SECURITY THEATER AND DATABASE-DRIVEN INFORMATION MARKETS: A CASE FOR AN OMNIBUS U.S. DATA PRIVACY STATUTE

*Candice L. Kline**

I. INTRODUCTION

THE government's pursuit of "Security Theater" following September 11, 2001 ("9/11") leverages anti-terrorism techniques that appear "high tech" and effective, but in reality are highly flawed. The government's aggressive acquisition of personal data raises concerns about civil liberties, especially the right to data privacy. Its use of database-driven information markets to acquire personal data reflects a desire to find an "easy" answer to national security problems; however, database-driven information markets contain inherent imperfections. They are not sufficiently tuned to protect individual data privacy or to promote an accuracy level expected in government investigations. Recognizing that in many cases the government's public and private database activities are institutionalized and often legitimate, better data privacy regulations modeled after the European Union Data Privacy Directive 95/46/EU ("EU Data Directive") are needed to protect individual privacy interests. Through greater recognition of individual data privacy rights, a U.S. data privacy statute would improve the accuracy and integrity of database-driven information markets and ensure a higher return on the government's investments in these markets.

Part II of this article provides an overview of the relationship between the government, public and private databases, and the emergence of database-driven information markets in the context of post-9/11 Security Theater. Part III analyzes the right to privacy under substantive law. Part IV discusses inadequacies in fourth amendment jurisprudence and statutes addressing data privacy. Part V uses the financial services industry to illustrate the nexus of issues concerning individual data privacy interests, the law, and database-driven information markets. Part VI argues that a statutory framework modeled after the EU Data Privacy Directive would effectively address weaknesses in the current U.S. legal privacy framework, protect individual privacy interests, and improve the integrity of database-driven information markets. Part VII

* J.D., University of Toledo College of Law, May 2008 expected. M.B.A., University of Chicago, Graduate School of Business. B.A., Oberlin College. The author is grateful for the assistance of Associate Professor Llewellyn Gibbons in exploring individual data privacy issues and especially appreciates the support of her husband, Thomas Henry Unger.

concludes that an omnibus statutory approach modeled after the EU Data Privacy Directive would benefit individual, corporate, and government interests by establishing better data management practices for all parties.

II. GOVERNMENT, TECHNOLOGY, AND SECURITY THEATER: BACKGROUND TO THE U.S. DATA PRIVACY PROBLEM

This section draws a landscape of the current data privacy problems facing the U.S. today. The desire to amass personal data in governments and corporations reflects the old adage that "knowledge is power." Throughout history, governments amassed personal data, sometimes leading to tragic ends. The powerful forces of government and corporate interests, however, continue to support a labyrinth of data aggregation and compilation in database-driven information markets. These markets further benefit from advancements in technology, and in particular, database-oriented technology. While personal data are gathered and traded commercially, most individuals are unaware of how their personal data are used and brokered among government and corporate interests. The widespread use of databases, complete with massive amounts of personal data, further encourages government use of these tools in its law enforcement and national security efforts. Such database tools provide a sense of progress and high-tech prowess in post-9/11 security programs, regardless of their effectiveness. Problems such as government scope expansion, persistent false positives in database-driven programs, such as air travel screening, and the introduction of numerous other security risks, including identity theft, challenge the existing laissez-faire approach to personal data privacy. The rapid expansion of database-driven information markets presents serious challenges to personal data privacy interests.

A. Government's Historical Love Affair with Data

Well before 9/11, the federal government gathered, leveraged, and mined public and private data using database technologies.[1] The purpose was twofold: to expand the use of new technologies to gather data and to figure out interesting ways in which to use this newly gathered data, legal or not.[2] Since the Franklin Delano Roosevelt administration, a "push me-pull me" political process has existed between advocates for more government access of data and opponents of

1. Database is defined as "a systematically arranged collection of computer data, structured so that it can be automatically retrieved or manipulated." ENCARTA WORLD ENGLISH DICTIONARY (N. Amer. Ed. 2006). Black's Law Dictionary provides that database is "[a] compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often today by electronic means." BLACKS LAW DICTIONARY 422 (8th ed. 2007).

2. *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1315-20 (2004) (providing a survey of government surveillance activities through the early 1970s, including its use against political opponents, chilling of first amendment rights, harm to individuals, and distorted intelligence reporting to influence public policy and opinion).

such access.[3] Advocates of the government's expanded use of private personal data believe in the effectiveness of data-driven tools in fighting crime and terrorism.[4] Opponents of that use raise concerns about violations of various privacy acts and individual constitutional rights, primarily rights rooted in the Fourth and Fifth Amendments.[5] Often, public opinion weighs against expanded government use of giant databases containing comprehensive personal data on individuals.[6]

Modern history includes cases of abuse and misuse by the government of personal data and databases to profile the personal details of targeted individuals.[7] Benign acquiescence to government compilation of personal data risks civil rights abuses. In the U.S., egregious examples of personal data abuse include The Red Scare, Japanese Internment during World War II, McCarthyism, and the misuse of data to coerce or harass dissidents or political opponents, such as Martin Luther King, Jr.[8] In the mid-1970s, the Church Committee, headed by Senator Frank Church (D-Idaho), uncovered evidence that "the FBI, the CIA, and other government agencies had engaged in pervasive surveillance of politicians,

3. *See generally* DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 83-84 (2006).

4. John Ashcroft, *Preserving Life & Liberty*, *in* AT WAR WITH CIVIL RIGHTS AND CIVIL LIBERTIES 17, 20 (Thomas E. Baker & John F. Stack, Jr. eds. 2006) ("Every cop and prosecutor in the room understands the value business records can play in an investigation.").

5. *E.g.*, Raymond Shih Ray Ku, *The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1336 (2002).

6. Recent examples of government database initiatives that were announced, but subsequently defunded after receiving criticism on privacy or other grounds, including effectiveness, primarily relate to 9/11-styled terrorism prevention. These databases are CAPPS II ("Computer Assisted Passenger Prescreening System"), replaced by "Secure Flight" in 2004, and Total Information Awareness, renamed Terrorist Information Awareness, which was denied funding by Congress in 2003. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 162-63. MATRIX ("Multi-State Anti-Terrorism Information Exchange") is a state-level coordinated law enforcement database initiative, abandoned by most participating states by 2005, except for a few states, including Ohio (now called the OHLEG-SE program) and Florida. MATRIX is an example of a database program criticized for privacy concerns because it mixes public and private data in partnership with a private database provider, Seisint, Inc., which also accrued controversy because of the criminal past of its founder. ROBERT O'HARROW, JR., NO PLACE TO HIDE 98-124 (2006). Seisint is now owned by LexisNexis U.S., a Dayton, Ohio-based subsidiary of UK-based Reed Elsevier Group PLC., which acquired Seisint for $775 million. Press Release, LexisNexis, LexisNexis Completes Acquisition of Seisint, Inc. (Sept. 1, 2004), *available at* http://www.lexisnexis.com/about/releases/0730.asp. Seisint was founded and headquartered in Boca Raton, Florida. Press Release, Reed Elsevier, Reed Elsevier announces the acquisition of Seisint, Inc. for $775 million (July 14, 2004), *available at* http://www.reed-elsevier.com/index.cfm?Articleid=965. For more information about OHLEG-SE, see generally *Search Engine for Law Enforcement in Ohio*, GOV'T TECH., Jan. 11, 2006, http://www.govtech.net/news/news.php?id=97825.

7. Examples include FBI and CIA domestic intelligence operations from 1940 to 1973, as well as U.S. army and police department surveillance of political dissidents. DANIEL J. SOLOVE, THE DIGITAL PERSON 177-84, 192-94 (2004). Examples during the Founder's time include writs of assistance and general warrants. O'HARROW, *supra* note 6, at 18, 20; Ku, *supra* note 5, at 1337.

8. *See* SOLOVE, *supra* note 7, at 182-85 (noting that FBI data collection and files were used in each of these cases). *See also* Daniel J. Steinbock, *Designating the Dangerous: From Blacklists to Watch Lists*, 30 SEATTLE U. L. REV. 65, 69-77 (2006) (summarizing various blacklist and loyalty programs used during the Cold War and McCarthy-era).

religious organizations, women's rights advocates, anti-war groups, and civil liberties activists."[9] The Church Report concluded that "'[t]oo many people have been spied upon by too many government agencies and too much information has been collected' through secret informants, wiretaps, bugs, surreptitious mail opening, and break-ins."[10] Even if these examples fail to "chill the spine," Nazi-controlled Europe and Rwanda offer extreme instances of government leverage of personal data and national identification systems to perpetrate genocidal crimes against targeted and disfavored populations.[11] Therefore, if history is our teacher, assuming a benevolent purpose behind government data collection efforts threatens civil liberties and is outright dangerous for certain individuals.[12]

Databases present a seductive allure to the government because knowledge is power.[13] Knowledge can be used to coerce individual behavior.[14] For example, the government uses personal data to coerce behavior when government benefits are at stake, such as screening the behaviors of welfare recipients for welfare benefits.[15] In other cases, the government's enhanced knowledge of the individual, regardless of accuracy, may be used to limit the individual's freedom of speech, association, or travel.[16] Whether by the Executive Branch or its bureaucratic agencies, enhanced power through knowledge is irresistible because of the possibility of unprecedented control over the individual.[17]

9. O'HARROW, *supra* note 6, at 18.

10. *Id*. O'Harrow discusses two additional government initiatives of the time period that illustrate abuse of government collection of lawful, personal data for suspect purposes, namely, COINTELPRO, an FBI counterintelligence program and the Army's CONUS intelligence operations.

11. SOLOVE, *supra* note 7, at 148 (noting that "[s]laves were required to carry identification papers to travel; identification cards were used by the Nazis in locating Jews; and the slaughter of Tutsis in Rwanda was aided by a system of identifiers").

12. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) ("And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."). *See also* O'HARROW, *supra* note 6, at 244.

13. COLIN J. BENNETT, REGULATING PRIVACY 29-31 (1992).

14. *Id*.

15. *See* SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 159 (describing Project Match, a 1977 federal Government program that compared computer employee records to benefit recipients in order to detect fraud).

16. *See* BRUCE SCHNEIER, BEYOND FEAR 42, 77, 228-31 (2003) (discussing knowledge, trade-offs, and experience in security decisions with analogies to corporate examples).

17. *See* SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 85 (reporting on President Nixon's use of wiretaps as against internal dissidents and radicals under the national security exception of the Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-22 (2000), until his interpretation was rejected by the Court in United States v. U.S. Dist. Court, 407 U.S. 297, 320-22 (1972) (requiring national security exception limited to foreign threats)).

B. Rise of Database-Driven Information Markets

The modern era of database-driven information markets started in the 1970s. Arthur R. Miller suggested in his 1971 book, *The Assault on Privacy*, that "[t]he new information technologies seem to have given birth to a new social virus—'data-mania'" and that "[w]e must begin to realize what it means to live in a society that treats information as an economically desirable commodity and a source of power."[18] Advancing computer technologies fuel the modern era. Innovations such as Moore's Law, which "states that the number of transistors on a chip doubles about every two years," explain this rapid expansion of technological capability.[19] Computer technology continues to grow in processing speeds and capabilities, to lower storage costs while increasing capacity, and to achieve higher levels of software sophistication.[20] Technology's rapid rise enabled the information markets.[21] Through technology, credit card companies and retailers (even grocery stores) pursue personal data on most Americans for profiling spending characteristics.[22] A vast new data brokerage industry emerged with the advancing ability of these companies to develop sophisticated databases to capture, organize, sift, and analyze growing amounts of individual personal data.[23]

A byproduct of enhanced technological capabilities is the ease with which data can be populated, aggregated, and exchanged across an increasingly diverse set of corporate interests.[24] These corporate interests span the economy and include retailers (Sears, Hallmark), pharmaceutical companies (Pfizer), technology firms (Microsoft, IBM), banks and financial services firms (Bank One, Bank of America), and automakers (GM, Toyota).[25] Data brokerage companies, such as Acxiom and LexisNexis repackage, augment, and sell personal data on individuals to corporate and public sector clients.[26] Credit reporting agencies, TransUnion, Equifax, and Experian sold collectively 1.2 billion credit reports in 2002.[27] Experian's database of credit information includes records on "about 215 million people and demographic information on

18. O'HARROW, *supra* note 6, at 41.

19. *Id*. at 290.

20. *Id.*

21. *Cf. id*. at 42, 43 (observing that one data broker, Acxiom, had "almost 1 million times the capacity for information in 2004 than it had in 1983.").

22. SCHNEIER, *supra* note 16, at 98-99.

23. O'HARROW, *supra* note 6, at 42.

24. *Id*. at 42-45. *See also id.* at 45 (quoting Richard Barton of the Direct Marketing Association: "[w]e have the capability to gather, store, analyze, segment and use for commercial (and many other) purposes more data about more people than was ever dreamed of," adding "technology is providing us with even more ingenious ways to reach into the lives of every American").

25. *Id*. at 43.

26. *Id*. at 44.

27. *Id*. at 76.

approximately 215 million consumers in 110 million U.S. households."[28] These firms have been able to partner, sharing data and technologies, to achieve greater scale and breadth without most individuals knowing of their activity or their existence.[29] The multi-billion dollar data brokerage industry manages individual data for use in commercial and marketing applications as well as government investigative activities.[30]

With widespread use of the Internet and technology-enabled processes, availability of many kinds of personal data has expanded exponentially since the mid-1990s.[31] Electronically available personal data culled from public and private records forms the backbone of the multi-billion dollar database-marketing industry.[32] Data brokers and their customers collect and trade massive amounts of digitized personal data on most Americans through database-driven information markets.[33] For example, ChoicePoint, self-described as the nation's leading provider of identification and credential verification services, maintains "14 billion records on individuals and businesses that can be used for tasks like pre-employment screening of job candidates."[34] Even small data brokers can effectively compete in this market because of the Internet and low technology costs.[35] The industry further benefits from the emergence of a government database build-up after 9/11 to serve national security.[36] Whether for profit or national security, government agencies act as both buyers and sellers of personal data and in essence subsidize the development of database-driven information markets.

These markets work well, except for the individual data subjects that form the basis of their operation. Personal data can be readily sourced, aggregated, and accessed by third parties, including government agencies, due to

28. Lee Tien, *Privacy, Technology & Data Mining*, 30 OHIO N.U. L. REV. 389, 390 (2004) (quoting Experian Factsheet, http://www.experian.com/corporate/factsheet.html (last visited Jan. 2, 2008)).

29. O'HARROW, *supra* note 6, at 44-52. O'Harrow describes the business development partnerships between Acxiom, a data broker with information on approximately 200 million adults, Abacus Direct Corp., a retailer consortium with records on 88 million households, HNC Software, a data mining intelligence firm, and TransUnion, a credit reporting bureau with credit histories on 500 million individuals globally. For more information about TransUnion, see About TransUnion, http://www.transunion.com/corporate/aboutUs/aboutUs.page (last visited Jan. 2, 2008).

30. *See* SOLOVE, *supra* note 7, at 166 (2004); Stan Karns, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 399-400 (2002). *See also* Big Brother, Big Business, http://www.cnbcbig brother.com/index.html (last visited Jan. 15, 2008).

31. SOLOVE, *supra* note 7, at 23-25, 167-68.

32. *Id*. at 19-21, 127-31.

33. Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2057 (2004). *See also* Daniel J. Solove, *Privacy & Power: Computer Databases & Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1407-08 (2001).

34. Tien, *supra* note 28, at 390 (quoting ChoicePoint, http://www.choicepoint.com/index.html (last visited Jan. 2, 2008)).

35. SCHNEIER, *supra* note 16, at 99 ("The costs to collect and store the data are so low that many companies just say, 'Why not?'").

36. O'HARROW, *supra* note 6, at 195 (highlighting the $200 million budget for the Total Information Awareness project).

improvement in technology and decreasing costs of processing and storage. Data are exchanged without ever providing notice or transparency into the processing of that data to individuals whose personal data are involved.[37] Aggregators and owners of these databases enjoy limited accountability to individual data subjects because procedural protections such as notice are absent.[38] Very few Americans are fully aware that they unleash their personal information into the stream of commerce everyday through disclosures made in discrete, even routine transactions, such as purchases, subscriptions, and warranty applications.[39] Even fewer Americans know that this data, once stored, exists forever.[40]

C. Government Database Use: Security Theater

Government's increased interest in amassing personal data since 9/11 "changed everything."[41] A specific danger lurks in government use of "Security Theater" to justify an appetite for more personal data and larger and more capable databases.[42] After 9/11, government faced pressure to improve security systems that "prevent[ed] adverse consequences from the intentional and unwarranted action of others."[43] One approach used is security systems that make people feel safer, but do not actually make them safer.[44] These systems are a form of Security Theater. Security Theater soothes public concerns at a time of fear and unease,[45] but also dulls the senses. The dark secret inherent in such systems—that they do not work—is protected by political discourse that discourages criticism and inquiry, and portrays a figurative "look behind the curtain" as unpatriotic.[46] Under a climate of national emergency, individuals and government officials are more likely to be deferential to government acquisition and use of personal data, especially for law enforcement purposes.[47] The national security curtain hides from public view government's actual activities, which may go beyond preventing acts of terrorism.[48]

37. SOLOVE, *supra* note 7, at 51.

38. *Id*. at 9, 38-39. *See also* O'HARROW *supra* note 6, at 139 (observing that there is no individual control over ChoicePoint data).

39. SOLOVE, *supra* note 7, at 51-53, 165-66. *See also* O'HARROW, *supra* note 6, at 300 (observing that data on daily life events are recorded and sold).

40. O'HARROW, *supra* note 6, at 138.

41. President Bush and Prime Minister Allawi Press Conference, http://www.whitehouse.gov/news/releases/2004/09/20040923-8.html (last visited Jan. 2, 2008).

42. SCHNEIER, *supra* note 16, at 38 (describing examples of Security Theater, which is defined as security countermeasures that "provide the feeling of security *instead of* the reality") (emphasis in original).

43. *Id*. at 11.

44. *Id*. at 38.

45. *Id*.

46. For a discussion of post-9/11 political culture, see generally Ronald Dworkin, *The Threat to Patriotism*, THE N.Y. REV. OF BOOKS, Feb. 28, 2002, http://www.nybooks.com/articles/15145.

47. *See, e.g.,* DAVID COLE & JAMES DEMPSEY, TERRORISM AND THE CONSTITUTION 195-97 (2006) (discussing the USA Patriot Act).

48. *Id*. at 206.

Publicized database initiatives are acts of Security Theater.[49] An inherently intuitive allure attaches to scanning massive amounts of data in dimly lit control rooms, using sophisticated algorithms and scientific computer-matching methods to predict future behaviors and identify suspect individuals.[50] This approach looks smart and makes some people feel safer.[51] Security Theater convinces some individuals that a tradeoff between security and civil liberties is required, with the tradeoff seemingly worthwhile because sophisticated databases and data mining technologies appear so clever and effective.[52] Accumulation of more data to the layman suggests not only better information, but potential for better intelligence.[53] Yet, data mining is inherently flawed in its ability to find "extremely rare instances of patterns across an extremely wide variety of activities and hidden relationships among individuals,"[54] and encourages "fishing expeditions."[55] Government data mining of personal data on mostly innocent individuals amounts to "a wholesale invasion of Americans' privacy that yields, basically, nothing in terms of finding terrorists."[56] Although Security Theater can make people feel safer, its costs may outweigh its benefits.

Although the economics might be questionable, government investment in database-driven security solutions grew since 9/11 due to the perceived panacea that this approach offers to counter-terrorism efforts and the appeal of increasing technological capabilities.[57] According to Daniel Solove, the federal bureaucracies "maintain almost 2,000 databases."[58] Government agencies increasingly use databases, whether aggregated internally or through third-party providers, as part of its "war on terror"[59] strategy to "smoke-out"[60] potential terrorists. For example, after 9/11, a new cabinet-level post was created, the Director of National Intelligence, to pull together intelligence data resources both within and external to the government.[61] Development of this massive new

49. SCHNEIER, *supra* note 16, at 38.

50. *Id*. at 137.

51. *See id.* at 38.

52. *Id*. at 42.

53. *See id*. at 162 (arguing that data analysis is more important than data collection).

54. Statement of Dr. Tony Tether, Dir. of the Def. Advanced Research Projects Agency, to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census Committee on Government Reform, United States House of Representatives (May 6, 2003), *available at* http://www.fas.org/irp/congress/2003_hr/050603tether.html [hereinafter Tether Testimony] (discussing data mining and privacy issues in the U.S.).

55. Tien, *supra* note 28, at 405.

56. Tether Testimony, *supra* note 54.

57. O'HARROW, *supra* note 6, at 208-13.

58. SOLOVE, *supra* note 7, at 15.

59. President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html (using the term "war on terror").

60. *Bush: 'We're Smoking Them Out*,' CNN.COM, Nov. 26, 2001, http://archives.cnn.com/2001/US/11/26/gen.war.against.terror/.

61. RICHARD A. BEST, JR., THE DIRECTOR OF NATIONAL INTELLIGENCE AND INTELLIGENCE ANALYSIS 2 (2005). *See also* Office of the Director of National Intelligence, About Us, http://www.dni.gov/aboutODNI/who.htm (last visited Jan. 2, 2008); National Counterterrorism

bureaucracy, operating under the justification of national security, set a more aggressive standard for data collection for other federal and state agencies. Government investment in massive database and data mining projects since 9/11 include Total Information Awareness, rebranded "Terrorist Information Awareness," an "experimental data mining program" intended to accumulate significant amounts of personal data on U.S. citizens under the auspices of screening for terrorism risk factors, and is still being pursued by government agencies.[62] The Federal Bureau of Investigation ("FBI") launched a program to recover data from Internet Service Providers for surveillance purposes, originally called Carnivore, but re-named DCS1000.[63] An example of a state-level database initiative is the Multi-State Anti-Terrorism Information Exchange ("MATRIX"), a law enforcement database that combines data from private and public sources to create a searchable database to assist in police investigations.[64] This high-tech sheen given to law enforcement or national security investigations requires private databases. Private data brokers provide an avenue for the government to access aggregated personal data for law enforcement and security databases.[65] Because these databases constitute valuable intellectual property in the private sector, and public deployment is shielded by national security secrecy, there is little public control over the use of these databases or the quantity or quality of data contained therein.[66] The dual forces of private market activity and Security Theater limit public awareness of the government's database activity. Privacy activist publicity and opposition to government use of private sector data seems to encourage some limits on government acquisition and use of database information.[67]

Center, About the National Counterterrorism Center, http://www.nctc.gov/about_us/about_nctc.html (last visited Jan. 2, 2008).

62. *See* SCHNEIER, *supra* note 16, at 253-54; SOLOVE, *supra* note 7, at 168-69. Shane Harris, *TIA Lives On*, NAT'L J. (Feb. 23, 2006), *available at* http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm. *See also* Posting of Bruce Schneier to Schneier on Security, http://www.schneier.com/blog/archives/2006/10/total_informati.html (Oct. 31, 2006, 06:59 PST).

63. SOLOVE, *supra* note 7, at 172.

64. *Id.* at 170. *See also* O'HARROW, *supra* note 6, at 104.

65. O'HARROW, *supra* note 6, at 300. *See also* Michael Chertoff, Sec'y of Homeland Sec., Remarks at the International Association of Chiefs of Police Annual Conference (Oct. 16, 2006) (transcript available at http://www.dhs.gov/xnews/speeches/sp_1161184338115.shtm) ("The best tool in dealing with homegrown terrorists is intelligence—collection, analysis and sharing").

66. O'HARROW, *supra* note 6, at 300.

67. *See, e.g.*, Electronic Privacy Information Center, http://www.epic.org/ (last visited Jan. 2, 2008).

D. Government "Scope Creep" and Individual Costs

"Scope creep"[68] characterizes government use and mission for its database initiatives as the power inherent in these databases becomes apparent to government and law enforcement officials.[69] Unfettered government database use places heightened importance on ensuring accurate data, particularized search methods, and limited-purpose databases.[70] Colin Bennett expresses a concern that information technology enhances government power "to collect and manipulate vast quantities of information about individual citizens."[71] Bennett highlights that increased government information gathering triggers a slippery slope toward tyranny by an "increasingly harsh and authoritarian public administration."[72] The ultimate danger of government use of database-driven information markets is that "[t]he computer has given bureaucracy the gift of omniscience, if not omnipotence, by putting into its hands the power to *know*. No fact unrecorded, nothing forgotten nor lost, nothing forgiven."[73] Bennett suggests that one way to control government appetite for data and knowledge is by enforcing an affirmative individual right to data privacy.[74]

Data mining and fishing expeditions by government database users reflect the typical use and utility of databases.[75] When the government uses these methods, the risk of a false positive[76] is borne by individuals.[77] Costs to individuals due to erroneous data use by government may cause significant harm, including lost civil liberties.[78] Government, however, is unlikely to be deterred by the few individuals that bear the cost of its searches, especially if they are

68. *See* University Information Services: Georgetown University, Data Warehouse: Glossary, http://uis.georgetown.edu/departments/eets/dw/GLOSSARY0816.html#S (last visited Jan. 2, 2007) (defining "scoop creep" as "[t]he common phenomenon where additional requirements are added after a project has started without reconsidering the resourcing or timescale of the project. Scope creep arises from the misapprehension that such small additions will not affect the project schedule").

69. *See* O'HARROW, *supra* note 6, at 244 (reporting on proposed use of passenger screening system to also search for people suspected of violent crimes).

70. *See* SOLOVE, *supra* note 7, at 181.

71. BENNETT, *supra* note 13, at 29.

72. *Id.* (quoting DUNCAN CAMPBELL & STEVE CONNOR, ON THE RECORD: SURVEILLANCE, COMPUTERS, AND PRIVACY 15 (1986)).

73. *Id.* at 29 (quoting M.G. Stone & Malcolm Warner, *Politics, Privacy, & Computers*, 40 POL. Q. 256, 260 (1969)).

74. *Id.* at 30. Bennett further argues that the right to information privacy is related to "inalienable human rights, limited government, the rule of law, and a separation between the realms of state and civil society." *Id.* at 31.

75. Tien, *supra* note 28, at 405.

76. A "false positive" is "[t]he erroneous identification of a threat or dangerous condition that turns out to be harmless. False positives often occur in intrusion detection systems." Answers.com, http://www.answers.com/topic/false-positive-technology (last visited Jan. 2, 2008).

77. SCHNEIER, *supra* note 16, at 54-55 (explaining that false positives are common and important to security decisions in applications ranging from passenger screening to ATMs because false positives can vastly outnumber the criminal events that actually occur).

78. *Id.* at 42.

members of certain ethnic communities or political dissenters.[79] Unfortunately, individuals bear the direct costs of these searches with no ability to redress the situation.[80] Enhanced individual data privacy rights that limit data mining and give redress for false positives may counterbalance largely unaccountable government database activities.

E. Airline Passenger Screening: Databases Amok

The current air passenger screening regime illustrates problems with government run databases. Here, a no-fly list is used for pre-emptive individual screening of terror suspects.[81] The no-fly list has been plagued by high profile false positives since it was expanded from sixteen names in 2001 to more than 44,000 names in 2006.[82] According to an October 2006 interview, 75,000 names are designated as passengers for further screening, bringing the total number of no-fly or suspect passengers to 540 pages and 119,000 names.[83] The no-fly list once included fourteen of the nineteen hijackers, although they were dead for more than five years.[84] Examples of high profile false positives include Senator Edward Kennedy (D-Mass.), Representative Donald E. Young (R-Alaska), and

79. For a recent example concerning Muslim Imams removed from their flight due to passenger, airline, and law enforcement unease, see *Andersen Cooper 360* (CNN News television broadcast Nov. 21, 2006).

80. For a humorous discussion on the state of TSA managed airport security, see Anna Quindlen, *Taking Off Your Shoes: Osama bin Laden Could Get through the Line If the Name on His License Was the Same as that on His Ticket and He Wasn't Packing Oil of Olay*, NEWSWEEK, Nov. 13, 2006, at 80.

81. The current airline passenger system is called the Computer-Assisted Passenger Profiling System (CAPPS). It has been in place since 1999 and relies on cooperation between the federal government and the airlines for passenger screening against government-compiled watch lists. SCHNEIER, *supra* note 16, at 164. A proposed successor to CAPPS, called CAPPS-II would have rated passenger's terrorist risk based on forty variables, including use of commercially available databases; however, it was not funded by Congress. *Id*. The Transportation Security Administration is developing a CAPPS replacement called Secure Flight, but its features and security problems have led to a delayed launch of the program. *See* Richard L. Skinner, Office of Inspector General, Department of Homeland Security*, Information Technology Management Needs to Be Stregthened at the Transportation Security Administration*, Oct. 26, 2007, at 14, *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_08-07_Oct07.pdf. *See also* EPIC Secure Flight Page, http://www.epic.org/privacy/airtravel/secureflight.html (last visited Jan. 2, 2008).

82. *Unlikely Terrorists on No Fly List: Steve Kroft Reports List Includes President of Bolivia, Dead 9/11 Hijackers*, 60 MINUTES, June 7, 2007, http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml?source=search_story [hereinafter *Unlikely Terrorists*] (characterizing the list as "awful" and "bad"). O'Harrow reports that according to a TSA memo, the watchlist has expanded almost daily by the intelligence agencies. O'HARROW, *supra* note 6, at 228. *See also* Steinbock, *supra* note 8, at 85-87 (describing the false positive problem in airline passenger screening programs).

83. *Unlikely Terrorists*, *supra* note 82. EPIC reports that the combined watch lists now include 325,000 names, "more than quadruple the 75,000 names on the lists when they were created in 2003." EPIC Secure Flight Page, http://epic.org/privacy/airtravel/secureflight.html (last visited Jan. 2, 2008).

84. *Id*.

Representative Loretta Sanchez (D-Calif.).[85] The list includes extremely common names that present a high risk of false positives, such as Daniel Brown, David Nelson, and Jim Thompson.[86] There is perhaps evidence of racial profiling in the case of Aquil Abdullah, the first African-American Olympic rower and a graduate of George Washington University.[87] In another example of the absurd, Johnnie Lockett Thomas, a seventy-one-year-old African-American widow, was matched with a no-fly list entry for John Thomas Christopher, "the alias of a white man wanted for murder who was already under custody."[88] The continued expansion of the no-fly list only makes wasteful false positives more likely.

Despite the false positives, there is minimal political incentive to the Transportation Security Administration ("TSA") bureaucracy to streamline or refine the no-fly list.[89] The TSA does not provide transparency into the administration of the no-fly list, citing national security concerns.[90] The TSA fails to proactively facilitate resolution of false positives when they occur.[91] The bias for more data and over-inclusiveness dominates the mindset of the TSA, regardless of the costs to wrongly flagged individuals or the effectiveness of the screening process. This bias reflects the TSA's awareness that it bears the risk of any false negative.[92] Only one false negative would severely damage its reputation.

The TSA's approach to passenger screening exhibits many of the problems of database-driven security measures. As Bruce Schneier points out, "[d]ata collection is easy; analysis is difficult."[93] By insulating its passenger screening system with national security-based secrecy, the TSA is not held accountable for

85. *See* SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 161; Gillian Flaccus, *No-Fly List Mix-Up Disrupts California Congresswoman's Travel*, S.F. GATE, Oct. 30, 2006, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2006/10/30/state/n174752S39.DTL. More recently, a British citizen and Muslim leader, 80-year old Kamal Helbawy, was removed from a flight headed to New York on Oct. 18, 2006 for a conference sponsored by New York University Law School. Michael Isikoff & Mark Hosenball, *Denied Entry[Kamal Helbawy, Tariq Ramadan]: U.S. Security Officials Have Prevented an Influential Islamic Scholar from Attending a Conference in New York*, CAMPUS-WATCH.COM, Oct. 18, 2006, http://www.campus-watch.org/article/id/2823 (last visited Jan. 2, 2008).

86. *See 'No-Fly' List Delays Marine's Iraq Homecoming*, MSNBC.COM, Apr. 12, 2006, http://www.msnbc.msn.com/id/12284855/ (describing delays encountered by reservist returning from Iraq because of no-fly list confusion); O'HARROW, *supra* note 6, at 228-29.

87. *Id*. at 229.

88. *Id.* at 230-31.

89. *See id*. at 91-92 (noting that aggregation of federally maintained watchlists, overseen by the TSA, was recommended in the 9/11 Commission Report, a bi-partisan effort).

90. *Id*. at 228.

91. For a discussion of the Johnnie Lockett Thomas experience, see *id*. at 231 ("Thomas has tried repeatedly to extricate herself from the situation, but her letters to the TSA and other agencies did not stop her detentions.").

92. A "false negative" is "[t]he erroneous identification of a benign condition that turns out to be harmful." Answers.com, http://www.answers.com/topic/false-negative-technology (last visited Jan. 2, 2008).

93. SCHNEIER, *supra* note 16, at 162. Schneier also notes that more data may be worse for security purposes because of the "needle and haystack" problem. *Id.*

accuracy or effectiveness.[94] Because the TSA places a premium on aggregation rather than analysis, costly and persistent false positives grow and further diminish the likelihood of preventing a future terrorist attack.[95] Flying is now a modern necessity. As long as airline passengers continue to fly and acquiesce to additional screenings,[96] there will be little pressure on the TSA to amend its procedures.

F. Other Database Security Risks and Identity Theft Crime

Amassing large databases creates inherent security risks other than false positives.[97] Large databases are attractive nuisances that draw hackers to them because a successful breach is both efficient and lucrative.[98] Attackers are primarily of two forms: those who want to penetrate and control the raw personal data and those who study the system to predict its future behavior.[99] Attackers come from within and outside the walls of an organization.[100] Development and maintenance of large databases requires many trusted people.[101] The bigger the system, the more vulnerable it is to attack because of the need for more trusted people.[102] This means layers of trustworthy staff that will not steal, resell, misuse, or otherwise violate security measures.[103] Frequently, security measures are targeted to prevent external hackers; however, these measures often overlook internal security breaches by employees or sub-contractors who have passwords or access to the premises.[104] Thus, as databases grow, security procedures and technologies must likewise expand to deter theft or unlawful exploitation of these increasingly valuable, and vulnerable, assets.

Another security problem in large database applications is the complexity of system design.[105] According to one security expert, "[c]omplexity is the worst enemy of security."[106] He argues that such systems are hard to secure because

94. *Cf.* Gilmore v. Gonzales, 435 F.3d 1125, 1129 (9th Cir. 2005). Plaintiff unsuccessfully challenged the TSA's identification policy requiring air passengers to produce identification or be subject to an additional search prior to their flight. *Id.* at 1137-39.

95. SCHNEIER, *supra* note 16, at 54-55.

96. Richard Schlesinger, *Racial Profiling in the Air* (CBS Evening News broadcast Apr. 23, 2003) ("I oscillate between thinking this is a good thing we have going on for security purposes and feeling that this is a horrible thing that we have.").

97. SCHNEIER, *supra* note 16, at 78, 99.

98. *Id*.

99. *Id*. at 164, 253 (illustrated by CAPPS and TIA examples).

100. *Id*. at 137.

101. *Id*.

102. *Id*. at 138.

103. *Id.* at 137, 205, 253 (describing the layers of staff and noting that "there isn't a government database that hasn't been misused by the very people entrusted with keeping that information safe – that is, the government itself").

104. *Id*. at 137. For examples of insider security breaches and identity theft, see Privacy Rights Clearinghouse, A Chronology of Date Breaches, http://www.privacyrights.org/ar/ChronData Breaches.htm (last visited Jan. 2, 2008).

105. SCHNEIER, *supra* note 16, at 90.

106. *Id.*

they are messier, more unpredictable, and prone to catastrophic failures.[107] Furthermore, all systems are vulnerable to hackers that study systems without perpetrating data theft or hacking. Fewer measures deter attackers that study the "output" of the system because they do not involve new technology investments. These attackers test system response and infer the data variables used and the algorithm deployed without using technology, but rather old-fashioned keen observation.[108] Complex technology-obsessed solutions remain vulnerable to low-tech cleverness.

Security breaches of all forms are on the rise due to public availability of so much personal data. There are many recent examples of security breaches due to hacking, theft, and disclosures from pretexting or improper use.[109] Acxiom reported two hacking incidents involving information on millions of people.[110] In 2005, ChoicePoint, a data broker with more than nineteen billion records on virtually every American,[111] sold personal data, including names, addresses, and social security numbers in 145,000 records, later revised to 163,000 records, to identity thieves operating a fake business.[112] The ChoicePoint breach resulted in potentially 1,400 cases of identity theft.[113] LexisNexis reported security breaches impacting 32,000 individuals in 2005.[114] Lax data security is not just a problem of data brokers. Government agencies have reported significant security breaches, including 26.5 million records lost by the Veterans Administration through an employee's stolen laptop in June 2006.[115] Universities also present a

107. *Id.* at 90-91.

108. *See id.* at 164 (describing the CAPPS example).

109. For a discussion of a recent pretexting scandal, see Tom Krazit, *FAQ: The HP 'Pretexting' Scandal,* CNET NEWS.COM, Sept. 6, 2006, http://www.news.com/FAQ-The-HP-pretexting-scandal/2100-1014_3-6113011.html.

110. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 255.

111. *Safeguarding the Data Brokerage Industry,* Part II (NPR News & Notes broadcast Mar. 14, 2005) [hereinafter S*afeguarding* Part II].

112. *Safeguarding the Data Brokerage Industry,* Part I (NPR News & Notes broadcast Mar. 14, 2005) [hereinafter Safeguarding Part I] (reporting 145,000 U.S. residents affected). Privacy Rights Clearinghouse, A Chronology Data Breaches—2005, *supra* note 104 (reporting later revision to 163,000 records).

113. Press Release, Federal Trade Commission, FTC Launches Redress Program for ChoicePoint Identity Theft Victims (Dec. 6, 2006), *available at* http://www.ftc.gov/opa/2006/12/choicepoint.shtm. Only 30,000 of these people initially were notified because they were protected under California state law, but still more than five months after ChoicePoint first became aware of the theft. Gary North, *They've Got Your Number (and More),* LEWROCKWELL.COM, Feb. 19, 2005, http://www.lewrockwell.com/north/north345.html.

114. *Safeguarding* Part I, *supra* note 112. The Privacy Rights Clearinghouse suggests an additional 280,000 were affected by the LexisNexis breach. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches—2005, *supra* note 104.

115. United States Department of Veterans Affairs: Public and Intergovernmental Affairs, Secretary Nicholson Provides Update on Stolen Data Incident: Data Matching with Department of Defense Providing New Details, June 6, 2006, http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1134. The VA Administration announced another stolen laptop, this time involving one of its subcontractors, Unisys Corporation, which contained insurance claim data, including names, addresses, and personal identifiers that was subsequently recovered on September 14, 2006. Press Release, Department of Veterans Affairs, Department of Veterans Affairs Office of

special opportunity for identity theft because many use social security numbers as student identification numbers, store large amounts of information, and typically under-resource IT departments. At Ohio University, hackers accessed the social security numbers of 137,000 individuals for more than a year.[116] The Privacy Rights Clearinghouse concludes that from the ChoicePoint 2005 data breach through January 17, 2008, data security breaches resulted in the disclosure of more than 217 million records containing personal data.[117]

Whether by theft or commercial acquisition, widespread ease in acquiring personal data may lead to tragic results.[118] In *Remsburg v. Docusearch, Inc*., data acquired by credit card through an information broker was used to execute a murder-suicide at the victim's place of employment.[119] In multiple Internet-based transactions, the broker sold data on the victim to the stalker, including the victim's social security number, acquired through a credit report header, and place of employment, confirmed using a pretextual call, and the key to completing the crime.[120] The case discussion suggests that the victim was unaware that her personal data were being acquired by her stalker.[121] Personal data acquisition, of whatever kind, lawful or unlawful, can cause significant harm beyond the widely reported financial risks of identity theft. Since the 1999 events described in *Remsburg*, personal data on the Internet, and the attendant risks of identity theft and misuse of such personal data, continues to expand as technology advances.[122]

As identity theft risk increases, the public will likely express more concern about data privacy. Identity theft is fundamentally a by-product of inadequate privacy protection in the U.S. Because legal protections ineffectively shield individuals from personal data predators, identity theft proliferates and arbitrages the great structural weaknesses in database infrastructures across public and private institutions. When identity theft implicates how individuals live, work, and travel because of its ricocheting affect across public and private databases,

Inspector General and the Federal Bureau of Investigation Announce the Recovery of Stolen Unisys Computer and Arrest of Khalil Abdullah-Raheem (Sept. 14, 2006), *available at* http://www.va.gov/oig/51/press2006/VAOIG-pr-Abdullah-Raheem.pdf.

116. Greg Sandoval, *University Server in Hackers' Hands for a Year,* CNET NEWS.COM, May 22, 2006, http://news.zdnet.com/2100-1009_22-6074739.html?tag=ni.

117. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches—2005 & 2006, *supra* note 104 (providing a detailed table of reported data breaches since January 2005). *See also* Ann Cavoukian, Information & Privacy Commissioner/Ontario, Address at the 16th Annual Fraud Investigators Conference, Identity Theft—Fraud at Its Worst: The Implications of Information Insecurity 15 (Dec. 15, 2006), *available at* http://www.ipc.on.ca/index.asp?navid=46&fid1=584 (describing identity theft and including a list of sample data breaches compiled by the Privacy Rights Clearinghouse).

118. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

119. *Id*. at 1006.

120. *Id*. at 1005-06.

121. *Id*. at 1006 (Place of employment was obtained through a pretextual call, thus disguising the purpose for the information to the victim.).

122. The author suggests that readers test this observation through Google and White Pages searches of their names to observe the amount of information readily available and the number of data broker advertisements prompted by such a search.

the issue of legal protections for personal data privacy becomes ever more urgent.

In 2002 and 2003, an estimated ten million Americans were affected by identity theft, resulting in estimated costs of $53 billion.[123] In 2004, identify theft cost U.S. citizens and businesses more than $52 billion.[124] Identity theft is the top complaint at the Federal Trade Commission, totaling thirty-nine percent of all complaints in 2004[125] and thirty-six percent in 2006.[126] The problem of identify theft illustrates many of the issues concerning database-driven information markets. Identity thieves skillfully leverage four structural limitations in database-driven information markets: (1) lack of individual control of personal data; (2) third-party dominance; (3) an inability to seek adequate legal remedies; and (4) a complete lack of transparency on data use. Individuals have few means to effectively protect themselves from identity theft crimes. When an identity theft event results in database entries, such as misleading credit report transactions or criminal histories, the negative impact on an individual's financial liberty and employment can be extreme. These new privacy-based harms require legal remedies to address data security risks and to encourage responsible database management practices.

III. THE RIGHT TO PRIVACY IN SUBSTANTIVE LAW

This section explores the right to privacy concept, its genesis, and its evolution in the substantive law areas of torts, contract, and property as defined by theorists and the courts. Courts are generally deferential to the creation and use of databases. Regardless of purpose or intent, once data has been released to third parties, courts rarely intervene to protect individuals. Substantive law approaches to the right to privacy provide limited personal data protections. Legal frameworks poorly address the complex nature of modern data privacy issues. The traditional legal focus on one-to-one adversarial relationships strains to fit the third-party problem in database-driven information markets. Third-party disclosures are not held to account under constitutional law because of weak interpretations of the Fourth and Fifth Amendments, both of which deal with aspects of an individual's right to privacy.

For example, the Supreme Court's twofold requirement of "subjective and objective expectations of privacy" in fourth amendment jurisprudence enforces a narrow view of the right to privacy. Once an individual releases his information into the stream of commerce, there can be no finding of either subjective or objective privacy. Even if a plaintiff were able to assemble a privacy-based tort case, the strong protections of the First Amendment often weigh in favor of third-

123. *Safeguarding* Part II, *supra* note 111.

124. Information Protection Security Act, S. 500 109th Cong. § 2(a)(6) (2005).

125. *Id*. at § 2(a)(5).

126. FTC—Identity Theft Victim Complaint Data, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf (last visited Jan. 21, 2008).

party commercial or publication interests.[127] Constitutional law offers few protections for individuals seeking a right to data privacy.

Contract and property law are similarly limited because of judicial deference to markets and choice in commercial transactions.[128] Contract and property law based restrictions on the free trade of personal data would therefore need to be statutory; however, legislative actions in the data privacy domain are inconsistent and leave vast gaps. These legislative problems reflect the lack of an omnibus data privacy statute and the ad hoc, reactive nature of legislating data privacy in the U.S.[129] Judicial deference on privacy issues furthers these gaps. Narrow statutory interpretations, questions of standing, and deference to law enforcement and national security objectives weaken the possibility of relief in the courts. The general lack of judicial oversight of personal data use essentially grants users, data brokers, and the government a "blank check" to freely tap database-driven information markets for commercial, investigative, or other profiling purposes.

A. Paparazzi and the Right to Privacy

Samuel D. Warren and Louis D. Brandeis first advocated for a right to privacy in their influential law review 1890 article, *The Right to Privacy*.[130] Their approach established the foundation for a right to privacy in tort law and

127. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 534 (2001) ("In these cases, privacy concerns give way when balanced against the interest in publishing matters of public importance."); *Id.* at 555 (Rehnquist, C.J., dissenting) ("Surely 'the interest in individual privacy,' ante, at 1765, at its narrowest must embrace the right to be free from surreptitious eavesdropping."); Florida Star v. B. J. F., 491 U.S. 524, 530 (1989) (finding that a newspaper is not liable for publishing a rape victim's name despite violation of state law); Smith v. Daily Mail Publishing Co., 443 U.S. 97, 105-06 (1979) (finding a state statute prohibiting publication of a juvenile delinquent's name unconstitutional under freedom of press); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 494-95 (1975) (finding no privacy interest in public court records accessed by the press); Time, Inc. v. Hill, 385 U.S. 374, 388-90 (1967) (finding that constitutional protections for speech and press precluded false report claim). *But see* Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 174-75 (2004) (holding that the privacy interests of Vincent Foster's family outweighed rationale for a FOIA disclosure request); Cohen v. Cowles Media Co., 501 U.S. 663, 665 (1991) (holding newspaper's first amendment right to publish did not render it immune in a breach of contract action for damages resulting from violation of a confidentiality agreement); U.S. Dept. of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989) (protecting rap sheets from disclosure under the Freedom of Information Act); Seattle Times Co. v. Rhinehart, 467 U.S. 20, 36-37 (1984) (finding newspaper's first amendment rights were not violated by protective order prohibiting publication of data accessed through discovery); Houchins v. KQED, Inc., 438 U.S. 1, 15-16 (1978) (finding that there is no specific press privilege to access penal institution); Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562, 578-79 (1977) (finding that the First Amendment was not a defense in right of publicity action); Gertz v. Robert Welch, Inc., 418 U.S. 323, 347 (1974) (holding petitioner was a private figure in his defamatory falsehood action against a magazine which won in both lower courts).

128. *See* SOLOVE, *supra* note 7, at 76-77, 81-84, 90 (arguing that an individual's lack of control, knowledge, and participation in data sharing defeats property and contract law theories).

129. *Id*. at 71.

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

followed the logic of a tort prima facie case.[131] The common law torts of invasion of privacy, intrusion upon seclusion, public disclosure of private facts, publicity in a false light, and appropriation are supported by this article.[132] Although courts still look to the article for a definition of a right to privacy,[133] it is now more than one-hundred years old and poorly adapts to the modern phenomenon of database-driven information markets.

The Warren and Brandeis framework is limited by its focus on physical invasions of privacy, for example, photographs and publications. When non-physical invasions are involved, such as private thoughts or expressions, their approach requires a showing of actual injury or harm.[134] Their limited scope reflects their original inspiration for the article: unwanted paparazzi coverage of personal affairs.[135] The harm requirement coupled with the consent exception together are now formidable barriers in tort-based actions against data sharing in database-driven information markets.[136] Although Warren and Brandeis captured the concept of a right to privacy, their formulation did not go far enough to promote an affirmative right to privacy.[137]

Warren and Brandeis embraced the idea that a right to privacy includes a "right to be left alone."[138] The emerging paparazzi's ability to use the new technology of "instantaneous photographs … to satisfy a prurient taste," in this case, for tabloid newspapers, greatly concerned Warren and Brandeis.[139] They recognized the harm to individuals caused by invasions of privacy from new technologies. They envisioned a time of increased complexity and modernity which would make "solitude and privacy … more essential to the individual."[140] Their focus on an individualized right to privacy was based on a theory of "inviolate personality."[141] This theory underpins the right to privacy embodied by defamation, breach of implied contract, and property law-based protections of intellectual property.[142]

By focusing on an individual's right to his personality, the right to privacy was conceived broadly to protect "thoughts, emotions, and sensations … whether

131. *Id*.

132. *See* RESTATEMENT (SECOND) OF TORTS § 652 (1979). *See also* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (setting forth the tort causes of action recognized by the courts).

133. Warren & Brandeis, *supra* note 130, at 193.

134. *Id*. at 197-98.

135. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 9-10.

136. Most activities involving data disclosures, such as buying a car, applying for employment, or applying for credit, involve consent from the applicant just to receive consideration. There is no bargaining power for individuals. *See* SOLOVE, *supra* note 7, at 85 (noting the "take it or leave it" choice of applicants). Harm is also difficult to prove. *Id*. at 95.

137. Warren & Brandeis, *supra* note 130, at 216-18 (noting that the right to privacy permits certain publications, although the subject matter is private, as in oral publication and consensual publication).

138. *Id*. at 195.

139. *Id*. at 195-96.

140. *Id*. at 196.

141. *Id*. at 205.

142. *Id*.

expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression[s]"[143] and are "rights as against the world."[144] A right to damages was recognized based on actual and emotional harm concepts.[145] Perhaps in an effort to complete the legal doctrine, Warren and Brandeis also set forth some exceptions to the right to privacy, including publication of matters of public or general interest, privileged communications under the law of slander and libel, oral publication, and consensual publication.[146] The consent exception is significant because most personal data collected to feed the database-driven information markets is under the auspices of default consent. This default consent is further reinforced by weak "opt-out" provisions in private data gathering activities or legally required data reporting to public authorities. These exceptions are so large they swallow the rule.

B. Tort and Contract Law: Right to Privacy Limitations

For example, tort plaintiffs find it difficult to overcome the exception for public interest when confronted with a publisher's right to publish under the First Amendment. In *Cox Broadcasting Corp. v. Cohn*, the Supreme Court determined that the State of Georgia could not enforce a private cause of action for invasion of privacy, namely the tort of public disclosure, when the personal data at issue was publicly available in a court record prior to publication.[147] Although it recognized the fundamental privacy consideration of the Warren and Brandeis article, the Court nonetheless weighed in favor of the press's first amendment rights over the plaintiffs' need to be protected from "mental pain and distress, far greater than could be inflicted by mere bodily injury."[148] The Court further constrained the specific individual protections endorsed by Warren and Brandeis by asking whether a "reasonable man" would find the unwanted disclosure "offensive."[149]

In *Cox Broadcasting Corp.*, the plaintiffs ultimately failed because the data they sought to protect from publication were a matter of public record.[150] Although the Court suggested that the appropriate remedy was to seal the court records, this approach ran counter to a strong presumption of public access to court records to instill public confidence in the government.[151] Although some court proceedings may contain sensitive matters and warrant protection, most cases do not qualify for such heightened protection. At a minimum, data

143. *Id*. at 206.
144. *Id*. at 213.
145. *Id*. at 219.
146. *Id*. at 214-18.
147. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 475-76 (1975).
148. *Id.* at 487 n.16 (citing Warren & Brandeis, *supra* note 130, at 196).
149. *Id.* at 496.
150. *Id.* at 495-96.
151. *Id.* at 492, 496. *See also* SOLOVE, *supra* note 7, at 129, 133-34 (describing that court records are typically presumed to be public and mechanisms such as protection order rules of civil procedure face a strong presumption against them).

disclosed in cases typically include names, addresses, places of employment, marital status, and social security numbers.[152] Daniel Solove concludes that "[a]ccess to court records permits people to examine the information considered by courts making decisions affecting the public at large."[153] Thus, the public records doctrine frequently trumps an individual's right to privacy, regardless of the strength of the individual's privacy interests.

In *Nixon v. Warner Communications, Inc*., the Supreme Court expressed firm support for public access to public court records when it held that "[i]t is clear that the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents."[154] Although the Court conceded that the right to inspection was not absolute, any restrictions are on a case-by-case basis at the discretion of the trial court judge.[155] A judge may exercise discretion if court files are used for "improper purposes" such as "'gratify[ing] private spite or promot[ing] public scandal.'"[156] As a result, public records are an important source of data for data brokers. Such data are actively traded commodities in the database-driven information markets. Efforts by public authorities to accumulate data and improve access to public records are an unintended public subsidy to data brokers and the database-driven information markets.[157] Personal information freely available through public records rarely triggers individual privacy concerns.[158]

Lack of protection for personal data stored in public records is consistent with the narrowness of tort privacy laws. Consensual or voluntary disclosure of personal data limits remedies available under tort law. For example, in *Dwyer v. American Express Co*., an Illinois appellate court granted defendant American Express's motion to dismiss in an action for invasion of privacy and consumer fraud relating to defendant's practice of renting its customer data.[159] American Express used its customer data to create lifestyle profiles and targeted customer lists for use by third-party merchants.[160] Under the invasion of privacy tort, a

152. SOLOVE, *supra* note 7, at 129.

153. *Id*. at 141.

154. Nixon v. Warner Comm'ns, Inc., 435 U.S. 589, 597 (1978).

155. *Id.* at 597-99 (citing to cases protecting the use of the courts from being repositories of damaging disclosures in divorce and business litigation).

156. *Id.* at 598 (quoting *In re* Caswell, 29 A. 259, 259 (R.I. 1893)). *Caswell* set forth a common law rule that persons gaining access to court records through the right to inspection must have an interest in the documents related to a legally recognized privacy interest. *Id.* Mere curiosity is insufficient. *Id.* In *Caswell*, the Supreme Court of Rhode Island used its discretion to bar access to the records in a divorce proceeding because it deemed the requestor, a publication, intended an "improper use." *Id.* Unfortunately, the Supreme Court has retreated to judicial discretion instead of exploring the right to inspection as it relates to privacy concerns and the use of court records to populate massive commercial databases.

157. For a further discussion on privacy market failures and subsidies, see Schwartz, *supra* note 33, at 2078-79.

158. *Cf.* SOLOVE, *supra* note 7, at 150-51 (observing that Freedom of Information Act information is frequently used for commercial purposes, such as mailing lists, rather than transparency in government).

159. Dwyer v. American Express Co., 652 N.E.2d 1351, 1353 (Ill. App. 1995).

160. *Id.*

four-part prima facie case requires: "(1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion which is offensive or objectionable to a reasonable man; (3) that the matter upon which the intrusion occurs is private; and (4) that the intrusion causes anguish and suffering."[161] In this case, the court held that because the cardholders voluntarily used the American Express card, there was no unauthorized intrusion.[162] The court further concluded that spending data were not private to the individual cardholders, but were rather business records of the card issuer.[163] Thus, simply by using their credit cards, individuals were releasing information about their spending habits to unknown third parties.

The *Dwyer* court also sought additional support in *Shibley v. Time, Inc*.[164] In *Shibley*, an Ohio court of appeals upheld a company's right to sell or rent magazine subscription lists to third parties based on limitations of the invasion of privacy tort.[165] The *Shibley* court refused to find a right to privacy cause of action and, in an act of judicial deference, suggested that the legislature was the appropriate forum.[166] Regardless of an individual's privacy concerns, tort law remedies for right to privacy violations often fail to cover many types of disclosures relied upon by commercial data brokers.[167]

Further, if personal data are deemed public in nature, the tort cause of action fails unless use of the personal data is "highly offensive to a reasonable person."[168] The problem with this standard is that it does not protect most personal data, such as names, addresses, social security numbers, purchasing, and financial transaction histories. In *Busse v. Motorola, Inc.,* an Illinois appellate court affirmed the trial court's decision to grant defendants' summary judgment in plaintiffs' claim for invasion upon seclusion.[169] Plaintiffs alleged that defendants violated their right to privacy when defendants provided customer data to a private research firm for a study on wireless telephone use and health.[170] The court concluded that the customer data shared in the study were of public

161. *Id.* at 1354. *See also* RESTATEMENT (SECOND) OF TORTS § 652B (1979).

162. *Dwyer*, 652 N.E.2d at 1354.

163. *Id*.

164. 341 N.E.2d 337, 339-40 (Ohio Ct. App. 1975).

165. *Id.* at 339 ("The short, though regular, journey from mail box to trash can … is an acceptable burden, at least so far as the Constitution is concerned" (quoting Lamont v. Comm'r of Motor Vehicles, 269 F. Supp. 880, 883 (S.D.N.Y. 1967))).

166. *Id.* at 340.

167. For an interesting case discussing permissible investigative methods and publicity in claims of libel and invasion of privacy as related to consumer reporting agencies, see Tureen v. Equifax, Inc., 571 F.2d 411, 415-19 (8th Cir. 1978).

168. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

169. Busse v. Motorola, Inc., 813 N.E.2d 1013, 1015 (Ill. App. Ct. 2004).

170. *Id.* at 1015 (The customer data disclosed included "names, street addresses, cities, states, zip codes, dates of birth, social security numbers, wireless phone numbers, account numbers, start-of-service dates and the electronic serial numbers of the customers' phones. ERI obtained missing data for some wireless customers through a contract with TRW, a credit bureau.").

record and not private data.[171] Because data such as social security numbers were not considered private data under state law, the court agreed with the defendants.[172] This result illustrates the third-party gap in tort protection. Third parties enjoy an almost unfettered right to access, use, and distribute public record information. Public data are not considered personal to the individual, regardless of how personal the data actually are to the individual.

In addition to tort law, Warren and Brandeis suggested contract law-based rationales for a right to privacy.[173] Express or implied contract terms for confidentiality are legally recognized means of protection against unwarranted disclosures.[174] Freedom to contract is upheld by the courts and implied terms are part of the contract.[175] In *Busse*, plaintiffs also alleged breach of contract based on the Federal Telecommunications Act of 1996.[176] Although the Act appeared "'to protect the confidentiality of proprietary information,'"[177] it had numerous loopholes biased in favor of carriers. For example, carriers were permitted to "use or disclose customer information to protect the carriers' own rights and property,"[178] and "provide aggregated information to other carriers or persons on reasonable terms upon reasonable request."[179] The Federal Communications Commission, which enforced the Act, also allowed carriers to "'use, disclose, or permit access to [customer information] for the purpose of conducting research on the health effects of wireless phone use.'"[180] These permissive uses of customer data defeated plaintiffs' right to privacy action. Although some exceptions may be warranted, carte blanche statutory authorization fundamentally interferes with an individual's privacy interests. Statutory frameworks like the Federal Telecommunications Act often make trade-offs contrary to an individual's data privacy interests.

C. Information Markets, Property Law, and the Right to Privacy

In the age of database-driven information markets, tort and contract law are not the only substantive law sources that fail to adequately protect individual privacy interests. Under both substantive property law and fourth amendment jurisprudence, the theory of personal data as property also achieves limited success in affirming an individual's right to data privacy. This failure reflects the

171. *Id.* at 1018 ("Matters of public record—name, address, date of birth and fact of marriage—have been held not to be private facts." (citing Geisberger v. Willuhn, 390 N.E.2d 945 (Ill. App. Ct. 1979))).

172. *Id.* at 1017-18.

173. Warren & Brandeis, *supra* note 130, at 210.

174. *Id*. at 208-10.

175. SOLOVE, *supra* note 7, at 77.

176. *Busse*, 813 N.E.2d at 1016 (citing 47 U.S.C. § 222 (2000)).

177. *Id*. (quoting 47 U.S.C. § 222(a) (2000)).

178. *Id.* (citing 47 U.S.C. § 222(d)(2) (2000)).

179. Busse v. Motorola, Inc., 813 N.E.2d 1013, 1016 (Ill. App. Ct. 2004) (citing 47 U.S.C. § 222(c)(3) (2000)).

180. *Id.* (quoting 47 C.F.R. § 64.2005(c)(2) (2003)).

property-influenced focus on "ownership status" of information.[181] Property-based theories that allocate ownership rights often break down when applied to third parties that trade personal data in the database-driven information markets.[182] Even if individual property interests in personal data are legally recognized, the practicality of enforcing such rights today, given the size and breadth of database-driven information markets, is questionable.[183] Further, data brokers may have a conflicting property claim over individual personal data because once such data are gathered and stored by the data broker, the data likely become the data broker's property.[184] Without recognized property rights, individuals have no claim to the profits earned from their personal data.[185]

Some commentators suggest that the growth of database-driven information markets reflects free-market capitalism at its best. Markets enable personal data to be traded like any other commodity for the benefit of corporations selling or using the data and for consumers enjoying more highly targeted and theoretically valuable advertising.[186] Accordingly, more trade in personal data is better because markets maximize utility, liberty, and efficiency.[187] Richard Posner further argues that free trade in personal facts is economically efficient because it addresses the problem of misrepresentation.[188] Posner sees the desire to conceal personal information as one of misrepresentation rather than a desire "to be let alone."[189] He argues that allocation of the property interest in personal data is therefore best held by third parties and not individuals.[190] Posner also suggests that transaction costs would be unacceptably high if individuals "owned" the personal facts about them.[191]

Although he argues against privacy protection for personal data, Posner maintains that protection is appropriate when an economic rationale for disclosure is absent. For example, Posner believes that the Supreme Court in *Cox Broadcasting Corp.* should have protected the family's privacy interest because the societal value of disclosure was non-existent and well below the harm caused to the family given that the individual behind the disclosure was

181. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000).

182. Schwartz, *supra* note 33, at 2056-57.

183. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV 1125, 1135 (2000) (describing the enormous transaction costs inherent in individual-level trading of personal data).

184. *See id*. at 1133 ("Because they may have invested time, money and energy in compiling, organizing, or processing the data, they may well think of themselves as owning the data they have gathered or otherwise acquired.").

185. *Cf. id*. at 1134-35 (noting that once property rights are recognized, individuals will be able to profit from the sale of their personal data to brokerage companies).

186. *See* Cohen, *supra* note 181, at 1392-93. *See also* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394-95 (1978).

187. SOLOVE, *supra* note 7, at 78-79.

188. Posner, *supra* note 186, at 395.

189. *Id*. at 398-400.

190. *Id.*

191. *Id*. at 398.

deceased.[192] Posner also recognizes privacy protection for personal communications.[193] He draws a line between communication and fact. Intrusions on personal communications through eavesdropping or efforts to obtain private notes, letters, and papers limit freedom of expression.[194] Even in Posner's market-based privacy framework, privacy protection is warranted to meet non-economic goals such as protection from harm, preservation of richness of ideas and dialogue, and as a "safeguard against political oppression."[195]

Pro-market arguments for the allocation of privacy rights often inadequately deal with four pervasive market imperfections: (1) imbalances in power between corporations, government, and individuals;[196] (2) asymmetric information among the players;[197] (3) vastly unequal transaction costs;[198] and (4) the inability of the markets to protect human dignity, self-realization, and personal liberty.[199] These market imperfections could be addressed by a right to privacy solution, but any solution would face opposition from the multi-billion dollar database-driven information markets, growing government use of third-party data, and rapidly expanding technological capabilities to gather, aggregate, and sell even more data. The right to data privacy requires a higher authority to gain traction. Constitutional authority through the Fourth Amendment's basic genesis of a right to data privacy should be revisited.

IV. FOURTH AMENDMENT INTERPRETATION STRUGGLE

This section explores fourth amendment jurisprudence chronologically, starting with early cases where the Court found strong protections for privacy interests and continuing through to more recent decisions. This survey highlights the potential of the Fourth Amendment to support individual privacy rights and suggests that the Court's treatment of fourth amendment-related interests is too narrow. The Court's deferential approach illustrates the Court's movement away from individual data privacy protection in favor of government investigatory interests. This modern approach to the Fourth Amendment is in stark contrast

192. *Id*. at 416.

193. *Id*. at 403-04.

194. *Id*. at 402-03, 420.

195. *Id*. at 409, 416-17, 419-21.

196. Cohen, *supra* note 181, at 1395.

197. Schwartz, *supra* note 33, at 2078 (observing that in the case of spyware, a type of secretive data gathering software tool spread through Internet applications, the asymmetric information problem is particularly acute as individuals typically do not know the data are being collected or how it will be further processed and shared. In this case, individuals have no information upon which to bargain.).

198. Cohen, *supra* note 181, at 1397.

199. *Id.* at 1386-87. Solove highlights the problems under market theory and the power of contract law to allocate privacy interests because of bargaining power imbalances, lack of competition, clandestine data collection practices, lack of knowledge among individual data subjects, vaguely worded privacy policies, and no market visibility into the conduct of third parties. He also notes that third party aggregation and use of personal data alone defeats contract and property theories as the transaction no longer involves the individual. SOLOVE, *supra* note 7, at 81-90.

from the Court's early cases. This erosion of protection prompted congressional response, but due to the nature of the legislative process, many holes and gaps remain. Thus, a comprehensive statutory framework is needed to address fundamental data privacy interests across all industries and applications.

A. Introduction to Fourth Amendment Jurisprudence

The Fourth Amendment on its face suggests strong protections for individual data privacy by providing

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[200]

Although the Fourth Amendment does not specifically use the word "privacy," it gives the people an affirmative right of security in their personal possessions and protects that right through procedural and judicial oversight.[201] According to Raymond Ku, fourth amendment privacy protection is more properly interpreted as protection against the power of the government than of an individual's right to privacy.[202] Ku contends that because the Founders were primarily concerned with "unfettered government power and discretion," the primary role of the Fourth Amendment was to "[protect] the people generally from self-interested government."[203] This privacy protection was embodied in the people as a check on overreaching government surveillance.[204] Based on historical precedent, Ku argues that the Founders clearly left the determination of what constituted a lawful search to the people, not to the courts.[205] Today, the power to determine whether a search violates the Fourth Amendment remains with the courts, not the people. Herein is the problem. If fourth amendment issues were treated as ones of fact rather than law, the people may have opted for more privacy protection than that currently embraced by the courts.

The Supreme Court's increasingly activist and narrow interpretation of the Fourth Amendment has tilted the balance toward government power at the expense of individuals.[206] This imbalance is especially true in cases involving the government's use of emerging technologies.[207] The Court's deference to law enforcement and other governmental interests in fourth amendment cases has

200. U.S. CONST. amend. IV.

201. U.S. CONST. amend. XIV.

202. Ku, *supra* note 5, at 1325 ("The Fourth Amendment protects power not privacy.").

203. *Id*. at 1332, 1338 (quoting AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 67-68 (1998)).

204. *Id.* at 1338.

205. *Id*. at 1340.

206. *Id*. at 1356-57.

207. *Id*. at 1356 ("[C]urrent Fourth Amendment law suggests that the use of surveillance technology is not a search.").

"allow[ed] technology to dictate the degree of privacy and security that society will enjoy."[208] Technology determines whether information is public or private, relegating fourth amendment protection to a shrinking realm of private information. Further, the Court permits the government to define the parameters of its technology-based searches unless it violates a traditional liberty interest enumerated in the Fourth Amendment.[209]

The Court struggles to enforce the Fourth Amendment in cases involving new technologies. The power of the Fourth Amendment only remains clear when framed by experiences closely analogous to those of the Founders. Justice Scalia advocates this perspective as illustrated by special concerns for physical intrusion of the home;[210] however, modern searches and seizures do not need physical intrusion as in the Founders time. In the case of government databases and data mining,[211] such activities amount to "covert surveillance" when done outside of the five basic procedural protections of the Fourth Amendment: (1) particularized suspicion; (2) probable cause; (3) particularized scope defined within the warrant itself; (4) judicial review; and (5) prior authorization.[212] Because the Fourth Amendment's "'basic purpose … is to safeguard the privacy and security of individuals against arbitrary invasions by government officials,'"[213] the Court's treatment of the Fourth Amendment can be successfully analogized to cover the government's data mining activities.[214] Data mining constitutes a search by its very definition.[215] The government's data mining activities are arguably done without particularity, probable cause, a warrant, or judicial review.[216] But data mining seems unlikely to fall under fourth amendment scrutiny. The evolution of fourth amendment jurisprudence reveals the Court's tendency toward a narrow interpretation and support for expanded law enforcement powers. This approach prevails at the expense of Brandeis's privacy argument, a perspective potentially more consistent with the intent of the

208. *Id*. at 1350.

209. *Id*. at 1367-68.

210. *See* Kyllo v. United States, 533 U.S. 27, 34-37 (2001) (holding that thermal imaging still involves intrusions on the home).

211. *See* Tien, *supra* note 28, at 393 (providing several definitions of data mining, including one from the General Accounting Office, as follows "the application of database technology and techniques-such as statistical analysis and modeling-to uncover hidden patterns and subtle relationships in data and to infer rules that allow for prediction of future results").

212. *Id.* at 401-02.

213. *Id*. at 400 (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949)).

214. *Id*. at 408.

215. *Id*. Tien suggests that many commentators and courts would typically exclude data mining as a search because the underlying raw data has been publicly disclosed, and thus, no remaining expectation of privacy exists in the individual and the Fourth Amendment is deemed not applicable. Tien's argument goes deeper though, by focusing on the "knowledge" gained by "connecting the dots" between these discrete data elements to create a picture of the whole. *Id*. at 408. He provides a useful illustration of a privacy expectation exposed by mere purchasing habits: the cycle of a woman's pregnancy can be observed by the woman's drug store purchasing pattern without a public disclosure by the woman that she is pregnant. *Id*. at 409.

216. *Id*. at 405-08.

Founders. Over time, the Court effectively diminishes several explicit protections in the Fourth Amendment.

B. Fourth Amendment: Early Cases

The Supreme Court initially gave breath to the Fourth Amendment. In *Ex Parte Jackson*, the Court held that letters and sealed packages were free from examination unless the examination met the conditions specified within the Fourth Amendment.[217] The Court thus recognized that the Fourth Amendment reached beyond the confines of a person's household "to their papers, thus closed against inspection, wherever they may be."[218] Likewise, the Supreme Court's holding in *Boyd v. United States* established that compulsory production of business records violated the Fourth and Fifth Amendments.[219] The Court in *Boyd* argued that these Amendments were related and should be liberally construed to protect from "gradual depreciation" caused by "stealthy encroachments thereon."[220] The Court's vigilant protection of privacy rights reflected an originalist interpretation that considered these Amendments a matter of "[the] very essence of constitutional liberty and security."[221] The government's actions contrary to the Fourth Amendment were treated by the Court as grave intrusions on an individual's "indefeasible right of personal security, personal liberty and private property."[222] Although Congress's transgressions were also deemed to be serious violations of these constitutional principles, the Court excused Congress's lapses because of distractions from the "vast accumulation of public business brought before it."[223] Therefore, an active judiciary protected individuals' right to privacy from congressional lapses under the Fourth and Fifth Amendments.

In facing its first new technology, the Court broke with tradition in *Olmstead v. United States* and held that the Fourth Amendment was limited only to physical intrusions.[224] *Olmstead* involved federal government wiretapping of telephone lines used by defendants during an investigation of Prohibition violations.[225] The majority argued that because telephones involved wires

217. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

218. *Id.*

219. Boyd v. United States, 116 U.S. 616, 634-35 (1886), *overruled by* Warden v. Hayden, 387 U.S. 294 (1967) ("[A] compulsory production of the private books and papers of the owner of goods sought to be forfeited in such a suit is compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution, and is the equivalent of a search and seizure—and an unreasonable search and seizure—within the meaning of the Fourth Amendment.").

220. *Id.* at 635.

221. *Id.* at 630.

222. *Id*.

223. *Id*. at 635.

224. Olmstead v. United States, 277 U.S. 438, 466 (1928), *superseded by statute*, the Federal Communications Act of 1934 § 605 (making wiretapping a federal crime) (codified now at 47 U.S.C. § 605 (2000)).

225. *Id.* at 454-57.

outside the home "reaching to the whole world" any expansion of the Fourth Amendment beyond the plain language of "houses, persons, papers, and effects" was unwarranted.[226] The Court held that any intrusions of one's privacy must be material or physical in nature.[227] New technologies such as telephony, although not in existence at the time the Fourth Amendment was written, did not receive protection because such technology was in a sense intangible.[228] In its majority opinion, the Court held for the first time that there should not be an expectation of privacy under the Fourth Amendment based on the medium used, here intangible telephony, by the individual.[229] The Court further concluded that although wiretapping violated a state law, the illegally obtained evidence was admissible because the law did not preclude evidence gathered by illegal wiretapping.[230] The Court in *Olmstead* thus departed from a path toward comprehensive privacy protection to one both fragmented and statutory in nature.

In a sharply divided decision, the majority opinion in *Olmstead* prompted a strong dissent from Brandeis. Quoting Chief Justice Marshall, Brandeis reminded the majority "that it is a constitution we are expounding," and that the Constitution was "designed to approach immortality as nearly as human institutions can approach it."[231] Brandeis believed that "[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a … capacity of adaptation to a changing world."[232] He argued that "[t]ime works changes, brings into existence new conditions and purposes."[233] To further his point, Brandeis warned that advances in science would enable even more non-intrusive means of government surveillance outside the protections of the now narrowly interpreted Fourth Amendment and with the effect of "'plac[ing] the liberty of every man in the hands of every petty officer.'"[234] Brandeis took seriously the liberty interests at stake because

> [o]f all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers, from the inspection and scrutiny of others. Without the enjoyment of this right, all others would lose half their value.[235]

226. *Id.* at 465.
227. *Id.* at 464.
228. *Id.* at 466.
229. *Id*.
230. *Id.* at 467.
231. *Id*. at 472-73 (Brandeis, J., dissenting).
232. *Id.* at 472 (Brandeis, J., dissenting).
233. *Id.* at 472-73 (Brandeis, J., dissenting).
234. Olmstead v. United States, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting) (quoting JAMES OTIS, AGAINST WRITS OF ASSISTANCE (1761), *reprinted in* M.H. SMITH, THE WRITS OF ASSISTANCE CASE 553 (1978)).
235. *Id.* at 475 n.3 (Brandeis, J., dissenting) (quoting *In re* Pac. Ry. Comm'n, 32 F. 241, 250 (N.D. Cal. 1887)).

The *Olmstead* decision proved unpopular and Congress addressed it through the Federal Communications Act of 1934, which made wiretapping by the federal government illegal.[236] This prompted statutory response to fill gaps left by the Court, a trend that would become typical in future fourth amendment cases.

C. Fourth Amendment Minimalization

Despite Brandeis's impassioned arguments for his right to privacy interpretation, the Supreme Court maintained its narrow view in a series of cases in the 1960s.[237] In 1967, the Court made two decisions that refused to acknowledge a general constitutional right to privacy under the Fourth Amendment.[238] Through an analogy to property law, the Court suggested that such protection was best left to the states.[239] In *Katz v. United States*, the federal government participated in wiretapping outside a public phone booth.[240] The Court held in *Katz* that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of fourth amendment protection."[241] Nonetheless, the Court was able to find fourth amendment protection over defendant's use of a public phone booth.[242] Although the Court's holding attached fourth amendment protections to the person and not the place, the fact that the defendant "shut[] the door behind him" was pertinent to the outcome.[243]

In his concurring opinion, Justice Harlan set forth a test for fourth amendment cases that went beyond the majority's physical intrusion mindset. Justice Harlan's test followed a typical test construction in substantive law—whether a person had a subjective expectation of privacy and whether that expectation is recognized by society as objectively reasonable.[244] Unfortunately, this test has proven hollow in modern times. Database-driven information markets and increased government surveillance since 9/11 challenge the objective expectation of privacy and make any subjective expectation of privacy

236. 47 U.S.C. § 605 (2000). The statutory approach making wiretapping a crime is a typical responsive approach seen in recent legislation such as the Identity Theft and Assumption Deterrence Act of 1998. Wiretapping remains a timely issue with several recent statutory changes making wiretapping by the government more easily accomplished without the procedural protections of warrants and probable cause. *See* USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of the U.S.C.);

USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (codified as amended in scattered sections of the U.S.C.).

237. Although the Supreme Court was interpreting a right to privacy in other areas of the Constitution, such as in Griswold v. Connecticut, 381 U.S. 479, 480 (1965), the Court otherwise retrenched on the Fourth Amendment.

238. Katz v. United States, 389 U.S. 347 (1967); Warden v. Hayden, 387 U.S. 294 (1967).

239. *See Katz*, 389 U.S. at 350-51.

240. *Id*. at 348.

241. *Id.* at 351.

242. *Id.* at 353.

243. *Id.* at 352-53. *See also* Silverman v. United States, 365 U.S. 505, 509, 511-12 (1948) (holding that eavesdropping using an electronic device to "hear through walls" is unconstitutional under the Fourth Amendment).

244. *Katz,* 389 U.S. at 361.

inherently unreasonable. Harlan's test supports a finding of privacy in a phone booth because the phone booth serves as a discrete, personal space.[245] *Katz* and the Harlan test prove less useful in a world with obsolete phone booths and defined physical spaces becoming more virtual or non-existent.

In *Warden v. Hayden*, the Supreme Court returned to the issue of property seized for mere evidentiary value and overturned *Boyd*, holding that personal effects, such as papers, or in this case, clothing, could be seized by the government, even at the risk of self-incrimination.[246] The Court asserted that "[w]e have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts."[247] By eliminating the distinction between property seized via "intrusions to secure 'mere evidence' from intrusions to secure fruits, instrumentalities, or contraband," the Court broadened the scope of lawful search and seizure and thereby reduced the Fourth Amendment to its procedural safeguards: probable cause, particularity, and a neutral magistrate; and removed the courts from assessing property or privacy rights based on substantive law in search and seizure cases.[248]

It did not take long for the Court to erode even this last remaining privacy protection under the Fourth Amendment. In *Terry v. Ohio*, the Court permitted warrantless police searches and seizures upon "reasonable suspicion" during a protective search for weapons, as long as the intrusion was brief.[249] The Court relaxed fourth amendment "probable cause" to a reasonableness test because of concerns about the physical safety of police officers and the public at large.[250] In *Terry*, the Court agreed that the officer who stopped Terry and two other men had a reasonable suspicion of criminal mischief and a fear of concealed weapons,[251] ultimately concluding that the warrantless search and seizure was permissible under the Fourth Amendment.[252] Although the majority strained to reconcile its opinion with the basic tenets of fourth amendment procedure,[253] the dissenting opinion of Justice Douglas clearly described the weaknesses in the

245. *Id*.

246. *Warden*, 387 U.S. at 300-01. For Justice Douglas's strong dissent based on history of the Fourth and Fifth Amendments and the spirit of the right to privacy, see *id*. at 312-25.

247. *Id.* at 304.

248. Warden v. Hayden, 387 U.S. 294, 298-99, 309-10 (1967).

249. Terry v. Ohio, 392 U.S. 1, 26 (1968). The test set forth in *Terry* follows the Harlan concurring opinion in *Katz*. The "*Terry* Stop" test is: (1) whether "a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger" and (2) whether the officer acted in an objectively reasonable manner given "the specific reasonable inferences which he is entitled to draw from the facts in light of his experience." *Id.* at 27.

250. *Id.* at 24 n.21 (mentioning the prevalence of firearm use and police fatalities and injuries over the prior seven-year period).

251. *Id.* at 6.

252. *Id.* at 30, 31.

253. *Id.* at 21-22.

Court's retreat from probable cause.[254] Douglas held fast to the fourth amendment's higher burden of proof required by probable cause and defended the warrant process as necessary in countering power imbalances between the police and the people.[255] As demonstrated by the *Terry* decision, fourth amendment protections substantially eroded in a few short years during the 1960s. The result was that the reasonable expectation test first proposed in *Katz* not only overtook an individual's right to privacy, but further gutted procedural protections. In the 1970s, the Court's narrow interpretation would again be applied to benefit law enforcement, but this time in the context of banking records.

D. Fourth Amendment's Last Temptation: Data-Rich Financial Records

In *California Bankers Ass'n v. Shultz,* the Supreme Court determined that there were no objectively reasonable expectations, and thus no subjectively reasonable expectations of privacy, in banking records.[256] By opening access to these records, the Court's decision ultimately required banks to maintain records of checks and other instruments, including account information on all customers for government law enforcement uses.[257] The Court upheld the broad authority granted to the Secretary of the Treasury in the Bank Secrecy Act of 1970.[258] Through its liberal data sharing provisions, the Act allowed any federal agency to receive regular reporting from banks. Under threat of penalty, banks were to report on transactions deemed by the government or the bank to be of a suspicious nature.[259] The Act did not contain any fourth amendment procedural protections for customers whose records were being reported in secret to the government.

The Bank Secrecy Act of 1970 contained two primary requirements: (1) record retention of account and (2) transactional information for government law enforcement use and proactive reporting by banks to the government on domestic and foreign transactions over $10,000, with some specified exceptions, as required by the United States Department of Treasury ("Treasury").[260] By

254. *Id.* at 36 (Douglas, J., dissenting) ("We hold today that the police have greater authority to make a 'seizure' and conduct a 'search' than a judge has to authorize such action. We have said precisely the opposite over and over again.").

255. *Id.* at 38 (Douglas, J., dissenting) ("To give the police greater power than a magistrate is to take a long step down the totalitarian path. Perhaps such a step is desirable to cope with modern forms of lawlessness. But if it is taken, it should be the deliberate choice of the people through a constitutional amendment.").

256. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 61-62 (1974).

257. *Id.* at 26, 66-67.

258. Pub. L. No. 91-508 § 101 (codified at 12 U.S.C. § 1829b(b)(1) (2000)) ("Where the Secretary of the Treasury … determines that the maintenance of appropriate types of records and other evidence by insured depository institutions has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, he shall prescribe regulations to carry out the purposes of this section.").

259. *Cal. Bankers Ass'n*, 416 U.S. at 40-41.

260. *Id.* at 39. These forms require: (1) "the name, address, business or profession and social security number of the person conducting the transaction; (2) similar information as to the person

allowing the government to use third parties to get around the fourth amendment prohibitions on search and seizure of private papers, the Court wrote "papers" out of the protection of the Amendment. The Court also opened the door on the government's liberal co-opting of third parties to avoid individual fourth and fifth amendment claims.[261] Individuals lost standing because banking records were now forcibly retained by law and viewed as the property of the third-party banks rather than account holders.[262]

The dissenting justices in *California Bankers Ass'n* raised serious concerns about the majority's blithe treatment of financial records and rejection of individual standing regarding such records. Justice Douglas recognized that "[t]he Bank Secrecy Act requires banks to record and retain the details of their customers' financial lives."[263] Douglas contended that

> [c]ustomers have a constitutionally justifiable expectation of privacy in the documentary details of the financial transactions reflected in their bank accounts. That wall is not impregnable. Our Constitution provides the procedures whereby the confidentiality of one's financial affairs may be disclosed.[264]

Financial records are not the only type of records for which mandatory retention is attractive because of information content. Mandatory transaction histories from bookstores, pharmacies, or hardware stores would likewise be "useful" in law enforcement.[265] The tremendous amount of personal information available from banking records goes beyond mere numbers to also reveal an individual's "religion, ideology, opinions, and interests" and his associations, beliefs, politics, and personality.[266] Furthermore, the scope of the Bank Secrecy Act, which extends to "all bank records of every citizen" in the interest of law enforcement, is extremely overbroad.[267] Alluding to the future problems of database-driven information markets, Douglas contended that the Act was just a pretense to create a massive government database for other impermissible

---

or organization for whom it was conducted; (3) a summary description of the nature of the transaction, the type, amount, and denomination of the currency involved and a description of any check involved in the transaction; (4) the type of identification presented; and (5) the identity of the reporting financial institution." *Id*. at 39 n.15. *See also* 12 U.S.C.A. § 1829b(a)-(b) (West 2000 & Supp. 2007); 31 C.F.R. §103.22(b) (2006) ("Each financial institution other than a casino shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000, except as otherwise provided in this section.").

261. For example, 12 U.S.C.A. § 1829b(a)(1)(A) and (a)(2) were both expanded after 9/11 to further extend the scope of the Bank Secrecy Act beyond crime to "such records [that] may also have a high degree of usefulness in the conduct of intelligence or counterintelligence activities, including analysis, to protect against domestic and international terrorism."

262. *Cal. Bankers Ass'n*, 416 U.S. at 68.

263. *Id.* at 80 (Douglas, J., dissenting).

264. *Id.* at 82 (Douglas, J., dissenting).

265. *Id.* at 84-85 (Douglas, J., dissenting).

266. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 85-86 (1974) (Douglas, J., dissenting).

267. *Id.* at 85 (Douglas, J., dissenting).

purposes.[268] Douglas argued that banking records fell within the protections of *Katz* because the private information conveyed was consistent with an individual's reasonable expectation of privacy.[269] He concluded that fourth amendment procedural protections must be preserved in the case of banking records.[270]

In his dissenting opinion, Justice Marshall echoed Justice Douglas's concerns that the Bank Secrecy Act was just

> the initial step in a process whereby the Government seeks to acquire the private financial papers of the millions of individuals, businesses, and organizations that maintain accounts in banks and use negotiable instruments such as checks to carry out the financial side of their day-by-day transactions. In my view, this attempt to acquire private papers constitutes a search and seizure under the Fourth Amendment.[271]

Marshall argued that the data are feeding an emerging government apparatus for mass surveillance on its citizens through their financial records. As a result, other liberties, such as the First Amendment's freedom of association, were at risk. For example, the government may access membership lists through mandatory financial records without the privacy safeguards of the Fourth Amendment.[272] Given post-9/11 amendments to the Act, the dissenting justices in *California Bankers Ass'n* properly warned of the government interest in this frictionless route to access, collect, and aggregate personal data.[273]

This maneuver around the Fourth Amendment became even easier with the Supreme Court's decision in *United States v. Miller*.[274] If any doubt remained as to the constitutionality of the Bank Secrecy Act, the *Miller* decision closed the door on any further scrutiny.[275] Not only did the majority aggressively assert that Miller had no fourth amendment rights in his banking records,[276] the Court also

268. *Id.* (Douglas, J., dissenting) ("These are all tied to one's social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.").

269. *Id.* at 88-89 (Douglas, J., dissenting).

270. *Id*. (Douglas, J., dissenting).

271. *Id.* at 94 (Marshall, J., dissenting).

272. *Id.* at 98 (Marshall, J., dissenting).

273. Since 9/11, Congress has found that banking records not only have a high degree of usefulness in criminal, tax, and regulatory investigations, but such records "also have a high degree of usefulness in the conduct of intelligence and counterintelligence activities, including analysis, to protect against domestic and international terrorism." 12 U.S.C.A. § 1829b(a)(1)(A), (a)(2) (West 2000 & Supp. 2007).

274. 425 U.S. 435 (1976).

275. *Id*. at 437, 440.

276. *See id*. at 442-43.

> [W]e perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their

concluded that any procedural safeguards defined by "existing legal process" did not require a warrant or court process, and that a subpoena was sufficient.[277] This weakening of judicial process and broad empowerment for the government's search and seizure of banking records was recently used to justify expansion of the Bank Secrecy Act for post-9/11 terrorism investigations. The direct search and seizure of international wire transfer information handled by SWIFT, a Belgium-based transaction services provider owned by the banking industry, illustrates the aggressive use of banking records in government investigations.[278]

E. Financial Data Paradise: SWIFT Network Access

Treasury's use of the SWIFT network to search for terrorism-related transactions under its Terrorist Finance Tracking Program ("TFTP") became the subject of controversy after a New York Times report on June 23, 2006.[279] Treasury relied on administrative subpoenas to compel SWIFT to give the Central Intelligence Agency ("CIA"), the FBI, and other agencies access to "tens of thousands" of financial transactions recorded by its database.[280] Implicit in most commentators' discussions about the tracking of financial transactions is

> employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings."
>
> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. United States v. White, 401 U.S. 745, 751-752 (1971). This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

See also Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (permitting the use of pen registers at the phone company to determine what numbers were dialed in a private home as not in violation of the Fourth Amendment).

277. *Miller,* 425 U.S. at 444-46.

278. *See* SWIFT, About SWIFT, http://www.swift.com/index.cfm?item_id=2333 (last visited Jan. 2, 2008) ("SWIFT is the industry-owned co-operative supplying secure, standardized messaging services and interface software to nearly 8,000 financial institutions in 206 countries and territories. SWIFT members include banks, broker-dealers and investment managers. The broader SWIFT community also encompasses corporations as well as market infrastructures in payments, securities, treasury and trade. Over the past ten years, SWIFT message prices have been reduced over 80%, and system availability approaches 5x9 reliability—99.999% of uptime.").

279. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1, *available at* http://www.nytimes.com/2006/06/23/washington/23intel.html (quoting Stuart Levy, the director of the TFTP program, that the Treasury Dept. had clear authority to issue broad subpoenas for the SWIFT banking records because "[p]eople do not have a privacy interest in their international wire transactions"). The N.Y. Times Public Editor has since rescinded his approval to publish the June 23, 2006 article, largely because of the legality of the SWIFT subpoenas under existing U.S. Law. Byron Calame, *Can 'Magazines' of The Times Subsidize News Coverage?*, N.Y. TIMES, Oct. 22, 2006, at 4, *available at* http://www.nytimes.com/2006/10/22/opinion/22pubed.html.

280. Lichtblau & Risen, *supra* note 279.

that it seemed to be a good idea, but was it legal? [281] The better question is whether it is effective. Critics contend that "broad surveillance of money movements in an effort to find terrorists is expensive and ineffective" because false positives and data dilution overwhelm detection of rare events, such as terrorists moving money in the banking system.[282] This is especially true given the limited funding levels needed for terrorist activities;[283] however, an inquiry into effectiveness is not part of fourth amendment tradition. The Supreme Court's refusal to extend fourth amendment protections to banking records, especially *Miller*, is used to justify the legality of the TFTP. [284] The net result is that banking records seem clearly outside fourth amendment protections.

F. Recent Fourth Amendment Cases: A Comeback?

The Supreme Court recently revisited the *Katz* test for expectation of privacy and potentially laid the groundwork for more protection of privacy rights. In *Kyllo v. United States*, Justice Scalia defined the extent of privacy protection as the "degree of privacy against the government that existed when the Fourth Amendment was adopted."[285] Scalia asserted strong, impenetrable protection for the home.[286] He also expressed some foresight that any holding in this case needed to apply to future technological advances.[287]

The introduction of a new factor, the public use test, to determine if the search is unreasonable—whether the technology used in the search is within general public use—is consistent with the *Katz* expectation of privacy test.[288] For example, if the public is aware of the technology, then notice is presumptively present, and there would likely be no subjective or objective expectation of privacy. This conclusion conflicts with Warren and Brandeis's view of a right to privacy that exists regardless of the technology used to invade an individual's zone of privacy.[289] Scalia's attempt to recast fourth amendment jurisprudence to the Founders' perspective seems as vulnerable as prior doctrines in terms of the

281. *See e.g.*, National Commission on Terrorist Attacks upon the United States, Monograph on Terrorist Financing, http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf (last visited Jan. 2, 2008).

282. SCHNEIER, *supra* note 16, at 248.

283. *See id*.

284. *See* United States Department of Treasury, Legal Authorities Underlying the Terrorist Finance Tracking Program, http://www.ustreas.gov/press/releases/reports/legalauthoritiesoftftp.pdf (last visited Jan. 2, 2008).

285. Kyllo v. United States, 533 U.S. 27, 34 (2001). The Court also held that actual visual surveillance by a passing law enforcement officer remains outside the Fourth Amendment protections because the *Katz* test is not satisfied. *Id*. at 32-34.

286. *Id.* at 37 ("In the home, our cases show, all details are intimate details, because the entire area is held safe from prying Government eyes.").

287. *Id*. at 36.

288. *Id.* at 40.

289. *See* Warren & Brandeis, *supra* note 130, at 195 (finding that a right should be recognized in light of "recent inventions and business methods").

long-term viability of his test and the depth of protection afforded to individuals outside the sanctity of one's home.[290]

Although the home still accrues many fourth amendment protections, the person does not, whether applied to data records, "papers," or personhood itself.[291] Personal identity is important to an individual's data privacy, especially in situations of compelled police investigations. The Supreme Court in *Hiibel v. Sixth Judicial Dist*. devalued an individual's interest in personal identity when it upheld the right of a state to require the disclosure of the individual's identity during a *Terry* stop.[292] In his dissenting opinion, Justice Stevens related the danger of this new power to the encroaching database-driven information markets when he warned that

> [a] name can provide the key to a broad array of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases. And that information, in turn, can be tremendously useful in a criminal prosecution. It is therefore quite wrong to suggest that a person's identity provides a link in the chain to incriminating evidence "only in unusual circumstances."[293]

Law enforcement now had broad powers to match any individual to the vast universe of information based only on reasonable suspicion.

The Court's approach to the Fourth Amendment has interpreted out the most important protections offered by the Amendment. For these reasons, Congress has tried, perhaps imperfectly, to restore these rights. But because Congress has been reactive instead of proactive to the Court's unfavorable interpretations of the Fourth Amendment, it has likewise been context bound, and its protections constrained by the facts of each concern. An omnibus approach to data privacy would mitigate piecemeal results and address gaps left by Congress's statutory efforts.

---

290. One of these loopholes remains the context in which the right to privacy is asserted. The Supreme Court appears still rooted in the literal language and historical analogies presented by the Fourth Amendment's reference to "persons, houses, papers, and effects." In two cases decided prior to *Kyllo*, the Supreme Court made context-based decisions concerning garbage bags (no protected privacy interest) and bus luggage (protected privacy interest). *See* California v. Greenwood, 486 U.S. 35, 39-40 (1988) (holding that a subjective expectation of privacy in garbage bags placed at the curb for pick-up is objectively unreasonable even when shredded); Bond v. United States, 529 U.S. 334, 338-39 (2000) (concluding that there exists both subjective and objective reasonable expectations that overhead luggage would be protected from physical intrusion).

291. *See generally* State v. Raines, 857 A.2d 19 (Md. 2004) (holding that DNA collection law is constitutional and that defendant is compelled under the law to surrender his DNA for a state database).

292. Hiibel v. Sixth Judicial Dist., 542 U.S. 177, 185-86 (2004).

293. *Id.* at 196. In another personhood case under the Fourth Amendment, the Court permitted mandatory drug testing because such tests were in the public interest, even though school officials did not have reasonable suspicions of drug use among the population tests. The Court wrote out of the Fourth Amendment its probable cause protections due to context; here, a public school administrative action outside of criminal proceedings. *See* Bd. of Educ. v. Earls, 536 U.S. 822, 828-29 (2002).

G. Congressional Response to Fourth Amendment Limitations

Following the Court's instruction to seek relief from fourth amendment-based claims through legislative action, Congress responded by enacting numerous statutes that addressed specific concerns arising out of judicial decisions. These statutory efforts reflect varying industry interests without careful adherence to a common basis for privacy protection. Congress has hinted at an omnibus approach, but most legislation addresses narrow privacy issues related to certain activities or industries. Critics of these Acts raise issues concerning scope, applicability to post-9/11 circumstances, or effectiveness in achieving their stated purposes.[294]

Together, these statutory efforts demonstrate Congress's awareness that data reporting is subject to vulnerabilities, improper use, and law enforcement overreach; however, disclosures serve an important role in the U.S. economy. Congress must balance individual data privacy interests with the needs of business and government service providers to meet individual needs in an efficient manner. The "tug and pull" between these interests has produced imperfect legislation that addresses individual data privacy interests by topic or industry without consistent overall guidance for government, industry, and individuals. A comprehensive privacy statute would consistently address individual privacy interests across the broad spectrum currently covered by piecemeal legislative efforts. This section provides a brief overview of key statutes that implicate privacy interests to illustrate the wide variety of uncoordinated privacy-based laws at the federal level and the resulting need for an effective omnibus approach.

1. *Omnibus Standard Efforts*

A standard for data privacy protections is outlined in the Fair Information Practices standard established by the Department of Housing, Education, and Welfare in 1973.[295] The standard emerged amid growing concern that

> an individual's control over the personal information that he gives to an organization or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused.[296]

Fair Information Practices require: (1) transparency (elimination of secrecy in personal data systems); (2) right of access; (3) specificity of purpose; (4) consent; (5) right to correct or amend personal data; and (6) an affirmative duty upon the database purveyor to assure reliability and to take reasonable

294. *See generally* Electronic Privacy Information Center, http://epic.org/ (last visited Jan. 2, 2008); American Civil Liberties Union, http://www.aclu.org/ (last visited Jan. 2, 2008); Cato Institute, Privacy Issues, http://www.cato.org/infopolicy/privacy.html (last visited Jan. 2, 2008).

295. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 3, at 145.

296. *Id*.

precautions to protect the data from misuse.[297] This affirmative duty is enforced by a private right of action and a damages provision.[298] A harmonized approach based on a standard such as the Fair Information Practices would enable more consistent policymaking among the numerous laws protecting dealing with individual privacy interests.[299]

An early statute, the Privacy Act of 1974, suggested an omnibus approach to data privacy, although it was limited to federal agencies.[300] The purpose of the Privacy Act was to "safeguard individual privacy from misuse of federal records" and to regulate data sharing among federal agencies.[301] The conditions of disclosure optimistically set forth that "no agency shall disclose any record which is contained in a system of records by any communication to any person, or to another agency."[302] Numerous exceptions, however, permitted data sharing, including upon written request and when intended for routine use.[303] Although the intent behind the Privacy Act was to safeguard data privacy, the exceptions in the Act permitted straightforward data sharing among federal agencies.[304]

2. *Non-Financial Individual Privacy Interests*

Concerned with management of advancing surveillance technologies, Congress passed the Foreign Intelligence Surveillance Act,[305] the Electronic Communications Privacy Act,[306] the Computer Matching and Privacy Protection Act,[307] and the USA Patriot Act.[308] The nexus between information data privacy

297. *Id.*

298. Privacy Act of 1974, 5 U.S.C. § 552a (2000). *See also* Conboy v. AT&T, 241 F.3d 242, 246 (2d Cir. 2001) (dismissing plaintiff's case for lack of standing because transfers of personal data alone did not give right to injury or cognizable damages).

299. Over thirty statutes at the federal level and over 100 statutes at the state level deal with data privacy. Managing the Digital Enterprise—Professor Michael Rappa, http://digitalenterprise.org/privacy/privacy.html (last visited Jan. 2, 2008). Several state constitutions contain an affirmative right to privacy. *See generally* National Conference of State Legislatures, Privacy Protections in State Constitutions, http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (last visited Jan. 2, 2008). State laws are not within the scope of this analysis; however, several were implicated in the fourth amendment analysis herein and would be preempted by the federal U.S. data privacy statute recommended in Part V.

300. 5 U.S.C. § 552a (reflecting many of the principles of the Fair Information Practices standard).

301. Pub. L. No. 93-579, 88 Stat. 1896 (1974).

302. 5 U.S.C. §552a(b).

303. *Id*.

304. *Id*.

305. 50 U.S.C. §§ 1801-1811 (2000) amended by the Protect America Act of 2007, P.L. No. 110-55, 121 Stat. 552 (regulating certain electronic surveillance activities by private and governmental actors).

306. *See* Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (2000) (describing lawful and unlawful interception practices of wire or electronic communications); Stored Communications Act, 18 U.S.C. §§ 2701-2709 (2000) (protecting disclosure of stored electronic communications and records).

307. 5 U.S.C. § 552a (2000) (stating that the purpose of the Act is "to ensure privacy, integrity, and verification of data disclosed for computer matching …").

and advancing technology has received significant scrutiny in the post-9/11 period. Congress continues to rewrite legislation concerning surveillance, and in turn, courts will assess the legality of these efforts.[309] All such legislative efforts are subject to criticism as Security Theater and an eroding of individual privacy interests.[310]

In an example of legislating individual data privacy protections in certain industries, Congress put in place protections concerning entertainment choice when it passed the Cable Communications Privacy Act[311] and the Video Privacy Protection Act.[312] The Cable Communications Privacy Act protects consumer information by requiring cable operators to inform subscribers of individual information collection practices and to require consent prior to disclosure of "personally identifiable information."[313] In the same spirit, the Video Privacy Protection Act extends these protections to the video rental market.[314] Both Acts provide the aggrieved individual suffering from wrongful disclosure actual or liquidated damages, access to punitive damages, and attorney's fees.[315]

Congress also protects individual data privacy concerns in traditionally private matters, such as health and family, in the Family Educational Rights and Privacy Act ("FERPA")[316] and the Health Insurance Portability and Accountability Act ("HIPPA").[317] FERPA protects student privacy by influencing privacy policies at educational institutions through specific guidance and under the threat of loss of funding if found noncompliant.[318] Individual health care information held by health care providers is similarly protected from disclosure under rules set forth by Congress.[319]

308. USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (amending various sections of the U.S.C.) ("An Act [t]o extend and modify authorities needed to combat terrorism, and for other purposes.").

309. *See, e.g.,* Protect America Act of 2007, P.L. No. 110-55, 121 Stat. 552 (2007) (amending the Foreign Intelligence Surveillance Act (FISA), 18 U.S.C. §§ 1801-1811).

310. *See* Darren McCullagh & Anne Broache, *FAQ: How Far Does the New Wiretap Law Go?*, CNET NEWS.COM, Aug. 6, 2007, http://news.com.com/FAQ+How+far+does+the+new+wiretap+law+go/2100-1029_3-6201032.html; Posting by Marjorie Cohn, FISA Revised: A Blank Check for Domestic Spying, to Huffington Post, http://www.huffingtonpost.com/marjorie-cohn/fisa-revised-a-blank-che_b_59884.html (Aug. 9, 2007 11:06PM EST).

311. 47 U.S.C. § 551 (2000).

312. 18 U.S.C. §§ 2710-2711 (2000). Enacted following the disclosure of Judge Bork's video rental records during his confirmation hearings. *See* EPIC Video Privacy Protection Page, http://www.epic.org/privacy/vppa/ (last visited Jan. 2, 2008).

313. 47 U.S.C. § 551 (2000).

314. 18 U.S.C. §§ 2710-2711 (2000).

315. *See* 47 U.S.C. § 551 (2000), 18 U.S.C. §§ 2710-2711 (2000).

316. 20 U.S.C. §§ 1221, 1232g (2000) (tying funding to privacy practices of educational institutions and governs unauthorized disclosures of "personally identifiable information" in education records).

317. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in multiple sections of the U.S.C.) (regulating disclosures of protected health information).

318. 20 U.S.C. §§ 1221, 1232g (2000).

319. P.L. No. 104-191, 110 Stat. 1936 (1996) (codified in multiple sections of the U.S.C.).

In one well-meaning piece of legislation, the Personal Responsibility and Work Opportunity Reconciliation Act,[320] Congress created State Directories of New Hires and a National Directory of New Hires. These directories require employers to report to their states, which then report to the federal government, new hire information on *all* new employees, including social security numbers, for the very narrow purpose of tracking deadbeat parents avoiding child support payments.[321]

In response to public outrage over state sales of motor vehicle records, Congress passed the Driver's Privacy Protection Act.[322] This Act protects personal and highly restricted personal information[323] (defined as photo or image, social security number, medical, or disability information) by state agencies to third parties or for purposes unrelated to the permissible uses defined in the Act.[324] The Act requires express consent of the individual prior to certain disclosures.[325] Further, violations may be redressed through a civil suit permitting actual or liquidated damages, punitive damages (willful or reckless standard), and attorney's fees.[326] The federal government may also fine states up to $5,000 per day for substantial noncompliance.[327]

Recognizing an increase in crimes relating to misappropriation of individual data and other inappropriate breaches of data privacy, Congress introduced new criminal statutes to address these crimes: the Identity Theft and Assumption Deterrence Act[328] and the Children's Online Privacy Protection Act.[329] The Identity Theft Act protects against the knowing possession, transfer, trafficking, possession, creation, and use of certain government identification documents, but does not protect against credit card or other credit fraud typical of identify theft crimes.[330] The Children's Online Privacy Protection Act prevents website and online service providers targeting children from collecting personal information

320. Personal Responsibility and Work Opportunity Reconciliation Act, Pt. D. Child Support and Establishment of Paternity, Pub. L. No. 104-193, 110 Stat. 2105 (1996) (codified as 42 U.S.C. § 652 (2000)).

321. FPLS Brochure—National Directory of New Hires, http://www.acf.hhs.gov/programs/cse/newhire/library/brochures/fpls/ndnh.htm (last visited Jan. 2, 2008) (making special note of the importance of the social security number as a cross-referencing and search tool in database matching efforts). *See also* Lee Tien, *supra* note 28, at 389.

322. 18 U.S.C. §§ 2721-2725 (2000). *See also* Reno v. Condon, 528 U.S. 141, 143 (2000) (holding that the Driver's Privacy Protection Act is constitutional); Kehoe v. Fidelity Bank & Trust, 421 F.3d 1209, 1210-11 (11th Cir. 2005) (regarding a dispute about a bank purchase of Florida motor vehicle records for junk mail solicitation).

323. 18 U.S.C. § 2725 (2000).

324. 18 U.S.C. §§ 2721-2725 (2000).

325. *Id*.

326. 18 U.S.C. § 2724 (2000).

327. 18 U.S.C. § 2723 (2000).

328. 18 U.S.C. § 1028 (2000). The use of criminal statutes to address identity theft has limited impact on the problems in database-driven information markets, which engage in massive data collection without appropriate security protocols as evidenced by the numerous identity theft breaches over the past several years.

329. 15 U.S.C. §§ 6501-6506 (2000).

330. 18 U.S.C. § 1028 (2000).

from children.[331] This Act promotes industry self-regulation, limited oversight by the Federal Trade Commission, and fewer remedies to aggrieved individuals than previously discussed privacy acts.[332]

3. *Financial Individual Privacy Interests*

In response to *California Bankers* and *Miller*, Congress enacted the Right to Financial Privacy Act.[333] The purpose of the Act is to preserve confidentiality of financial records and limit government access to such records except under certain circumstances, such as a search warrant or judicial subpoena.[334] The Supreme Court, however, unanimously interpreted the Act in law enforcement's favor, although its ruling could have "the effect in practice of preventing some persons under investigation … from asserting objections to subpoenas issued … to third parties for improper reasons."[335]

In response to calls for proactive privacy policy notification to customers, Congress passed the Gramm-Leach-Bliley Act.[336] This Act requires financial institutions to send annual privacy notices to customers with instructions for "opt-out" procedures in order to limit disclosure of nonpublic personal information with affiliated and nonaffiliated third parties.[337] The Act does not preempt state laws that offer greater consumer protections.[338] Although some commentators have criticized the Act, others see merits in its approach to privacy legislation.[339]

4. *Conclusion*

The numerous legislative activities that impact individual data privacy infrequently refer to common principles as set forth in the Fair Information Practices standard. References to the Privacy Act are often limited to how to avoid its application upon new agency data mining efforts, especially in national security initiatives.[340] The problem with this patchwork quilt of statutes and regulations is the difficulty for all parties—individuals, government, and industry—to understand and behave in a manner consistent with legal requirements. The financial industry best illustrates the confluence of privacy

331. 15 U.S.C. § 6502 (2000).
332. 15 U.S.C. §§ 6504-06 (2000).
333. 12 U.S.C. §§ 3401-3422 (2000).
334. *Id.*
335. SEC v. O'Brien, 467 U.S. 735, 751 (1984).
336. 15 U.S.C. §§ 6801-6809 (2000).
337. *Id.*
338. 15 U.S.C. § 6807 (2000).
339. *See generally* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263 (2002).
340. *See* Electronic Privacy Information Center, Spotlight on Surveillance, *Customs and Border Protection's Automated System Targets U.S. Citizens*, Oct. 2006, http://www.epic.org/privacy/surveillance/spotlight/1006/.

legislation, national security interests, database-driven information markets, and risks to individuals of data theft and misuse.

V. FINANCIAL SERVICES: NEXUS OF INDIVIDUAL DATA PRIVACY CONCERNS

The financial services industry provides a useful case study on how industry data aggregation practices, individual privacy concerns, regulations, and inadequate legal protections confront consumers. Data reporting is critical to efficient credit markets; however, the regulatory environment often fails to ensure accurate and responsive industry performance. Several cases brought against credit reporting agencies or entities reporting to such agencies suggest that without greater individual data privacy rights, judicial remedies remain reserved for only the most egregious cases.

A. Financial Services as a Personal Data Reporting Industry

Financial services regulation remains at the nexus of individual data privacy rights and the power of the database-driven information markets. Data accumulated by the primary credit reporting agencies, TransUnion, Experian, and Equifax, are used in aggregated databases accumulated and re-sold by data brokers for purposes beyond credit, such as employment and insurance. Together, these firms keep records on approximately 200 million Americans.[341] There are good reasons for supporting a third-party credit reporting capability, namely, ease of information access to credit providers, faster processing, larger and more flexible credit markets, and reliable means to address misrepresentation concerns.[342] Congress recognized the importance of balancing individual data privacy interests with consumer credit provider interests. The Fair Credit Reporting Act ("FCRA"),[343] amended by the Fair and Accurate Credit Transactions Act of 2003,[344] regulates the procedures used by credit reporting agencies and attempts to satisfy both commercial and consumer interests through fair and equitable processing of personal data relevant to credit reporting.[345]

A primary purpose of the FCRA is to protect consumers from inaccurate information in their credit reports.[346] Unfortunately, individuals have found it very difficult to enforce these protections because of inherent weaknesses in the legislation. For example, not all data inaccuracies stem solely from credit reporting agencies, but rather originate with the reporters of the consumer data.

341. Gary M. Victor, *Identity Theft, Its Environment and Proposals for Change*, 18 LOY. CONSUMER L. REV. 273, 288 (2006); Consumer Data Indus. Ass'n—About CDIA, http://www.cdiaonline.com/about.cfm (last visited Jan. 20, 2008). *See also* SOLOVE, *supra* note 7, at 21 n.49.

342. FRED H. CATE ET AL., FINANCIAL PRIVACY, CONSUMER PROSPERITY, AND THE PUBLIC GOOD, AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES 8, 11-20 (2003). For more discussion of the misrepresentation problem, see generally Posner, *supra* note 186, at 395.

343. 15 U.S.C. §§ 1681-1681x. (2000).

344. Pub. L. No. 108-159, Stat. 1952 (2003) (amending sections 15, 20, and 31 of the U.S.C.).

345. 15 U.S.C. §§ 1681-1681x.

346. *See* Guimond v. Trans Union Credit Info. Co., 45 F.3d 1329, 1333 (9th Cir. 1995).

Entities that report to the credit reporting agencies receive much less scrutiny under the Act.[347] These barriers to effective redress result in significant costs to the individual. Given the rapidly growing database-driven information markets, these costs may grow exponentially because of widespread data sharing of consumer credit records. Credit reporting agencies regularly trade data throughout the private sector and with the government. Growing reliance on credit reports as sources of personal information makes the integrity and accuracy of these reporting services a priority. Unfortunately, numerous cases of data inaccuracies, misuse, unnecessary and excessive consumer costs, and credit reporting agency unresponsiveness suggest an urgent need for improved consumer protections.

B. Industry and Legal Responses to Cases of Data Misuse and Inaccuracies

Data misuse sometimes results from domestic disputes and unlawful access to credit data reports to gain leverage in such disputes. Credit reports are not sufficiently protected from coercive and destructive behaviors. As demonstrated in *Phillips v. Grendahl*, if data are readily available to a prospective mother-in-law unhappy with her daughter's choice,[348] then potential abuse by political opponents, a spiteful coworker, or the government is certainly possible. In the case of *Smith v. Sears, Roebuck & Co.*, a woman accessed her ex-husband's credit report fourteen times through a system called First Pursuit, a system made available to her by her employer, Sears.[349] Although the Mississippi district court concluded that her purpose of investigating her ex-husband to collect child support payments was improper and violated the FCRA, her employer was not held vicariously liable under state agency law.[350] While other courts held that employers were liable for the improper use of credit reporting information by their employees, the Mississippi court distinguished those cases and expressed reluctance to hold Sears liable for activities clearly outside the scope of employment.[351]

Another line of cases under the FCRA illustrate the high personal costs incurred by individuals who suffer from inaccurate data in their credit reports.

347. *See, e.g.,* Lewis v. Ohio Prof'l Elec. Network LLC, 248 F. Supp. 2d 693, 696 (S.D. Ohio 2003). This case deals with a data entry error by a clerk at the Stark County Sheriff's Department who entered the last four digits of an arrested felon's phone number as the last four digits of the plaintiff's social security number, thereby linking the felon's criminal record to plaintiff. *Id*. at 695. This information was then republished by a sheriff's association through two data brokers that sell data to private sector users. *Id*. at 696.

348. 312 F.3d 357, 360-61 (8th Cir. 2002). Prospective mother-in-law hired private investigator to investigate daughter's fiancé, including a report that contained consumer credit information, allegedly in violation of the FCRA as an improper use of consumer information. *Id.*

349. Smith v. Sears, Roebuck & Co., 276 F. Supp. 2d 603, 604-05 (S.D. Miss. 2003). Plaintiff was able to detect improper use of his credit report because the credit report inquiries of his ex-wife were reported on his credit report. *Id.*

350. *Id.* at 609-14. The district court supported its decision not to enforce vicarious liability against Sears because the FCRA does not include an affirmative duty "to employ adequate and necessary procedures to prevent FCRA violations by its employees." *Id*. at 611.

351. *Id*.

These costs are high because many common transactions rely upon credit reports, including mortgages, college loans, and insurance. Credit reporting errors tarnish the credit report for years and require significant individual resources to correct because resolution is cumbersome and often elusive. In *Carlson v. Trans Union, L.L.C.*, plaintiff was denied credit and mortgage applications for more than a year and subjected to collection agency activities because of an inaccurate credit report.[352] The error resulted from plaintiff's former employer leaving an outstanding debt with Verizon, which Verizon erroneously assumed was guaranteed by the plaintiff.[353] Plaintiff never held an account with Verizon.[354] Although he tried to settle his case with Verizon and TransUnion before bringing suit under the FCRA, matters remained unresolved. Plaintiff then sued, adding state-based claims for defamation and negligence.

Plaintiff's negligence claim was dismissed because of the federal preemption section in the amended FCRA.[355] The FCRA federal preemption provision overrides state laws and requires the plaintiff to prove that the inaccurate information reported to the credit agencies was "furnished with malice or willful intent to injure such consumer,"[356] even if only negligence is required for state-based claims. The federal preemption provision protects furnishers of credit information and credit reporting agencies by limiting legal liabilities and lowering performance standards, but leaves individuals with enormous personal costs and few legal tools to reallocate these costs back to the source of the problem.[357] By requiring "malice and intent to injure" for FCRA claims, most consumers have no remedy for mishandling or erroneous data reporting under the FCRA.[358]

Although it is possible that plaintiffs can prove "malice or willful intent," and receive punitive damages against furnishers of credit information and credit reporting agencies, it comes at great personal costs. In *Evantash v. G.E. Capital*

352. Carlson v. Trans Union, L.L.C., 259 F. Supp. 2d 517, 518-19 (N.D. Tex. 2003). *See also* Fashakin v. Nextel Commc'ns, No. 05 CV 3080, 2006 U.S. Dist. LEXIS 45807, at *1-5 (E.D.N.Y. June 28, 2006). A similar fact pattern also involving TransUnion and defendant's alleged unresponsiveness to a consumer's contention of erroneous data reporting. *Id.*

353. *Carlson,* 259 F. Supp. 2d at 518.

354. *Id*.

355. *Id.* at 520, 522 (referring to federal preemption provision 15 U.S.C. §1681h(e) (2000)). This provision prohibits consumers from bringing actions against credit reporting agencies, their customers, or the furnishers of data for defamation, invasion or privacy, or negligence. *Id.* The only cause of action permitted under this Act is for "false information furnished with malice or willful intent to injure such customer." *Id*. Plaintiff's defamation claim was limited by the Texas statute of limitations, but was permitted to go forward. *Carlson,* 259 F. Supp. 2d at 522.

356. *Id.* at 520.

357. *See, e.g.*, Lawrence v. Trans Union L.L.C., 296 F. Supp. 2d 582, 585-86 (E.D. Pa. 2003). In this case, TransUnion reported bad data received from a subcontractor that plaintiff had an outstanding judgment against her for five years. *Id.* Plaintiff actually received a judgment in her favor and had an excellent credit rating prior to the error. *Id.* Thereafter, she suffered many reverses in her credit opportunities and had to pay higher annual percentage rates than would have been the case without the error. *Id.* Plaintiff's allegations suggest that TransUnion only "parroted" the subcontractor instead of making a reinvestigation for itself. *Id*. at 589.

358. 15 U.S.C. §1681h(e).

Mortgage and Trans Union, plaintiff sued defendants under the FCRA after repeated yet futile attempts to correct an erroneous report that she was bankrupt.[359] Although plaintiff succeeded in getting G.E. Capital Mortgage to instruct TransUnion to correct her report, an automated tape from G.E. Capital Mortgage to TransUnion erroneously repopulated the misleading data.[360] Thereafter, plaintiff made at least four more attempts to have TransUnion correct the misleading data through instructions by G.E. Mortgage.[361] In the meantime, plaintiff's incorrect credit report circulated among her existing creditors, the annual percentage rates on her credit cards were increased, and Fleet reduced her credit limit.[362]

In rejecting defendants' summary judgment motion, the district court relied on the policy behind the FCRA to hold that a reasonable jury could find that the defendants acted with conscious disregard to the degree eligible for punitive damages.[363] The policy of ensuring accurate data reporting through reasonable procedures and reinvestigations to ensure "fairness, impartiality, and respect for consumer's right to privacy"[364] was not fulfilled by the repeated, low-effort exchanges between the defendants, which constituted solely of "short, electronic messages."[365] Despite plaintiff's vigilance for correction, the level of carelessness in the defendants' exchanges demonstrated the inadequacy of FCRA safeguards in credit reporting activities.

Data inaccuracies not only threaten the financial well-being of consumers, but also impact "the nation's economy as a whole."[366] Cases based on data inaccuracies resulting from identity theft are particularly vulnerable to dismissal under the FCRA.[367] As these FCRA cases illustrate, the legal remedies available in existing legislation do not protect individuals from either privacy invasions or harm caused by inaccurate data reporting. Increased utilization of credit reporting agency data throughout the economy and government investigations deepens the impact on individuals who suffer from these errors and face statutory limitations in enforcing their legal interests.

359. Evantash v. G.E. Capital Mortgage Servs., Inc., No. 02-CV-1188, 2003 U.S. Dist. LEXIS 23131, at *2 (E.D. Pa. Nov. 25, 2003).

360. *Id.* at *4.

361. *Id.* at *4-6.

362. *Id.* at *5.

363. *Id.* at *26-27.

364. *Id.* at *9 (quoting 15 U.S.C. § 1681(a)(4) (2000)).

365. *Id.* at *9-10, 22.

366. *Id.* at *10 (quoting Philbin v. Trans Union Corp., 101 F.3d 957, 962 (3d Cir. 1996)).

367. *See, e.g.*, Jarrett v. Bank of Am., 421 F. Supp. 2d 1350, 1351-52, 1355 (D. Kan. 2006) (granting defendants' partial motions to dismiss because of federal preemption of state claims, including plaintiff's claim for injunctive relief).

VI. THE EU DATA PRIVACY DIRECTIVE: A USEFUL MODEL FOR A U.S. DATA PRIVACY STATUTORY FRAMEWORK

The EU Data Directive provides a valuable framework for addressing privacy rights and concerns in database-driven information markets.[368] The EU Data Directive was enacted in October 1995 with EU Member State compliance required by October 1998.[369] The purpose of the EU Data Directive is equivalence and harmonization of data protection laws across the EU Member States.[370] This approach is in direct contrast with the U.S., which has taken a more industry-based approach, relying on legislation, regulation, and self-regulation by corporate and governmental entities with solutions that vary widely by industry and application.[371] The benefits to the U.S. of adopting the EU harmonization approach are: (1) improved database-driven information markets through clearly defined guidelines to data privacy; (2) effective leverage of individual data subjects to address database accuracy; and (3) enhanced individual awareness of privacy interests and expectations. The EU Data Directive harmonization approach addresses imperfections in database-driven information markets and is a useful model for improving U.S. database-driven information markets.

A. Opportunities in Modeling the EU Data Directive

The EU Data Directive provides workable definitions for database-driven activities and secures an affirmative right to privacy for individuals in database-driven information markets.[372] By setting cross-industry and cross-Member State standards for data processing activities, the EU Data Directive corrects imbalances between sectors of economic activity with weak protections on personal data and sectors providing stricter data privacy regulations.[373] The EU

368. Council Directive 95/46/EC, 1995 O.J. (L281), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter Council Directive].

369. *Id*. art. 32(1).

370. *Id.* ¶ 12. *See* Paul M. Schwartz, *The EU Directive, the Safe Harbor and Other International Privacy Issues*, *in* SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD, at 621, 623 (PLI Patents, Copyrights, Trademarks & Literary Prop., Course Handbook Series No. 8966, 2006).

371. *See* U.S. Dept. of Commerce, Safe Harbor, Safe Harbor Overview, http://www.export.gov/safeHarbor/sh_overview.html [hereinafter Safe Harbor] (last visited Jan. 2, 2008).

372. Council Directive, *supra* note 368, ¶¶ (1)-(2).

373. *Cf. id*. art. 8. The Directive encourages Member-State conformance in data privacy protection of personal data, but allows Member-States to implement sector-specific special processing conditions for "Special Categories of Processing" as defined in Art. 8. *See also* DOUWE KORFF, FINAL REPORT: THE FEASIBILITY OF A SEAMLESS SYSTEM OF DATA PROTECTION RULES FOR THE EUROPEAN UNION 15 (1999) (finding that "the most fundamental data protection principles and 'criteria' should apply 'ad omnibus,' to all processing operations in all sectors of society").

Data Directive facilitates a common data privacy platform across all industry sectors involved in EU-related commerce.[374]

The EU Data Directive offers a legal framework that clarifies the interaction between personal data processing and the rights of individual data subjects because the EU Data Directive targets database-driven information markets, and specifically the processing of personal data through structured and automatic means.[375] Under the EU Data Directive, data-processing activities are recognized as tools "to serve man" and are subordinated to the fundamental rights of man, including the right to privacy.[376] Pursuant to this approach, the EU Data Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject')," where "an identifiable person is one who can be identified, directly or indirectly, … by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[377]

The EU Data Directive describes data-processing broadly to include most database-driven information market activities as:

> any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[378]

A broad and consistently applied approach to regulating database-driven information markets prevents the gaps and loopholes present in U.S. privacy laws.

The EU Data Directive therefore regulates, but does not prohibit, database-driven information markets. Availability of personal data is realistically viewed as a natural byproduct of increased trade flows and technological advances in data-processing.[379] By acknowledging the free-flow of personal data and overlaying such flows with rules that improve data accuracy and ensure sensitivity to individual data privacy rights in data-processing, the EU Data

374. Council Directive, *supra* note 368, ¶ (3). *See* Julia M. Fromholz, *Data Privacy: The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 462 (2000) (adding that the Directive reduces transaction costs for European companies).

375. Council Directive, *supra* note 368, ¶ 15.

376. *Id*. ¶¶ 2, 10, art. 1(1). *See* The Treaty of the European Union, Maastricht Treaty, Title I, art. 5, *available at* http://www.worldwideschool.org/library/books/hst/european/TheTreatyoftheEuropeanUnion—TheMaastrichtTreaty/chap2.html ("The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law."). *See also* Council of Europe ETS no. 005, Convention for the Protection of Human Rights and Fundamental Freedoms, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (Article Eight—Right to Respect for Private and Family Life).

377. Council Directive, *supra* note 368, art. 2(a).

378. *Id*. art. 2(b).

379. *Id*. ¶¶ 3-9.

Directive facilitates database-driven information markets while balancing individual privacy rights in personal data with modest additional costs to industry and the government.[380] The EU Data Directive accomplishes this balance by establishing five basic rule categories: (1) data accuracy and quality; (2) legitimate data processing practices; (3) additional protection for sensitive personal data; (4) right to notice for data subjects; and (5) affirmative individual rights to access, to object, and to seek a judicial remedy for any breach of applicable Member State privacy laws.[381] The EU Data Directive further ensures that these rules are not circumvented through outsourcing or transmission to third-party countries that fail to ensure "an adequate level of protection."[382] This third-party transfer provision ensures global attention and conformance to the EU Data Directive guidelines.[383]

Rules on data quality and data processing offer specific performance standards to assist Member States in conforming laws and guide database-driven information providers in their daily operations.[384] These standards emphasize accuracy and narrowly tailored uses of personal data in collection, processing, and storage.[385] Data accuracy is particularly important as Article Six requires that personal data must be "accurate, and where necessary, kept up to date" and that incomplete or inaccurate data are "erased or rectified."[386] This accuracy requirement is furthered by the individual oversight rights conferred by the EU Data Directive.[387] Besides valuing the importance of accurate personal data, the EU Data Directive narrows collection and processing to "specified, explicit, and legitimate purposes."[388] Personal data collection in databases must be "adequate, relevant and not excessive" relative to both intended purposes and further processing.[389] Storage of personal data must not be stored beyond the time necessary to serve the purposes of the data collector or processor.[390] These standards enforce industry recognized best practices and maximize consumer protection because they apply to all market participants, closing loopholes created by non-compliant sectors.

Together, these provisions direct Member States to raise the bar on the performance of database-driven information markets by placing a burden of proof on market participants to demonstrate to regulators and individual data

380. *See* RAMBØLL MANAGEMENT, FINAL REPORT: ECONOMIC EVALUATION OF THE DATA PROTECTION DIRECTIVE 95/46/EC 5 (May 2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf (concluding that among companies surveyed that the implementation costs are limited and not a significant burden).

381. *Id. See also* Schwartz, *supra* note 370, at 623.

382. Council Directive, *supra* note 368, art. 25(1).

383. *See, e.g.*, Safe Harbor, *supra* note 371.

384. Council Directive, *supra* note 368, art. 6, 7.

385. *Id.* art. 6(1).

386. *Id*. art. 6(1)(d).

387. *Id.* art. 12 (providing, in part, an individual data subject the right to rectify, erase or block data in the event that such data are incomplete or inaccurate).

388. *Id*. art. 6(1)(b).

389. *Id*. art. 6(1)(c).

390. *Id.* art. 6(1)(e).

subjects that collected personal data are accurate, necessary, and related to a legitimate purpose.[391] In significant contrast with U.S. practices, the EU Data Directive requires market participants to solicit and receive consent from the individual data subject, unless the processing is necessary to fulfill five narrow exceptions.[392] The EU Data Directive's consent and exception approach receives a higher level of scrutiny for special categories of data, which include "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[393] The data processing restrictions in the EU Data Directive require active data management in a manner closely aligned with a legitimate purpose.[394] The focus on end-use purpose improves market performance by limiting risks associated with imprecise data collection methods, ill-informed data aggregation, and out of context misinterpretations.[395]

B. Individual Rights under the EU Data Directive

Individual privacy rights pertain to any processing of personal data governed by Member States in compliance with the EU Data Directive.[396] This government-driven approach to data privacy protection is individual-centric as opposed to the U.S.'s industry-centric approach.[397] By centering privacy rights in individual data subjects, the EU Data Directive targets data collection practices and ensures processing oversight resources across all industry sectors and applications, thereby reinforcing accuracy, relevance, and legitimate purpose.[398] Through a centralized regulatory authority, the EU Data Directive further reinforces awareness and compliance by information market participants.[399]

391. *Id*. art. 6(1)(d).

392. *Id*. art. 7(a) ("Member States shall provide that personal data may be processed only if ... the data subject has *unambiguously* given his consent.") (emphasis added). *See also* Seagrumn Smith, *Microsoft and the European Union Face Off over Internet Privacy Concerns*, 2002 DUKE L. & TECH. REV. 0014, 2 (describing the EU Data Directive as an "opt-in" approach as characterized by the consent requirement in contrast to the typical U.S. "opt-out" presumption which presumes consent unless the individual data subject "opts-out" of the data collection or processing).

393. Council Directive, *supra* note 368, art. 8.

394. *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 166-67 (2001) ("[W]hen isolated bits of personal information are confused with genuine knowledge, they may create an inaccurate picture of the full range of our interests and complicated personalities.").

395. *Id*. at 205 (raising special concern that the ubiquity of computer databases contributes to the problem of misinterpretations due to "confusion of information with knowledge").

396. Council Directive, *supra* note 368, art. 1(1).

397. *See* Fromholz, *supra* note 374, at 471 ("Traditionally, Americans have been less likely than Europeans to turn to the government to regulate private enterprise, instead relying on the market or new technologies to address public concerns about commercial activity.").

398. Individual rights of notification, access, and objection might have prevented a data accuracy lapse "during the 2000 Presidential election [when] thousands of Florida voters were excluded from the polls because ChoicePoint, a private company working for the state, inaccurately identified those individuals as convicted felons who were ineligible to vote." Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 721 (2001).

399. Council Directive, *supra* note 368, art. 18.

Affirmative rights for individual data subjects ensure compliance with Member State data privacy laws. If a violation occurs, the Member State must provide a right to a judicial remedy, including a right to seek damages.[400] Individual data subjects are engaged under the EU Data Directive to monitor and actively participate in database-driven information markets through rights to notice, access, objection, and enforcement.[401] Both primary and third-party data collectors must notify individual data subjects of the identity of the collector, the purpose of the data collection, and other relevant information.[402] This notification requirement promotes transparency of the database-driven information markets and invites individual data subjects to ensure fair processing.[403] Once notified, the individual data subject uses an affirmative right to access the data and assess compliance with the Member States privacy laws pursuant to the EU Data Directive.[404] The individual may object on "compelling legitimate grounds relating to his particular situation to the processing" of her data "on request, and free of charge" to third-party disclosures, such as direct marketing uses.[405] In the event of any breach of the applicable Member State privacy laws, every individual is granted the right to a judicial remedy.[406]

Most importantly, individual data subjects become active participants in database-driven information markets by leveraging their personal knowledge to improve effectiveness with limited additional costs to industry.[407] Individual participation ensures that markets are collecting, processing, and sharing data in a manner that limits personal data to legitimate purposes and minimizes use of extraneous, inaccurate, and misleading data.[408] By bolstering individual privacy rights, the EU Data Directive provides individuals an incentive to understand the relationship between their disclosures and how such data are used in the market. Database-driven information markets would develop control mechanisms that more sensitively mirror the complex values that individuals hold with regard to the right to data privacy. Market imperfections, such as the criminal use of data and the extreme costs to individuals in correcting errors, would decrease through greater oversight of the use and handling of individual data. Bringing individual subjects into the information markets would improve data accuracy, force adoption of security best-practices, and encourage reasonable care when sharing personal data with third parties or third-party countries where data protections may be less developed. Perfecting information market-mechanisms through

400. *Id.* art. 22.

401. *Id*.

402. *Id*. arts. 10, 11.

403. *Id*.

404. *Id*. art. 12.

405. *Id*. art. 14.

406. *Id*. art. 22.

407. *See* ROSEN, *supra* note 394, at 230 (describing that knowledge must be earned by the slow, reciprocal sharing of personal information, but is short-circuited when private information is taken out of context). *But see* Cohen, *supra* note 181, at 1406-08 (criticizing the knowledge theory argument for data privacy protections as inherently flawed and better characterized as a Marxist-style struggle for power over knowledge).

408. *See* Council Directive, *supra* note 368, ¶¶ 25, 28.

greater transparency and accountability promotes quality in these markets and their usefulness in highly sensitive applications, such as national security efforts.

C. Individual Personal Data Privacy Rights under a U.S. Data Privacy Statute

Under a U.S. data privacy statute, individual rights over the use and handling of personal data would be protected through a private cause of action based upon the negligence standard, rather than the willful and wanton misconduct standard used in the FCRA. The statute would contain a minimum for liquidated damages per breach incident. Actual damages would not be required to bring an action under the statute. The statutory minimum addresses cases where although a theft occurred, the individual was not or not yet financially harmed by it. The statute would further permit recovery even if the harm is only fear and anxiety of future identity theft, loss of economic opportunity, or stress related to inaccurate reporting. A shift in liability would encourage formalized performance monitoring by providing economic incentives to prevent theft and misuse.[409] Legal remedies that enforce liabilities enhance security by mandating responsible data handling practices.[410] These remedies also promote integrity in the industry and increased reliance on its output for an expanded field of applications.

The statute would also remove any federal preemption provisions in existing privacy-related legislation to ensure that states can enact privacy laws consistent with their constitutions and legislative agendas. The promotion of federalism and recognized role of states as "laboratories of experimentation" spur progress of data privacy protections as demonstrated by California's leadership in this area.[411] A safe harbor provision, similar in spirit to the existing safe harbor agreement facilitating U.S. corporate compliance with the EU Data Directive, may be necessary if compliance requires either extended implementation time or flexibility in certain industry sectors. By focusing on liability reform, the U.S. data privacy statute and its state-based counterparts would perform an important role for industry in improving standards and practices.

D. Society's Choice for the Future

A compelling way for the U.S. to confront these challenges is to adopt a comprehensive data privacy law modeled after the EU Data Directive. Congress, privacy advocates, and industry appear to share a desire to clarify the rules of the playing field when it comes to balancing privacy interests with database-driven

409. SCHNEIER, *supra* note 16, at 268-69 (noting that the insurance industry drives security because insurance companies vary risk premiums based on levels of security).

410. *Id*. at 267 (suggesting that criminal penalties, perhaps more than civil penalties, would provide a strong economic incentive to companies to improve data management practices).

411. *See generally* California Office of Privacy Protection, http://www.privacy.ca.gov/ (last visited Jan. 2, 2008).

information markets.[412] Microsoft and other leading technology companies publicly advocate for a comprehensive federal privacy statute.[413] Even James Lee, the Chief Marketing Officer of ChoicePoint, acknowledges that society needs to make a judgment regarding use of information in society, including whether to create a better framework.[414]

Industry leaders such as Acxiom have used high-powered political leaders, including General Wesley Clark, a member of Acxiom's Board of Directors in 2001, to press their commercial interests in Washington.[415] After 9/11, data brokerage firms aggressively and opportunistically sought lucrative government contracts by peddling data mining solutions as effective national security solutions without concern for individual data privacy rights. The profit potential in large government contracts is enormous. With huge interests at stake, large data brokerage companies, credit companies, and other corporate and government stakeholders argue that legislation enforcing omnibus privacy protections like the EU Data Directive are unnecessary for primarily three reasons: (1) industry can effectively self-regulate and protect individual privacy interests; (2) the current industry serves important functions that benefit society; and (3) the freedom with which Americans surrender data suggests little public concern for privacy protections. Further, industry would likely threaten that EU style regulations would shut the industry down, eliminate jobs, and take value out of the economy.

Although like most new regulations, new burdens would be placed on the industry, many of these costs should have been part of a well-crafted business model from the start. Data accuracy and reliability is paramount to any sensitive application of data such as national security. Further, using and selling individual data without consent and accountability, and with almost no transparency, seems clandestine and suspect. Identity thieves leverage this lack of accountability throughout the chain of custody and thrive in database-driven information markets. Lax data management practices today may lead to significant economic costs that jeopardize our open economy tomorrow. Public consensus may coalesce for stricter privacy legislation and greater industry regulations as more Americans are impacted by false positives, inaccurate data reporting, and identity theft, with costs well beyond the occasional unwanted mailer, airport screening, or rejected mortgage application. The opportunity is

412. *Safeguarding* Part II*, supra* note 111 (featuring an interview with Robert O'Harrow, Jr., author of *No Place to Hide* (2006), and Senator Bill Nelson (D-FL)). *See also* Senator Hillary Clinton, Remarks at the American Constitution Society for Law and Policy National Convention (June 16, 2006), *available at* http://www.acslaw.org/node/2967.

413. Press Release, Microsoft, Microsoft Advocates Comprehensive Federal Privacy Legislation (Nov. 3, 2005), *available at* http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx.

414. *There Are Good Uses of Information, and Bad* (NPR Morning Edition broadcast Mar. 8, 2006), *available at* http://www.npr.org/templates/story/story.php?storyId=5250978.

415. O'HARROW, *supra* note 6, at 59-60 (2006); Press Release, Acxiom, General Wesley K. Clark Joins Acxiom Corporation Board of Directors (Dec. 6, 2001), *available at* http://www.acxiom.com/default.aspx?ID=1967&DisplayID=18.

now for the industry to take a proactive step in shaping this future debate by instituting best practices today.

The EU Data Directive should be considered when debating viable privacy frameworks because it provides workable definitions of database-driven activities and secures affirmative rights for an individual's right to privacy. The EU Data Directive shares several attributes with the Fair Information Practices template and thus relates to longstanding U.S. views on individual data privacy. A U.S. data privacy statute would provide omnibus protection for individuals by establishing baseline regulatory expectations for the federal government, states, corporations, and individuals. It would also address numerous weaknesses in existing federal and state data privacy laws. A U.S. data privacy statute would counteract weak Supreme Court interpretations of the Fourth Amendment and extend privacy protections to the private sector. Courts would benefit from a U.S. data privacy statute that sets forth statutory interpretation guidelines using a clearly expressed data protection framework no longer mired in out-dated theories of the right to privacy. This omnibus statutory approach would comprehensively regulate the vast database-driven information markets with efficiency, consistent guidance, and maximum coverage.

VII. CONCLUSION

The U.S. should adopt a properly adapted version of the EU Data Privacy Directive because increased utilization of database-driven information markets, including uses by the government, requires new legislation to improve the performance of these markets. This approach would address key imperfections, recognize an affirmative right to data privacy, and revive an expectation of privacy within individuals, an expectation now decimated by the actions of both the Supreme Court and Congress. The new privacy legislation could be further supported by a sensible interpretation of the Fourth Amendment that restores the Amendment's full breadth and relevancy to today's technologies and challenges. Since a revival of fourth amendment protections seems unlikely, a comprehensive U.S. data privacy statute is best positioned to restore individual privacy rights and bolster the long-term viability of database-driven information markets. The data brokerage industry, the government, and corporate interests would benefit from greater individual participation in database-driver information markets. Improved data accuracy, positive marketing gains driven by notice and consent requirements, and appropriate risk transfer back to industry to better deal with data theft and misuse, will together ensure viable and robust database-driven information markets for the future.