, even in cases where the job has no security function. Outside the pre-employment context, shoddy, electronic-only background checks have become increasingly less expensive. There has to be some way to put balance back into this situation and limit the contexts in which background checks are performed.

Dennis Bailey contends that many nonsecurity jobs could have security implications; he gives the example of felons working for service companies that might assault people in their homes.[180] We think that some line must be drawn that establishes categories of jobs that are available without a background check. Almost any job imaginable has some security implication, but the connection is often attenuated. We think the line that we have drawn, one that allows background checks for caretakers, handlers of large sums of money, and for functions articulated by Congress in the Polygraph Act, properly balances employer and employee interests.

Michael Sankey of BRB Publications, Inc. criticizes the background check section, and notes that "the employer can be sued for negligent hiring if [pre-employment screens] are not done."[181] We think this is precisely the reason why a line must be drawn. As pre-employment screening becomes cheaper, it becomes difficult for employers to refrain from engaging in prescreening. One could foresee the day when even the most menial job will require a clean record. Obviously, if the Model Regime restricts an employer from conducting a background check for a particular position, the employer shall not be deemed negligent for not conducting one.

11. Private Investigators

Jim Horning recommends against limiting the private investigator profession, arguing that private investigators are not central to the problems at issue in the Model Regime.[182] We disagree. Private investigators

179. E-mail from Jim Horning to Daniel Solove and Chris Hoofnagle, *supra* note 110.
180. Bailey, *supra* note 114.
181. E-mail from Michael Sankey to Daniel Solove and Chris Hoofnagle, *supra* note 123.
182. E-mail from Jim Horning to Daniel Solove and Chris Hoofnagle, *supra* note 110.

are frequent users of the information provided by data brokers. Too little is known about this industry. Certainly, there are beneficial examples of private investigators using personal information (i.e., to locate lost children). But private investigators engage in other practices largely unknown to the public. Moreover, there are many instances of private investigators assisting unscrupulous individuals, stalkers, and others bent on violence. For example, the stalker who murdered Rebecca Shaeffer obtained her address from a private investigator.[183] We believe that because private investigators engage in significant use of personal information, they should be subject to the Model Regime just like other principal users of such data. Failure to address private investigators would leave a significant gap in protection.

12. Limiting Government Access to Business and Financial Records

Michael Shankey questions the logic of this section. He notes that requiring the government to obtain court process "is extremely time consuming and costly" and that the government "can utilize the services of a private sector public record database vendors to do the same search of the same government agencies in a fraction of the time for a fraction of the cost."[184] But this is exactly our point—access and aggregation have tipped the scale of power away from the individual to the government. Using public records or information volunteered from private companies, the government can learn much more about its citizens than it could a century or even a decade ago.

13. Government Data Mining

The section on government data mining has received much attention from commentators. Jim Harper argues in support of our proposal that "to the extent [that data mining] means sifting through databases trying to discover incipient wrongdoing . . . [it is] probably ineffective."[185] Others criticize the proposal, arguing that the government should be able to employ the same tools that the private sector uses for marketing. For example, Dennis Bailey argues that the idea that restricting government data mining would "keep government inefficient by depriving it of tools from the private sector" is no longer a widely accepted belief.[186] Some of the criticism, we think, flows from a misunderstanding of our proposal. We have proposed limits on data mining for prospective wrongdoing.

183. 139 CONG. REC. S15762 (daily ed. Nov. 16, 1993) (statement of Sen. Boxer).

184. E-mail from Michael Sankey to Daniel Solove and Chris Hoofnagle, *supra* note 123.

185. E-mail from Jim Harper, Director of Information Policy Studies, The Cato Institute, to Declan McCullagh, Chris Hoofnagle, Director, Electronic Privacy Information Center, and Daniel Solove, Associate Professor, The George Washington University Law School (Mar. 14, 2005, 01:00 PM) (on file with authors).

186. Bailey, *supra* note 115.

Data mining regularly occurs, and with good reason, to address crimes that have already occurred (a form of data matching was used to help identify the Washington D.C. area sniper, for instance). Data mining prospectively to interdict future crimes raises profound due process questions, and it is that practice that we have sought to address in this principle.

In his book, Dennis Bailey elaborates on his support for government data mining and contends that the problems created by data mining can be minimized by avoiding a "centralized data warehouse."[187] Bailey observes that the government could search multiple databases with a subpoena or court order and "[o]nly when a suspicious pattern turned up would an individual be identified, most likely after court approval was obtained."[188] This suggestion resembles one made in the Markle Report, which recommends against centralization such as in the Total Information Awareness program.[189] According to the Markle Report, "[a]ttempting to centralize this information is not the answer because it does not link the information to the dispersed analytical capabilities of the network."[190] In other words, the Markle Report suggests that the government enlist the assistance of various companies and other entities to conduct the data mining. Moreover, the Markle Report recommends that "personally identifiable data can be anonymized so that personal data is not seen unless and until the requisite showing . . . is made."[191] The problem with this suggestion is that merely decentralizing the databases does not provide adequate protection when such information can readily be combined at the push of a button. Such outsourcing of government intelligence functions presents other problems as well, since private sector entities lack the openness and accountability of government as well as the legal limitations on the collection and use of personal data. Anonymizing the identities of data subjects and searching for patterns only to identify those suspicious people still involves a dragnet search. Concealing the names at the stage of the initial pattern analysis will provide little meaningful protection because it does not change the dragnet nature of the search and because the search for patterns is conducted by computers for which the names of the individuals will not be relevant anyway.

187. *See* BAILEY, *supra* note 115, at 110.

188. *Id.*

189. MARKLE FOUNDATION, CREATING A TRUSTED NETWORK FOR HOMELAND SECURITY: SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE 5–7, 11–12 (2003), *available at* www.markletaskforce.org/reports/TFNS_Report2_Master.pdf.

190. *Id.* at 11.

191. *Id.* at 35.

14. Control of Government Maintenance of Personal Information

Jim Harper observes in agreement that the Privacy Act requires significant revision because the Act "is a paper tiger."[192] Harper contends that the Act must be revised "especially in light of the end-run made possible by companies like ChoicePoint who do the dossier-building that the Privacy Act is meant to prevent."[193]

15. Preserving the Innovative Role of the States

Preemption continues to be one of the more controversial proposals in the Model Regime. Eric Goldman writes, "[s]tates have no business trying to regulate privacy. . . . State-based regulation creates a patchwork-quilt of laws that cannot be reconciled, leading to unnecessary costs or a most-restrictive compliance strategy."[194]

Government and businesses have struggled for centuries to draw appropriate lines between state and federal regulation. To simply say that the information privacy cannot be subject to state consumer protection law raises many questions. The state has played a large historical role in protecting consumers. Why should such a role be rejected in the context of information privacy? What is so unique about e-commerce that justifies treating it differently than other interstate commerce, such as catalog sales?

At some level, there is an inconsistency between the data broker industry's declarations of their technological capabilities to engage in personalization and customization with consumer data and their asserted inability to use this same technology to comply with differing state consumer privacy laws. Numerous other industries have faced differing state laws and have found ways to comply. For example, the insurance industry has demonstrated that it can offer state-specific quotes online, despite the fact that the industry is regulated by all fifty states. In light of this, we remain skeptical that compliance with a "patchwork" is impossible.

Moreover, complaints about the difficulties in following the laws of all fifty states are often really disguised attacks on the laws of just a few states, such as California. In many cases, only one or two states have laws addressing a particular issue that diverge from the norm (or even have such laws at all). Ed Mierzwinski of U.S. PIRG comments that a patchwork of state laws is not likely if Congress "does a good enough

192. E-mail from Jim Harper to Declan McCullagh, Chris Hoofnagle, and Daniel Solove, *supra* note 185.

193. *Id.*

194. E-mail from Eric Goldman to Daniel Solove, *supra* note 100.

job."[195] Mierzwinski reasons that if Congress passes effective laws, the states will focus on problems other than privacy.

Historically, federal privacy laws have not preempted stronger state protections or enforcement efforts. The Electronic Communications Privacy Act,[196] the Right to Financial Privacy Act,[197] the Cable Communications Privacy Act,[198] the Video Privacy Protection Act,[199] the Employee Polygraph Protection Act,[200] the Telephone Consumer Protection Act,[201] the Driver's Privacy Protection Act,[202] and the Gramm-Leach-Bliley Act[203] all allow states to craft protections that exceed federal law. Even the FCRA allows for stronger state law in many circumstances.[204]

Although the federal government has enacted privacy laws, most privacy legislation in the United States is enacted at the state level. Many states have privacy legislation on employment privacy (drug testing, background checks, employment records), SSNs, video rental data, consumer reporting, cable television records, arrest and conviction records, student records, tax records, wiretapping, video surveillance, identity theft, library records, financial records, insurance records, privileges (relationships between individuals that entitle communications to privacy), and medical records.[205]

States have engaged in significant innovation in addressing consumer protection and privacy issues. It was the states, not the FTC, that first acted to create telemarketing Do-Not-Call lists. Ed Mierzwinski of the U.S. PIRG comments that "the vast majority of 2003 federal FACTA [Fair and Accurate Credit Transactions Act] reforms were first passed in the states."[206]

Jim Harper suggests that federal law should neither be a ceiling or a floor, allowing states to regulate upward or downward—that is, provide their citizens more or less privacy.[207] Harper reasons that many people choose to have their privacy invaded, and thus states should be able to make the choice to provide their citizens less privacy protection. Such a

195. E-mail from Edmund Mierzwinski, Consumer Program Director, U.S. PIRG, to Declan McCullagh, Chris Hoofnagle, Director, Electronic Privacy Information Center, and Daniel Solove, Associate Professor, The George Washington University Law School (Mar. 20, 2005, 06:05 PM) (on file with authors).

196. 18 U.S.C. § 2510 (2000).

197. 12 U.S.C. § 3401 (2000).

198. 47 U.S.C. § 551(g) (2000).

199. 18 U.S.C. § 2710(f) (2000).

200. 29 U.S.C. § 2009 (2000).

201. 47 U.S.C. § 227(e) (2000).

202. 18 U.S.C. § 2721(e) (2000).

203. 15 U.S.C. §§ 6807, 6824 (2000).

204. *Id.* § 1681t.

205. SMITH, *supra* note 147.

206. Edmund Mierzwinski to Declan McCullagh, Chris Hoofnagle, and Daniel Solove, *supra* note 195.

207. E-mail from Jim Harper to Declan McCullagh, Chris Hoofnagle, and Daniel Solove, *supra* note 185.

system, however, would depart significantly from the general approach of federal regulation, which provides a minimum floor of protections. Under Harper's suggestion, federal law would amount to little more than a recommendation, a guideline that could be followed or rejected by the states. We doubt that such a redefinition of the role of federal law would be amenable to Congress. As for citizens choosing to have less privacy protection, we certainly recognize that people may choose different degrees of privacy. We have crafted our Model Regime to afford people meaningful choices about their privacy; people are free to reject these if they want. The goal of privacy regulation is to ensure that when people do exercise choice with regard to their privacy protection, such choice is a meaningful choice, not a one-sided transaction where people are given few reasonable options and not enough information to make an informed decision.

16. Effective Enforcement of Privacy Rights

Several commentators suggested that civil penalties be severe, so as to prevent privacy violations from occurring as a "cost of doing business."[208] "Rodolphe Ortalo," commenting on Bruce Schneier's blog, suggests that company executives be criminally liable for security.[209] A significant segment of the public agrees that criminal liability is appropriate for those who invade privacy. However, unless there is willful or malicious behavior, we think ordinary civil liability will suffice to deter wrongdoing.

208. *See* Posting of Bruce Schneier to Schneier on Security: U.S. Medical Privacy Law Gutted, http://www.schneier.com/blog/archives/2005/06/us_medical_priv.html (June 7, 2005, 12:15 PM).

209. Posting of Rodolphe Ortalo to Schneier on Security: Ideas for Privacy Reform, http://www.schneier.com/blog/archives/2005/03/ideas_for_priv.html (Mar. 17, 2005, 04:18 AM).