Saint Louis University Public Law Review

Volume 25
Number 1 *Strife, Liberty & the Pursuit of Privacy: The Conflict Between Freedom of Information and Privacy in the Post-9/11 ERA (Volume XXV, No. 1)*

Article 6

2006

Personal Information in Government Records: Protecting the Public Interest in Privacy

Grayson Barber

PERSONAL INFORMATION IN GOVERNMENT RECORDS: PROTECTING THE PUBLIC INTEREST IN PRIVACY

GRAYSON BARBER*

INTRODUCTION

Governmental agencies, including the courts, have a special obligation to protect the public's interest in individual privacy. Government records and court records are being harvested for personal information about individuals, contributing to a surge in identity theft, consumer profiling, and the development of a stratified society where individuals are pigeonholed according to the electronic trail they leave of transactions that disclose personal details about them. Personal information is valuable to commercial interests, but the state has no obligation to disclose data about its citizens. To the contrary, the government should protect individuals who disclose information about themselves to the state only because they are forced to do so.

All governments collect and use personal information in order to govern.[1] Government records include data that contain personal information about

* Grayson Barber, a First Amendment litigator and privacy advocate in Princeton, New Jersey, wishes to thank those whose insights and essential support have contributed to the work presented here: Peter D. Meyers, Frank Askin, Ed Barocas, Thomas J. Cafferty, Fred Cate, Frank Corrado, Chris Hoofnagle, Stuart Kaplan, William John Kearns, Jr., Helen Nissenbaum, Daniel Solove, Jay Stanley, and Barry Steinhardt.

1. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002) (giving an excellent analysis of government records and the perils of aggregating individual information).

> States maintain records spanning an individual's life from birth to death, including records of births, marriages, divorces, professional licenses, voting information, worker's compensation, personnel files (for public employees), property ownership, arrests, victims of crime, criminal and civil court proceedings, and scores of other [pieces of] information. . . .. These records contain personal information including a person's physical description (age, photograph, height, weight, eye color); race, nationality, and gender; family life (children, marital history, divorces, and even intimate details about one's marital relationship); residence, location, and contact information (address, telephone number, value and type of property owned, description of one's home); political activity (political party affiliation, contributions to political groups, frequency of voting); financial condition (bankruptcies, financial information, salary, debts); employment (place of employment, job position, salary, sick leave); criminal history (arrests, convictions, traffic citations); health and medical condition (doctors' reports,

individuals. Many of these records have long been open for public inspection for a number of reasons. Government offices, including the courts, must moderate their need to collect information with their obligations to be open to the people and simultaneously to protect the privacy of individuals.

Every individual in this country is compelled to disclose personal information to the government. One has no choice.[2] In order to receive government services, in order to do business with the government, and in order to be a law-abiding citizen, one must provide one's home address, telephone number (listed or unlisted), and much more to the government. The government, therefore, must protect the public interest by maintaining the privacy of personal information in government files.[3] No commercial entity is likely to do so, and individuals rarely have the power to protect their personal privacy from commercial pressures to treat personal data as a commodity.[4]

The core purpose of open government records statutes is to enhance public understanding of the operations and activities of government.[5]

> Official information that sheds light on a state agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but reveals little or nothing about an agency's own conduct.[6]

The government collects a great deal of information about its citizens that, if re-disclosed and assembled in a new mosaic, could be exploited to the detriment of individual privacy. States require their citizens to disclose data about their personal affairs, including Social Security numbers, medical information, financial information and home addresses.[7] The government may well have important reasons for collecting such information, but, as noted by the U.S. Supreme Court, "[t]he right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory

---

> psychiatrists' notes, drug prescriptions, diseases and other disorders); and identifying information (mother's maiden name, Social Security number). This list is far from complete.

Id. at 1139.

2. Basic family relationships, for example, such as marriage and divorce, involve obtaining licenses and decrees from the executive and judicial branches respectively. *Cf.* Loving v. Virginia, 388 U.S. 1, 12 (1967) (fundamental constitutional right to marry).

3. *See* Mainstream Mktg. Serv., Inc. v. F.T.C., 358 F.3d 1228, 1246 (10th Cir. 2004) (holding that the public interest in privacy, especially in the home, was sufficient to defeat a First Amendment challenge to the "Do-Not-Call" list).

4. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995).

5. U.S. Dep't. of Def. v. F.L.R.A., 510 U.S. 487, 495 (1994).

6. *Id.* at 495-96 (citations omitted).

7. Whalen v. Roe, 429 U.S. 589, 605 (1977).

duty to avoid unwarranted disclosures. . . . . In some circumstances that duty . . . has roots in the Constitution . . . ."[8]

The availability of personal information in government records is exploited for commercial and sometimes criminal purposes. Commercial data aggregators routinely mine government records to gather information about individuals.[9] This practice in turn has been exploited for fraudulent purposes. In February 2005, for example, the country's largest information broker, ChoicePoint, unwittingly sold personal information on at least 145,000 Americans to a criminal ring engaged in identity theft.[10] ChoicePoint sent letters to residents of California, notifying them of the wrongful disclosure of their personal information, but only because California had a state law on the books forcing ChoicePoint to take the action.[11] In response to a letter from thirty-eight state attorney generals, ChoicePoint sent out letters to other potential victims of identity theft across the country, but it did not disclose to the victims the data it disclosed to the thieves.[12] ChoicePoint obtains much of its data from government files.[13]

8. *Id.*

9. Stephanie Kirchgaessner, *Access Denied: The Data Industry May Face New Restriction after Privacy Breaches*, FINANCIAL TIMES (LONDON), May 20, 2005, at 17.

10. Evan Perez & Rich Brooks, *File Sharing: For Big Vendor of Personal Data, A Theft Lays Bare the Downside*, WALL ST. J., May 3, 2005, at A1. *See also* Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Sept. 21, 2005) (listing a chronology of data breaches, which demonstrates that many databases collect and store sensitive personal information with inadequate security, including banks, schools, retailers and government offices); Chris Jay Hoofnagle, *Data Security: The Discussion Draft of Data Protection Legislation*, Testimony & Stmt. for the Record before the House Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection (Jul. 29, 2005), *available at* http://www.epic.org/privacy/choicepoint/datasec7.28.05.html (discussing some of the motives for security breaches, including identity theft, debt collection, extortion, voyeurism, and competition).

11. *After the Breach: How Secure and Accurate is Consumer Information Held by ChoicePoint and other Data Aggregators?: Hearing on S.B. 550 Before the Comm. on Banking, Finance and Insurance*, Cal. Senate, 2005-06 Reg. Sess. (Mar. 30, 2005) (testimony of Dan McGuffey, Vice President, Data Acquisition and Strategy, ChoicePoint Services, Inc.), *available at* http://www.epic.org/privacy/choicepoint/cp3.30.05.pdf (last visited Sept. 21, 2005). The title of the hearing can be found at http://info.sen.ca.gov/pub/bill/sen/sb_0501-0550/sb_550_cfa_20050504_153527_sen_comm.html (last visited Nov. 16, 2005).

12. *38 AGs Send Open Letter to ChoicePoint*, USA TODAY, Feb. 19, 2005, *available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-19-ag-letter-to-choicepoint_x.htm.

13. *After the Breach: How Secure and Accurate is Consumer Information Held by ChoicePoint and other Data Aggregators?: Hearing on S.B. 550 Before the Comm. On Banking, Finance and Insurance*, Cal. Senate, 2005-06 Reg. Sess. (Mar. 30, 2005) (testimony of Chris Jay Hoofnagle, Director, Electronic Privacy Information Center), *available at* http://72.14.203.104/search?q=cache:irwkp5EPpBoJ:www.epic.org/privacy/choicepoint (last visited Nov. 16, 2005).

Reed Elsevier, the Anglo-Dutch publishing giant, similarly reported in April 2005 that unauthorized people using customer passwords of its subsidiary, Seisint, may have gained access to the personal information of up to 310,000 people in the United States.[14] Seisint and Lexis-Nexis (Reed Elsevier's legal department) often obtain data from government records.[15]

Since the ChoicePoint breach was first reported, scores of similar breaches have been reported, affecting the personal information of millions of individuals.[16] These breaches reflect a failure of self-regulation on the part of the commercial entities that collect, store, and sell personal information.

A recent report described the ease with which government records may be combined to create dossiers on citizens.[17] Computer scientists at Johns Hopkins University replicated the methods of companies like ChoicePoint by linking databases such as death records, property tax information, campaign donations, and occupational license registries.[18] For less than $50 it was possible to enter a single name and generate multiple layers of information on individuals, including home address, phone number, occupation, birth dates, and family details. [19]

The question arises, therefore, as to whether the government should take steps to withhold sensitive personal information from disclosure on the Internet. The companies that turn a profit from collecting and then selling such

---

The title of the hearing can be found at http://info.sen.ca.gov/pub/bill/sen/sb_0501-0550/sb_550_cfa_20050504_153527_sen_comm.html (last visited Nov. 16, 2005).

14. Kirchgaessner, *supra* note 9, at 17.

> [T]he Financial Times obtained a comprehensive report on one individual generated by Seisint's Accurint database. It included the person's Social Security number[,] . . . . . political party affiliation, date of birth, every address at which the person had lived within the U.S., the names and birth dates of some neighbours . . . . . and details of a property sale. . . .
>
> The report also included the names, previous and current addresses and telephone numbers of the individual's immediate family members; the first five digits of the family members' Social Security numbers; the names and birthdates of their neighbours; and "neighbourhood profiles" - the average age of residents in the neighbourhood, the average number of years of education, the median household income and the median home value.
>
> Accurint also offered information on whether the individual had any registered motor vehicles or merchant vessels; whether they were certified by the Federal Aviation Administration; whether they had a criminal record or had committed any sexual offences; or whether they owned a hunting or fishing permit or a permit to hold a concealed weapon.

Id.

15. Heather Timmons, *Reed Elsevier Raises Toll for Data Theft at LexisNexis Unit*, INTERNATIONAL HERALD TRIBUNE, Apr. 14, 2005, at 16, *available at* http:www.westlaw.com.

16. *See* Privacy Rights Clearinghouse, *supra* note 10.

17. Tom Zeller, Jr., *Personal Data for the Taking: Students Surfing Public Records Learn It's Easy to Find Out a Lot*, NEW YORK TIMES, May 18, 2005, at A1.

18. *Id.*

19. *Id.*

information, often through open government records requests, have lobbied forcefully to ensure that public sources of private information remain open.[20] This article, by contrast, makes the case that state actors have an obligation to protect confidential personal information from unwarranted disclosure.

Part I of this article describes the kinds of personal information collected, stored, and disclosed by government offices, including the courts, and describes the principles of fair information practices that should be brought to bear upon the release of personal information to commercial data brokers. Part II explicates the tensions between privacy and disclosure, using the specific examples of home address information and a heated debate before a state privacy study commission in New Jersey. Part III asks whether a "right to information privacy" can survive in the digital age, examining the constitutional, statutory, and normative arguments for and against disclosure of personal information in government files. Part IV discusses the eroding distinction between government and commercial databases and implications for civil liberties. Part V offers policy recommendations to protect public interest in privacy.

I. PERSONAL INFORMATION IN GOVERNMENT RECORDS

To withstand the profit imperative, individuals in the United States are protected by a patchwork of narrow privacy statutes. One's video rental records, for example, are amply protected by federal law,[21] but one's health records may be disclosed for marketing purposes.[22] The privacy interests of a single individual are rarely strong enough to prevail against countervailing commercial interests, but most Americans sense they are entitled to a measure

20. The leading advocate for keeping public records open to data mining companies is the Coalition for Sensible Public Records Access ("CSPRA"). Members of CSPRA include Acxiom Corporation, Donnelly Marketing, The Dun & Bradstreet Corporation, Equifax Inc., Experian, First American Real Estate Solutions, Lexis Nexis, The Polk Company, and Trans Union. Fred H. Cate & Richard J. Varn, *The Public Record, Information Privacy and Access: A New Framework for Finding the Balance*, http://www.netcaucus.org/books/privacy2001/pdf/Limitsofoptin.pdf. Ironically, CSPRA appears to have taken down its website, at least temporarily (www.cspra.org/csprasite/). Some of its activities are described in a white paper at http://www.netcaucus.org/books/privacy2001/pdf/Limitsofoptin.pdf.

For more information on lobbying efforts by the Newspaper Association of America, the Society of Professional Journalists, the Reporters Committee for Freedom of the Press, the Associated Press, and the American Society of Newspaper Editors, see Jonathan Kaplan, *The Freedom of Information Center: Advocates for Journalists May Take Agenda to K Street*, THE HILL, Feb. 10, 2005, *available at* http://foi.missouri.edu/firstamendment/advforjs.html. S*ee also* Tom Zeller, Jr., *The Scramble to Protect Personal Data*, N.Y. TIMES, Jun. 9, 2005, at C1.

21. Video Protection Privacy Act, 18 U.S.C. § 2710 (2000).

22. *See* HIPAA Privacy Act, 45 C.F.R. §§ 164.500(a), 164.501 (defining marketing), 164.508(a)(3), 164.512(b)(1)(iii)(D) (2005).

of privacy that goes above and beyond the claims that are recognized by tort law.[23]

A. Open Government Records Statutes

Open government records are essential for a functioning democracy, allowing citizens to understand and evaluate the inner workings of state and local government. Open government records are also a valuable tool for protecting individuals from governmental intrusion into personal privacy. Privacy advocates often use the Freedom of Information Act and other open government records statutes to limit governmental intrusion into the private lives of individuals.[24]

23. The tort of invasion of privacy was first proposed by Louis D. Brandeis and Samuel D.Warren in *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890). This tort differs substantially in its origins from the line of cases following the constitutional right to information privacy and FOIA-type statutes. *See, e.g.*, Kinsella v. Welch, 827 A.2d 325, 333 (N.J. Super. Ct. App. Div. 2003) ("A crucial distinction between the constitutional right of privacy and its common law namesake is that the common law right operates as a control on private behavior, while the constitutional right operates as a control on government. The two rights are necessarily different because our concept of appropriate behavior for private persons and government officials is different."). Open government records statutes apply to state action, and the tort applies to commercial or other non-governmental actors. *See generally Understanding the Federal Courts: The Jurisdiction of the Federal Courts*, THE ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 1999, at 7-10, http://www.uscourts.gov/UFC99.pdf; 28 U.S.C. § 1331 (1980). Legally recognized privacy interests have been aptly described as a haystack in a hurricane; examples of privacy invasions abound, yet they often defy systematic labeling. Ettore v. Philco Television Broad. Corp., 229 F.2d 481, 485 (3d Cir. 1956). The Second Restatement of Torts adopted Prosser's classic system of categorizing four different kinds of privacy invasions: 1) intrusion (e.g., hidden videotape cameras); 2) appropriation (e.g., commercial use of name or likeness); 3) false light (from which spring, for example, disclaimers on motion pictures, denying any resemblance to persons living or dead); and 4) public disclosure of private facts (e.g., disclosing privileged communications). RESTATEMENT (SECOND) OF TORTS § 652A (1977). This system of categorization has operated as both a blessing and a curse. The categories have allowed litigants to recover for some kinds of invasions, but have seriously limited those who fall outside the parameters of the four compartments. Allstate Insurance Co. v. Ginsberg, 351 F.3d 473, 479-81 (11th Cir. 2003) (refusing to extend the invasion of privacy to include unwelcome touching in a sexual manner).

24. *See* Solove, *supra* note 1. Personal information, including home addresses and telephone numbers, may be obtained from state government records without using open government records statutes as the avenue for submitting the request. *Id.* at 1143-45. The courts remain another avenue for obtaining non-public government records. *Id.* at 1156 . A common law right exists in most states to inspect government records so long as the requestor has a good reason to inspect the records, and the requestor's reasons for inspecting the records outweigh the state's interest in confidentiality. *Id.* A substantial body of case law generally provides broader access to government records, but requires a judicial balancing test. In many jurisdictions, however, the common law right of access to government records permits the state to inquire into the requestor's reasons for seeking governmental records. *Id.* at 1158.

Federal offices are governed by two companion statutes: the Freedom of Information Act ("FOIA"), and the Privacy Act of 1974 ("Privacy Act"), both of which pertain to the disclosure of information about individual citizens.[25] The presumption behind FOIA is that government records belong to the people and should be disclosed unless they fall within one of nine specific categories.[26] The Privacy Act creates a presumption that if a government record pertains to an individual citizen, it should not be disclosed unless certain specific exceptions apply.[27]

As discussed in the New Jersey Privacy Study Commission Report,[28] when Congress considered these measures in the early 1970s, the United States Privacy Protection Study Commission articulated a set of fair information practices to limit the government's use of personally identifiable information.[29] These principles provide guidelines to limit the collection, use, disclosure, retention, and disposal of personal information by the government, and they have become widely accepted.[30] The following principles of fair information practices have become the foundation for many privacy laws and codes of practice around the world:

Collection limitation. There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.

Data Quality. Personal data should be relevant to the purposes for which the data are gathered and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

Purpose Specification. The purposes for which personal data are collected should be specified no later than the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

25. The Freedom of Information Privacy Act, 5 U.S.C § 552 (2002); The Privacy Act, 5 U.S.C. § 552a (2004).

26. The exemptions are for (1) national security; (2) internal agency rules; (3) other statutes; (4) business information; (5) internal government memos; (6) private matters; (7) law enforcement investigations; (8) regulation of financial institutions; and (9) oil wells. 5 U.S.C. § 552(b).

27. 5 U.S.C. § 552a(b).

28. *See* SPECIAL DIRECTIVE SUBCOMM., N.J. PRIVACY STUDY COMM'N, DRAFT OF THE REPORT OF THE SPECIAL DIRECTIVE SUBCOMMITTEE TO THE NEW JERSEY PRIVACY STUDY COMMISSION 17 (Sept. 8, 2003), *available at* http://www.nj.gov/privacy/eo26.pdf.

29. *See* PERSONAL PRIVACY IN AN INFORMATION SOCIETY: REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, *available at* http://www.epic.org/privacy/ppsc1977report.

30. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (permissible purposes of consumer reports); Privacy Act of 1974, 5 U.S.C. § 552a (fair information practices for personally identifiable information).

Use Limitation. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the purpose specification principle except with the consent of the data subject or by the authority of law.

Security Safeguards. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Openness. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data custodian.

Individual Participation. An individual should have the right:

(a) to obtain from a data custodian confirmation of whether or not the data custodian has data relating to him;

(b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Accountability. A data custodian should be accountable for complying with measures that give effect to the principles stated above.[31]

The United States Privacy Protection Study Commission recognized that "[t]he real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[32] The Internet has realized this prediction. Indeed, credit card companies, financial institutions, and government agencies share or

31. New Jersey Information Practices Act, N.J. STAT. ANN. § 17:23A-1 (1985) (governs HMOs and other insurance entities); Canada Privacy Act, R.S.C., ch. P 21 (1985). Every state in the European Union has adopted fair information practices as law. *See* Council Directive 95/46/EC, 1995 O.J. (L 281), 31-51 (EC) (Directive of the European Parliament and the Council of Ministers of the European Commission on the protection of individuals with regard to the processing of personal data and on the free movement of such data); THE ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2005), *available at* http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html.

32. U.S. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY Ch. 13 (1977), *available at* http://www.epic.org/privacy/ppsc1977report/c13.htm.

sell personal information unless the affected individuals take affirmative steps to demand that their records not be disclosed.[33]

As presently constituted, many state open government records statutes threaten to expose individual citizens to greater invasions of privacy, not by government, but by commercial enterprise.[34] Many requests for government records come not from watchdog groups, the press, or private citizens, but from data mining companies that glean personal information from governmental records for the purpose of creating "profiles" or dossiers on individuals.[35]

B. Court Records

Courthouse records, similarly, are mined and harvested for personally identifiable information. Court records often contain information that is exquisitely personal, such as:

- Social Security numbers;
- income and business tax returns;
- information provided or exchanged by the parties in child support enforcement actions;
- home addresses of litigants, witnesses and jurors;
- photographs depicting violence, death, or children subjected to abuse;
- name, address, or telephone number of victims, including sexual assault and domestic violence cases;
- names, addresses, and telephone numbers of witnesses in criminal cases;
- names, addresses ,and telephone numbers of informants in criminal cases;
- names, addresses, or telephone numbers of potential or sworn jurors in criminal cases;
- juror questionnaires and transcripts of voir dire of prospective jurors;
- medical or mental health records, including examination, diagnosis, evaluation, or treatment records;

33. Gramm-Leach-Bliley, Pub.L. No. 106-102, 15 USC, Subchapter I, Sec. 6801-6809 (1999) (financial institutions may sell or disclose personal financial records unless the individual "opts-out"). See http://www.zabasearch.com for an example of a website that obtains unlisted telephone numbers from government records and makes them freely available online.

34. Different states vary considerably in their approaches to providing access to government records. *See* Solove, *supra* note 1, at 1163.

35. The federal Government Accountability Office defines "data mining" as "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 the prediction of future results." U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 1 (2004), *available at* http://www.gao.gov/new.items/d04548.pdf.

- psychological evaluations of parties, for example regarding competency to stand trial;
- child custody evaluations in family law or abuse and neglect actions;
- information related to the performance, conduct, or discipline of judicial officers;
- information related to alleged misconduct by entities or individuals licensed or regulated by the judiciary;
- trade secrets and other intellectual property.[36]

The personal information taken from government records is often not used for its intended purpose but instead purchased and sold for purposes totally unrelated to government mandates.[37] Citizens are compelled to disclose information about themselves to the courts, but their information may be mined and sold for a profit.[38] Nor is the information used for purposes that benefit the individual.

These court records can be used to create an underclass of people who cannot get jobs, rent apartments, or obtain credit. For example, data mining companies that perform employee background checks keep permanent records of arrests and criminal sentences.[39] Once recorded in commercial databases, these records cannot be corrected or expunged, even if the arrests never led to conviction or if the data become stale and irrelevant.[40] Currently, African-Americans are disproportionately represented in the vulnerable population of people who have such records.[41]

The courts and state and local government agencies must not disregard the consequences of publishing these records. State actors have no obligation to help data mining companies make a profit. However, state and local government agencies do have an obligation to protect the public interest in privacy. This can be done without compromising the spirit and purpose of open government records legislation, which is to shed light on government operations.

36. *See* Solove, *supra* note 1, at 1145-48.

37. *Id*. at 1194-95.

38. *See id*. at 1145, 1149-50, 1152.

39. *See, e.g.*, Jennifer Bayot, *Use of Credit Records Grows in Screening Job Applicants*, N.Y. TIMES, March 28, 2004. *See also*, Solove, *supra* note 1, at 1152 (explaining that an anonymous woman was terminated from her job after a background check erroneously indicated a past drug conviction).

40. Congress has elicited comments on the Attorney General's report on Criminal Records and Employment Screening (OLP Docket No. 100). *See* Government in the Sunshine Act Meeting Notice, 70 Fed. Reg. 32,849 (June 6, 2005); Groups Warn of Privacy Risks in Employment Screening, August 8, 2005, *available at* www.privacyrights.org/ar/DOJbackgrd.htm. *See also* Kim Zetter, *Bad Data Fouls Background Checks*, WIRED, March 11, 2005, www.wired.com/news/privacy/0,1848,66856,00.html.

41. *See* EVAN HENDRICKS, CREDIT SCORES AND CREDIT REPORTS: HOW THE SYSTEM REALLY WORKS WHAT YOU CAN DO 235 (2004).

II. THE STATE HAS AN OBLIGATION TO PROTECT CITIZENS

Confidence in government at all levels is best sustained by access to the information necessary to promote the vigorous public discussion that a well-functioning democracy requires. However, when dealing with information that individuals reasonably expect to remain private and to not be published by the government, there should be a presumption that such information will remain confidential unless there is an overriding justification for its disclosure.

To that end, the state should confer special protection for four categories of information: home address, Social Security Number, medical information and financial information.[42] The privacy value of the Social Security Number is well known,[43] and there is widespread support for keeping medical and financial records confidential.[44] To illustrate the tension between privacy and disclosure and to explicate the constitutional and statutory limits on publication by the government, one highly controversial data item provokes heated debate: the home address.[45]

Home address information is avidly sought by commercial data aggregators and avidly protected by a comparatively small population of individuals who seek confidentiality and sometimes protection.[46] The government's obligation to protect or disclose home address information is subject to constitutional, statutory, common law, and normative limits.

A. Home Address Information

Home addresses poignantly illustrate the debate about whether state agencies should disclose personal information about citizens pursuant to open

42. See *infra* p. 27 and nn. 320 & 330 for the proposition that two exceptions should apply to home address: voter registration records and tax assessment records should remain public, whereas all other home address records should remain confidential. See *infra* nn. 328-31 and accompanying text for the proposition that one exception should apply as to financial records: the salaries of public employees.

43. *See* UNITED STATES GENERAL ACCOUNTING OFFICE REPORT TO THE CHAIRMAN, HOUSE SUBCOMMITTEE ON SOCIAL SECURITY, SOCIAL SECURITY NUMBERS: PRIVATE SECTOR ENTITIES ROUTINELY OBTAIN AND USE SSNS, AND LAWS LIMIT THE DISCLOSURE OF THIS INFORMATION, *available at* http://www.gao.gov/new.items/d0411.pdf.

44. *See* U.S. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977), *available at* http:/ www.epic.org/privacy/ppsc1977report.

45. *See, e.g.*, Rowan v. U.S. Post Office Dept., 397 U.S. 728, 738 (1970) (rejecting argument that vendors have a right under the Constitution to send unsolicited mail into another's home); Paul P. v. Verniero, 170 F.3d 396, 399 (3d Cir. 1999) (explaining that plaintiffs argued that the law infringed their constitutionally protected privacy interest by disseminating their home address).

46. *See, e.g.*, National Network to End Domestic Violence, *Public & Internet Access to Court Records: Safety & Privacy Risks for Victims of Domestic Violence & All Citizens Using the Justice System, available at* www.ischool.washington.edu/lawsymposium/docs/CourtRecordsand Victims.pdf; Solove, *supra* note 1, at 1138-40.

government records requests. On one side, data aggregators and journalists argue that home address is a valuable identifier that should always be in the public domain.[47] On the other, privacy advocates and many individuals argue that the state should not be in the business of disclosing personally identifiable information.[48]

Citizens disclose their home addresses because they are compelled to do so by state law and in order to receive basic governmental services.[49] Since they have no choice but to give their home addresses to the government, they should reasonably expect that the government will not re-disclose their addresses to unknown third parties. As explained below, there exists a right to privacy in one's home address, under the United States Constitution, some state constitutions, and by statute.[50]

i. Special Status of the Home. "The home has long enjoyed significant legal protection as a private place."[51] The maxim that "a man's home is his castle" appeared as early as 1499.[52] Parliamentarian William Pitt wrote, "The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter – all his force dares not cross the threshold of the ruined tenement!"[53] The Supreme Court recognized in 1886 the importance of protecting "the sanctity of a man's home."[54] "In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home . . . ."[55]

The home enjoys a special status as refuge from intrusions by the state and commercial enterprise.[56] One of the most famous formulations of the right to

47. *Compare* Solove, *supra* note 1, at 1149, *with* Fred H. Cate & Richard J. Varn, *The Public Record, Information Privacy and Access: A New Framework for Finding the Balance*, http://it.ojp.gov/initiatives/files/Public_Record.pdf.

48. *See, e.g.*, GENERAL ACCOUNTING OFFICER REPORT TO CONGRESSIONAL REQUESTERS, SOCIAL SECURITY NUMBERS, GOVERNMENT BENEFITS FROM SSN USE, BUT COULD PROVIDE BETTER SAFEGUARDS, *available at* http://www.epic.org/privacy/ssn/d02352.pdf.

49. *See* Solove, *supra* note 1, at 1143-44.

50. *See infra* Part I.A.i-iii.

51. MARC ROTENBERG & DANIEL J. SOLOVE, INFORMATION PRIVACY LAW 585 (2003).

52. *Id*.

53. *See* Miller v. United States, 357 U.S. 301, 307 & n.7 (1958) (quoting William Pitt's speech before Parliament in 1763).

54. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

55. Payton v. New York, 445 U.S. 573, 589 (1980).

56. *See, e.g.*, Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 738 (1970) (rejecting the argument that a vendor has a Constitutional right to send unwanted material into the home of another); Mainstream Mktg. Serv., Inc. v. F.T.C., 358 F.3d 1228, 1246 (10th Cir. 2004) (holding that governmental interest is sufficient to defeat First Amendment challenge to "do-not-call" registry); F.L.R.A. v. U.S. Dep't of Navy, 966 F.2d 747, 756 (3d Cir. 1992) (finding that the disclosure of an individual's home address infringes upon a recognized privacy interest);

privacy calls it "the right to be let alone - the most comprehensive of rights and the right most valued by civilized men."[57] In *Rowan v. United States Post Office*, the U.S. Supreme Court held that the "right to be let alone" in one's home requires upholding, against First Amendment challenges, the rights of homeowners to take their names and addresses off various mailing lists:

> We . . . categorically reject the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another. . . . That we are often "captives" outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. . . . The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain."[58]

Rowan places the right to be let alone in one's home "in the scales" with the constitutionally protected rights of others to communicate.[59]

ii. Federal Constitutional Protection for Home Address Information. The United States Constitution explicitly protects the home as a refuge from governmental action, including dissemination of personal information. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers and effects . . .[,]"[60] the Third Amendment protects the home from military use,[61] and the First Amendment protects free expression in the home.[62] The Due Process clause of the Fourteenth Amendment specifically protects private conduct in the home.[63]

The United States Supreme Court defined a distinct constitutional right to "information privacy" in *Whalen v. Roe*, which addressed the constitutionality of a state law that required physicians to report patients who obtained certain kinds of prescription drugs.[64] The Court held that the right to privacy embraced both (i) an "individual interest in avoiding disclosure of personal matters" and (ii) an "interest in independence in making certain kinds of

F.L.R.A. v. U.S. Dep't of Treasury, 884 F.2d 1446, 1453 (D.C. Cir. 1989) (finding that federal employees have privacy interests in their home addresses); N.A.R.F.E. v. Horner, 879 F.2d 873, 879 (D.C. Cir. 1989) (finding there was no public interest in the disclosure of addresses of individuals receiving federal employee retirement benefits).

57. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

58. 397 U.S. at 738 (citations omitted).

59. *Id*. at 736.

60. U.S. CONST. amend. IV.

61. U.S. CONST. amend. III.

62. *See, e.g.*, Stanley v. Georgia, 394 U.S. 557, 565 (1969).

63. *See, e.g.*, Lawrence v. Texas, 539 U.S. 558, 562, 578 (2003). Many Supreme Court cases make the point in a variety of contexts that the home is the last refuge of privacy. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 29-31 (2001) (thermal imaging); Frisby v. Schultz, 487 U.S. 474, 483-85 (1988) (residential picketing); FCC v. Pacifica Found., 438 U.S. 726, 748-49 (1978) (broadcast media).

64. 429 U.S. 589 (1977).

important decisions."[65] Interpreting this right to information privacy, the United States Court of Appeals for the Third Circuit has held that case law "reflect[s] the general understanding that home addresses are entitled to some privacy protection, whether or not so required by a statute."[66]

iii. Statutory Protection for Home Address Information: FOIA and the Privacy Act. As the Supreme Court has recognized, there exists a substantial privacy interest in home address information.[67] This interest is expressed, in part, through legislation, of which the best current example is the Privacy Act, which Congress enacted as a companion statute to the FOIA.[68]

The FOIA was enacted in 1966 and amended in 1974.[69] FOIA creates procedures whereby any member of the public may obtain records of the agencies of the federal government.[70] It has served as the model for most open government records statutes in the states.[71]

Although the goal of FOIA is full disclosure of government records, Congress concluded that some confidentiality would be necessary for the government to function.[72] A federal agency may refuse to release certain types of information.[73] There are nine legal categories that are exempted from FOIA under section 552(b) of the law.[74] One of the exemptions is for "private matters;"[75] another is for other statutes, including the Privacy Act.[76]

The Privacy Act permits individuals to obtain their own records, gives them the right to correct, amend, or delete information about themselves, and gives them the right to sue federal agencies if they refuse to correct or amend the records.[77] The Privacy Act creates a default presumption that records regarding personal individuals will not be disclosed.[78]

Reading FOIA and the Privacy Act together, the U.S. Supreme Court has said that people have a reasonable expectation of privacy with respect to their

65. *Id*. at 599-600, 604-05.

66. Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999).

67. U.S. Dep't of Def. v. F.L.R.A., 510 U.S. 487, 502 (1994) (interpreting the Freedom of Information Act and the Privacy Act of 1974).

68. Privacy Act of 1974, 5 U.S.C. § 552a (2005).

69. Freedom of Information Act, 5 U.S.C. § 552 (2005).

70. § 552(a)(1).

71. *See* Solove, *supra* note 1, at 1161.

72. *See* 5 U.S.C. § 552(b).

73. § 552(b).

74. For a list of the nine exceptions, see *supra* note 26 and accompanying text.

75. § 552(b)(6).

76. § 552(b)(3).

77. 5 U.S.C. § 552a(d) (2005). This is consistent with the principles of fair information practices. *See supra* notes 32-33 and accompanying text.

78. 5 U.S.C. § 552a(b) (2005).

home addresses.[79] In *United States Department of Defense v. Fair Labor Relations Authority*, the Court explained:

> It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but in an organized society, there are few facts that are not at one time or another divulged to another. . . . . An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form. . . . . We are reluctant to disparage the privacy of the home, which is accorded special consideration in our Constitution, laws, and traditions.[80]

This is consistent with ordinary experience. Many people have a reasonable expectation that their home addresses will be private. These include children and people who have made a genuine effort to keep their home address information private by getting an unlisted telephone number or asking to be removed from mailing lists. Other groups of people often seek protection of their home address information: celebrities, domestic violence victims, stalking victims, witnesses in criminal cases, abortion doctors, and police officers.

If one does not want one's residence to be known, the importance of its being unknown goes to the core of individual privacy. People who do not want the government to disclose their home addresses have limited means for preventing disclosure and little recourse once the disclosure has been made. The government should not force individuals to sacrifice their privacy as a condition of doing business.[81] Indeed, if a state were routinely to give out home addresses, it would be at peril not only of violating the Constitution, but it would also repudiate the privacy protections of the federal FOIA approach, which is the approach on which most state open government records statutes are modeled.[82]

In *Forest Guardians v. U.S. FEMA*, the Tenth Circuit affirmed privacy for geographic information systems ("GIS"), finding that disclosure would invade privacy by giving away the location of residential structures in New Mexico's flood plains.[83] The court found there was no public interest in disclosure.[84]

79. U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 502 (1994).

80. *Id*. at 500-01 (citations and quotations omitted).

81. Some states allow victims of domestic violence to use an alternate address for all state and local governmental purposes, including driver's licenses and registration, professional licensing, banking and insurance records, welfare, etc. *See, e.g.*, N.J. STAT. ANN. § 47:4-1 (1998). New Jersey laws also enable victims of domestic violence to vote without revealing their addresses. N.J. STAT. ANN. § 19:31-3.2 (2001). Victims of sexual assault and stalking may use an alternate address on their driver's license and registration. N.J. STAT. ANN. § 39:3-4 (2004).

82. *See, e.g.*, McClain v. Coll. Hospital, 492 A.2d 991, 996 (N.J. 1985).

83. 410 F.3d 1214, 1216-19 (10th Cir. 2005).

84. *Id*. at 1219.

The Forest Guardians, an environmental group, asked for the information in order to show that FEMA was promoting overdevelopment in flood plains.[85] FEMA released the information in paper form, but declined to disclose its GIS files.[86] The court held that "[i]n the context of an individual residence, 'the privacy interest of an individual in avoiding the unlimited disclosure of his or her name and address is significant. . . . . ."[87]

> The type of privacy interests Congress intended to protect under Exemption 6 [of FOIA] encompass the individual's control of information concerning his or her person. Such private information includes, for example, an individual's name and home address. The privacy interest in an individual's home address becomes even more substantial when that information would be coupled with personal financial information. In this case, the electronic GIS files are exempt from disclosure under Exemption 6 . . . [as they] reveal specific geographic point locations for NFIP ["National Flood Insurance Program"] insured structures. Such information, coupled with property records, can lead to, among other things, the names and addresses of individual property owners and thus applies to particular individuals.[88]

The court found commercial solicitation to be sufficiently intrusive to invoke governmental protection.[89]

> NFIP policyholders have a privacy interest – the extent of which we need not quantify today. . . . . Furthermore, disclosure of the electronic GIS files and, the concomitant disclosure of personal information, could subject individuals to unwanted contacts or solicitation by private insurance companies. Given the commercial interests involved in the NFIP and, the large-scale participation by the private insurance industry, a palpable threat exists that disclosing information that could reveal names, home addresses, and other personal insurance policy information could lead to an influx of unwanted and unsolicited mail, if not more.[90]

B. One Local Debate: The New Jersey Privacy Study Commission

Debating authorities and interest groups engaged in vigorous dispute over access to home address information before a state commission in New Jersey. The New Jersey Privacy Study Commission[91] was convened for the purpose of

85. *Id*. at 1216.

86. *Id*. at 1217.

87. *Id.* at 1220 (quoting Nat'l Ass'n of Home Builders v. Norton, 309 F.3d 26, 35 (D.C. Cir. 2002)).

88. *Forest Guardians*, 410 F.3d at 1218 (citations and quotations omitted).

89. *Id*. at 1221.

90. *Id*. at 1220-21 (citations omitted).

91. The New Jersey Privacy Study Commission, on which the author served, was ably staffed by Catherine Starghill and the New Jersey Department of Community Affairs. State of

exploring the impact of the state's new open government records statute, the Open Public Records Act ("OPRA").[92] New Jersey had gone from having one of the most restrictive FOIA-type statutes, to having one of the most open.[93] Under a special directive from the governor, the Privacy Study Commission grappled specifically with the issue of home addresses, generating considerable controversy.[94] Over the course of a year and a half, the Privacy Study Commission elicited testimony from scores of witnesses, who argued for and against the disclosure of home address information from state and local government files.[95]

i. Arguments Against Disclosure of Home Address Information. The most common argument against disclosing home address and telephone information is "When I give my home address to the government I don't want the government to give it to anyone else."[96] The National Network to End Domestic Violence, for example, criticized the practice of publishing domestic violence, sexual assault, and family law cases on the Internet.[97] The New Jersey Coalition for Battered Women submitted a written statement strongly opposing the disclosure of names, addresses, phone numbers, and personal information to the general public.[98] "No victim of domestic violence should be impeded in her or his efforts to remain safe from a batterer by the unmonitored disclosure of their contact information by the government."[99]

An expert on privacy and government records, Professor Daniel J. Solove,[100] provided written testimony to the Commission, taking the position that governmental disclosure of home address information might in some instances violate the federal or state constitution.[101] To disclose home

New Jersey Privacy Study Commission, Commission Members and Staff, http://www.nj.gov/privacy/members.html (last visited Nov. 7, 2005).

92. State of New Jersey Privacy Study Commission, http://www.nj.gov/privacy (last visited Nov. 7, 2005). For the full text of the Open Public Records Act, including the charge to the Privacy Study Commission, see Open Public Records Act, http://www.state.nj.us/grc/act.html.

93. *See* 1963 N.J. Laws 223; N.J. STAT. ANN. § 47:1A-1 (2005).

94. Exec. Order No. 26, State of New Jersey, Aug. 13, 2002, *available at* http://www.state.nj.us/infobank/circular/eom26.shtml.

95. N.J. PRIVACY STUDY COMMISSION, FINAL REPORT: N.J. PRIVACY COMMISSION 15 (Dec. 2004), *available at* http://www.nj.gov/privacy/prc_final_report_v21.pdf (last visited Nov. 18, 2005) [hereinafter N.J. PRIVACY REPORT].

96. *Id.* at 18.

97. Testimony before the Privacy Study Commission is on file with the author and at the New Jersey Department of Community Affairs. *See* National Network to End Domestic Violence, *supra* note 46.

98. N.J. PRIVACY REPORT, *supra* note 95, at 27.

99. *Id*.

100. Daniel J. Solove is an associate professor of law at George Washington University Law School. The George Washington University Law School, *Daniel J. Solove*, http://docs.law.gwu.edu/facweb/dsolove (last visited Nov. 10, 2005).

101. N.J. PRIVACY REPORT, *supra* note 95, at 24.

addresses and telephone numbers under open government records statutes, he explained, would constitute a departure from the federal approach under the FOIA[102] and could potentially be unconstitutional.[103] There are several groups of people who have a strong interest in keeping their home addresses confidential, and ample case law from federal and state courts recognizes a state interest in preserving residential privacy.[104] Professor Solove emphasized the following points:

1. There are very compelling reasons why people want their addresses and phone numbers to remain private.
2. The addresses and phone numbers in public records are often not acquired by the government voluntarily. People are compelled to supply this information. Without privacy protection for this information, what the state would be doing is compelling people to divulge information to the public that they may want to remain confidential.
3. The Third Circuit case law, which governs in New Jersey, has recognized that there is a constitutional interest in the nondisclosure of personal information.[105] The government has the burden of justifying why it needs to disclose certain personal information and why that disclosure outweighs people's privacy interests.
4. This issue is too important and complex for absolute rules. An appropriate solution must balance the interests on both sides and take into account that many people have compelling safety reasons for not disclosing their addresses and phone numbers.
5. The primary purpose for public access to government records is to enable the people to learn about how their government functions. Government records are not supposed to be a way to spy on citizens or find out the personal information they would like to keep confidential. These aims satisfy private interests, not public ones.[106]

102. Professor Solove authored a casebook entitled INFORMATION PRIVACY LAW, and has written extensively on the subject. *See generally* ROTENBERG & SOLOVE, *supra* note 51; DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004). His written testimony, and all written testimony received by the New Jersey Privacy Study Commission, is posted on the Commission's web site. *See* N.J. Privacy Study Commission, www.nj.gov/privacy/ (last visited Nov. 10, 2005).

103. N.J. PRIVACY REPORT, *supra* note 95, at 24.

104. *Id*.

105. *See* A.A. v. N.J., 341 F.3d 206, 211-12 (3d Cir. 2003); Paul P. v. Farmer, 227 F.3d 98, 99, 101 (3d Cir. 2000); Paul P. v. Verniero, 170 F.3d 396, 406 (3d Cir. 1999); Doe v. Poritz, 662 A.2d 367, 408-09 (N.J. 1995).

106. *See* N.J. PRIVACY REPORT, *supra* note 95, at 24-25.

According to Professor Solove:

> It is important to note that the personal information in public records is often compelled by the government. People don't give it out freely but are often forced to do so. Broad disclosure of people's addresses can compromise people's safety. It may benefit the media, which wants easy access to information, and commercial interests, which want to use addresses for marketing purposes. But in balancing under the Constitution, courts look to the extent to which the greater public interest is served by disclosure.[107]

ii. Arguments in Favor of Disclosing Home Address Information. The Privacy Study Commission received several comments articulating the view that no privacy interest should attach to data if the data can be found anywhere in the public domain.[108] Therefore, they argue, such data should be available from the state through requests for open government records.[109] This view is consistent with much case law.[110] It is also consistent with Fourth Amendment search-and-seizure law; the United States Supreme Court has held that unless a matter is kept secret, it enjoys no "reasonable expectation of privacy."[111] For example, although the Court has found a reasonable expectation of privacy within the four walls of the home,[112] it found no reasonable expectation of privacy in sealed, opaque garbage bags discarded by the curb.[113]

Professor Fred H. Cate told the Privacy Study Commission "that no constitutional privacy right attaches to home addresses and home telephone numbers."[114] In his view, "the constitution does not prohibit public access to home addresses . . . in government records."[115] Indeed, "he stated that the Constitution permits and even encourages public access to such information."[116]

107. *Id*. at 25.

108. *Id*. at 42.

109. *Id*.

110. *See* 62A AM. JUR. 2D *Public Records* § 107 (2005) ("The right of privacy is not infringed by the publication of matters of public record.").

111. *See, e.g.*, Illinois v. Andreas, 463 U.S. 765, 771 (1983).

112. *See, e.g.*, Kyllo v. U.S., 533 U.S. 27, 40 (2001).

113. California v. Greenwood, 486 U.S. 35, 39-40 (1988).

114. N.J. PRIVACY REPORT, *supra* note 95, at 28. Professor Cate is a professor at Indiana University School of Law-Bloomington, Indiana. *Id.* at 28 n.29. His research and his trip to New Jersey were supported by the Coalition for Sensible Public Records Access, a not-for-profit group funded by businesses that "aggregate and enhance public records for public use." *Statement on the Constitutionality of the Disclosure of Name and Address Information from Public Records*: *Hearing on Address and Telephone Information in Public Records*, N.J. Privacy Study Commission 1 (2003) (statement of Fred Cate, Professor, Indiana University School of Law-Bloomington), http://www.law.indiana.edu/people/cate/Testimony/Cate.New%20Jersey.pdf [hereinafter Cate Statement].

115. N.J. PRIVACY REPORT, *supra* note 95, at 28.

116. *Id*.

According to Professor Cate, "there is no right to privacy guaranteed by the Constitution that would speak in any way to the government's disclosure of home address" information.[117] He testified that no court has found a constitutional right of privacy with respect to information such as home address.[118] The United States Court of Appeals for the Fourth Circuit, for example, struck down the Drivers Privacy Protection Act, stating that "neither the Supreme Court nor this Court has ever found a constitutional right to privacy with respect to the type of information found in motor vehicle records. Indeed, this is the very sort of information to which individuals do not have a reasonable expectation of privacy."[119] The case, *Condon v. Reno*, was reversed by the Supreme Court on other grounds.[120]

Professor Cate stated that only one U.S. Supreme Court case, *Whalen v. Roe*, has articulated a constitutional right in the nondisclosure of information, and that it did so in the context of nondisclosure *to* the government, rather than any obligation of nondisclosure *by* the government.[121] He further stated that the U.S. Supreme Court had never decided a case in which it found that disclosure *to or by* the government violated the constitutional right recognized in *Whalen*.[122] He cited *U.S. West, Inc. v. FCC*,[123] for the proposition that if government agencies decline to publish information, the agencies should have the burden to show that dissemination of the information would inflict *specific and significant harm* on individuals.[124]

Professor Cate acknowledged that the government legally owes a higher obligation to individual citizens than do private companies of nonprofit groups.[125] For constitutional and practical reasons, pertaining to the Fourth Amendment and the non-competitive environment in which it operates, the government has a higher obligation with regard to its own collection and use of information.[126] He supported the proposition that certain categories of information might be exempt from disclosure.[127] In certain circumstances, for example, involving undercover police officers and people protected by restraining orders, he said, "it would be reasonable to conclude that despite the

117. *Id*. at 29.

118. *Id*.

119. Condon v. Reno, 155 F.3d 453, 464-65 (4th Cir. 1998).

120. Reno v. Condon, 528 U.S. 141, 151 (2000).

121. N.J. PRIVACY REPORT, *supra* note 95, at 29.

122. *Id.*

123. 182 F.3d 1224, 1235 (10th Cir. 1999).

124. N.J. PRIVACY REPORT, *supra* note 95, at 29. As to this standard, see *infra* notes 156-60 and accompanying text.

125. *Home Addresses and Telephone Numbers in Government Records: Public Hearing*, N.J. Privacy Study Commission 87 (2003) (testimony of Fred Cate, Professor, Indiana University School of Law-Bloomington), www.nj.gov/privacy/ph_111203.pdf [hereinafter Cate Testimony].

126. *Id.* at 88.

127. Cate Statement, *supra* note 114, at 7.

constitutional values served by public access, [home] address . . . [information] should be protected."[128] With respect to categories such as medical records, he said that "most people would accept that there probably should be some limit on disclosing the names and addresses of people who have certain diseases[, but that] the state . . . [should nevertheless] provide aggregate information on the . . . reported incidents of . . . diseases and . . . the locations of the people who have them."[129] Although Professor Cate saw no harm per se in publishing Social Security numbers on the Internet, he acknowledged that it would be possible and in some cases, appropriate to disaggregate identifiers like the Social Security Number before publishing the "anonymized" remainder of a governmental record.[130]

III. CAN INFORMATION PRIVACY SURVIVE?

A common view of the right to privacy holds that if a piece of information can be found anywhere in the public domain, it should be available from the state through open government records requests.[131] For example, if a citizen's home address can be found in the telephone book, voter registration records, or property tax records, this view holds that there is no "reasonable expectation of privacy," and therefore the state should disclose the home address when it appears as part of any government record.[132]

On this view, it is tempting to think the right to information privacy has vanished. Under open government records statutes, it is the state, rather than commercial enterprise, disclosing information about individuals. This makes a difference.[133] An individual's home address may be found in a telephone book or on the Internet, but this fact does not justify action by the government to disclose the same home address where the individual has an expectation of

128. *Id.*

129. Cate Testimony, *supra* note 125, at 61.

130. *Id.* at 27.

131. *See, e.g.*, Paul P. v. Farmer, 227 F.3d 98, 101 (3d Cir. 2000).

132. This view is consistent with criminal search-and-seizure laws. The United States Supreme Court has held that, under the Fourth Amendment, unless a matter is kept secret, it enjoys no "reasonable expectation of privacy."" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). For example, the Court has found no reasonable expectation of privacy in sealed, opaque garbage bags discarded by the curb. California v. Greenwood, 486 U.S. 35, 40-41 (1988). On the other hand, the Fourth Amendment, which protects "the right of the people to be secure in their persons, houses, papers, and effects" establishes a reasonable expectation of privacy within the four walls of the home. *See* Kyllo v. United States, 533 U.S. 27, 31, 34 (2001) (thermal imaging). *See generally* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1121-24 (2002).

133. *See* Kinsella v. Welch, 827 A.2d 325, 333 (N.J. Super. Ct. App. Div. 2003) (explaining the distinction between the constitutional right of privacy, which pertains to government action, and its common law namesake, which pertains to non-governmental action).

privacy and, indeed, has no alternative but to give the information to the government.

A. Open Government Records and the Constitutional Right to Privacy

Improper disclosure of information by the government is a recognized injury.[134] The courts recognize a privacy interest every time the government discloses an individual's home address, even when the disclosure results in only a minimal effect, such as unsolicited contact.[135] The government has a duty to protect the privacy of individuals who have taken steps to protect themselves.[136] This is true despite, and indeed because of, the technological advances that have made individuals vulnerable to unwarranted intrusions.

State action has a constitutional dimension. The U.S. Supreme Court's decision in *Whalen v. Roe* has generated appellate precedent for the proposition that the state is not free to disclose confidential information about its citizens.[137] A majority of circuit courts have accepted the constitutional right to information privacy.[138]

The Third Circuit has articulated the constitutional right to information privacy, and repeatedly found a specific privacy interest in home address information.[139] In *United States v. Westinghouse Electric Corp.*, the court

134. *See, e.g.*, Greidinger v. Davis, 988 F.2d 1344, 1354-55 (4th Cir. 1993) (holding that voter registration system found to be unconstitutional because it required voters to disclose their Social Security numbers publicly in order to vote).

135. *See, e.g.*, U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 500-01 (1994).

136. *See* Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring) ("[T]he Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information. . . .").

137. *See, e.g.*, Sterling v. Borough of Minersville, 232 F.3d 190, 194, 196-97 (3d Cir. 2000); Borucki v. Ryan, 827 F.2d 836, 839-41, 848 (1st Cir. 1987); Barry v. City of New York, 712 F.2d 1554, 1558-59 (2d Cir. 1983).

138. *See, e.g.*, *In re* Crawford, 194 F.3d 954, 959 (9th Cir. 1999); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); *Barry*, 712 F.2d at 1559; United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-580 (3d Cir. 1980); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978). One circuit court has expressed "grave doubts" as the existence of the right, but has stopped short of confronting the issue of whether the right existed. Am. Fed'n. of Govt. Employees v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791-93 (D.C. Cir. 1997). The Sixth Circuit recognizes the right, but only as a narrow corollary to the decisional privacy cases, pertaining to personal information relating to one's health, family, children, and other interests protected by the Court's substantive due process right to privacy decisions. J.P. v. DeSanti, 653 F.2d 1080, 1089-90 (6th Cir. 1981).

139. *See* Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (holding that case law "reflect[s] the general understanding that home addresses are entitled to some privacy protection, whether or not so required by a statute").

described a balancing test to determine whether an individual's interest in privacy outweighs the public interest in disclosure:

> The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[140]

Under this analysis, the government's disclosure of home addresses under open government records statutes may in some cases violate a constitutionally protected right to privacy.[141] This would occur if an individual's interest in confidentiality outweighed the government's interest in disclosure, but a government agency nevertheless disclosed the information.[142]

Of course, many people do not care if their addresses are published. However, for some it can be a matter of life or death. Rebecca Shaffer, for example, was killed by a stalker who got her address from motor vehicle records.[143] The fact that some - or even most - people allow their home addresses to be published by commercial entities does not mean that the government should disclose the same information about the few who do not. As the Third Circuit explained:

> The compilation of home addresses in widely available telephone directories might suggest a consensus that these addresses are not considered private were it not for the fact that a significant number of persons, ranging from public officials and performers to just ordinary folk, choose to list their telephones privately, because they regard their home addresses to be private information. Indeed, their view is supported by decisions holding that home addresses are entitled to privacy under FOIA, which exempts from disclosure personal files

140. 638 F.2d at 578.

141. *See supra* note 134 and accompanying text.

142. The constitutional interest in residential privacy has been held to outweigh the 6th Amendment right of confrontation. *See, e.g.*, People v. Ramirez, 64 Cal. Rptr. 2d 9, 14-15 (Cal. Ct. App. 1997) (name of anonymous victim); Montez v. Superior Court, 7 Cal. Rptr. 2d 76, 81-82 (Cal. Ct. App. 1992) (home addresses of witnesses); People v. Lewis, 184 Cal. Rptr. 31, 33-34 (Cal. Ct. App. 1982) (home addresses of arresting police officers). *But see* Reid v. Superior Court, 64 Cal. Rptr. 2d 714, 22 (Cal. Ct. App. 1997) (holding that a victim's right to privacy "cannot provide the basis for a. . .court. . .to interfere with the defendant's normally unrestricted right to contact prosecution witnesses").

143. Condon v. Reno, 972 F. Supp. 977, 979 n.4 (D. S.C. 1997). *See also* Remsburg v. Docusearch, 816 A.2d 1001, 1005-06, 1008-09 (N.H. 2003) (Amy Boyer was murdered by stalker who obtained her home address via commercial database.).

> "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[144]

Even loathsome members of society, such as sex offenders, have constitutional rights, including a limited privacy interest in home address information. In *Doe v. Poritz*, the New Jersey Supreme Court reluctantly concluded that "under both the Federal and State Constitutions, the Registration and Notification Laws implicate protectable liberty interests in privacy and reputation, and therefore trigger the right to due process."[145] The

144. Paul P. v. Farmer, 227 F.3d 98, 101 (3d Cir. 2000) (citations omitted) (quoting Freedom of Information Act, 5 U.S.C. § 552(b)(6)).

145. 662 A.2d 367, 420 (N.J. 1995). The public reaction to *Doe v. Poritz* was outrage. *Proposes Constitutional Amendment Establishing that State may make Available to General Public Certain Information Identifying Sex Offenders: Public Hearing Before the Assembly Law and Public Safety Committee*, Assembly Concurrent Resolution No. 1, 1-2 (2000), *available at* http://www.njleg.state.nj.us/legislativepub/Pubhear/060100gg.pdf (last visited Nov. 18, 2005). The state constitution was amended to provide that, "[n]otwithstanding any other provision of this Constitution and irrespective of any right or interest in maintaining confidentiality, it shall be lawful for the Legislature to authorize by law the disclosure to the general public of information pertaining to the identity, specific and general whereabouts, physical characteristics and criminal history of persons found to have committed a sex offense." N.J. CONST., art. IV, § 7, ¶ 12 (adopted Nov. 7, 2000 and effective date of Dec. 7, 2000). The constitutional amendment stripped sex offenders of any right to privacy of their home address, but left the right to privacy intact for others. *Proposes Constitutional Amendment Establishing that State may make Available to General Public Certain Information Identifying Sex Offenders: Public Hearing Before the Assembly Law and Public Safety Committee*, Assembly Concurrent Resolution No. 1, 1-2 (2000), *available at* http://www.njleg.state.nj.us/legislativepub/Pubhear/060100gg.PDF (last visited Nov. 18, 2005). The transcript of a public hearing makes it clear that this was the intent of the sponsors of the constitutional amendment:

> What we are looking to do with this constitutional amendment is to see that, once and for all, the public's right to have knowledge about sexual predators is actually provided and that there is constitutional backing to allow such disclosure.Many of us, myself included, believe that, under both the New Jersey Constitution as well as the U.S. Constitution, notwithstanding the provisions of the 14th Amendment, that this right exists today. And nevertheless, given that there are those in the 3rd Circuit, as well as perhaps on our State Supreme Court, who feel differently, we want to make sure that there is no ambiguity as to the intent of this Legislature, and hopefully the administration, in terms of seeing that this information is information which rightly should be broadly disseminated. The question, constitutionally, is whether or not the privacy rights of the individual sex offenders takes precedence over the public's right to know. We strongly believe that the right to know and to protect the public, given the nature and the high probability of recidivism of many of these offenders, clearly is of greater import than the protection of privacy rights of the individuals in question.

Id. Perhaps paradoxically, the full implication of the constitutional amendment is that, while sex offenders have been stripped of any privacy interest in home address information, that interest remains intact, and more specifically so, for other members of society. *See id.*

Court explained that "disclosure of plaintiff's home address, particularly when coupled with the other information disclosed, implicates a privacy interest."[146]

> [T]he question of whether an individual has a privacy interest in his or her *bare* address does not fully frame the issue. The more meaningful question is whether inclusion of the address in the context of the particular requested record raises significant privacy concerns, for example because the inclusion of the address can invite unsolicited contact or intrusion based on the additional revealed information.[147]

i. Home Addresses Appear In Context. One objection to the assertion of constitutional protection for home address information is that legal authorities to date have dealt with compilations of personal information, rather than access merely to home addresses.[148] As noted above, in *Doe v. Poritz* and *Paul P. v. Verniero*, the courts did not consider whether the plaintiffs had a privacy interest in home address information alone, but whether the inclusion of the plaintiffs' addresses, along with other information, implicated any privacy interests.[149]

This objection does not account for the fact that home addresses are *always* disclosed in a context. Home address information would be almost meaningless if it were disclosed in a vacuum; it is hard to imagine that there would be any public interest in privacy with respect to a bare listing of residences. Only when paired with other data - name, income, disability status, etc. does home address information invoke a public interest in privacy. In some cases, the context of the information may touch an individual privacy interest that is sensitive enough to invoke statutory or constitutional protection.[150]

Different jurisdictions have adopted different standards to determine whether personally identifiable information should be disclosed under open government records laws. Some recommend creating categories of individuals whose home addresses and telephone numbers would be exempt from

146. *Poritz*, 662 A.2d at 409.

147. *Id*.

148. S*ee* Paul P. v. Verniero, 170 F.3d 396, 399, 403-04 (3d Cir. 1999); *Poritz*, 662 A.2d at 409.

149. *See* A.A. v. New Jersey, 341 F.3d 206, 212, 214 (3d Cir. 2003) (holding that (1) sex offenders' right of privacy in their home addresses gave way to the state's compelling interest to prevent sex offenses, (2) the state's internet publication of their home addresses did not violate offenders' constitutional privacy rights, and (3) the state's compilation of information on them, including offenders' names, ages, race, birth date, height, weight, and hair color, did not violate offenders' constitutional right to privacy).

150. *See, e.g.*, Trans Union Corp. v. FTC, 267 F.3d 1138, 1140, 1143 (D.C. Cir. 2001) (lists that contain only names and addresses carry significance because of context).

disclosure.[151] Others, by contrast, recommend that records custodians be given discretion to deny access when there is clear evidence of the substantial likelihood of harm or threat resulting from the disclosure of personal information.[152]

There has been a split in the circuits on this issue. The Tenth Circuit has held that "the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals. . . ."[153] The District of Columbia Circuit came out the other way on a very similar issue, holding that the government may restrict disclosure of people's names and addresses in spite of a corporation's First Amendment claim of entitlement to the information.[154]

However, even under a "clear evidence of substantial likelihood of harm" standard, home address information has a constitutional dimension. In *Kallstrom v. City of Columbus*, for example, the defense attorney for forty-one defendants charged with drug conspiracy sought the names and addresses from the personnel files of the police officers involved in the arrests.[155] The court held that release of the information invaded the police officers' privacy because it exposed them to a substantial risk of harm.[156] Not only did it implicate their fundamental interest in personal safety, it also violated their constitutional rights.[157] "The City's release of private information . . . rises to constitutional dimensions by threatening the personal security and bodily integrity of the officers and their family members. . . ."[158] The information extended beyond addresses; however, the court's reasoning suggests that the primary concern giving rise to the privacy interest was the officers' safety, and it is the address information that was central to these safety concerns.[159]

The purpose of open government records statutes is to shed light on the operations of government agencies, not to publish information about individuals.[160] Government agencies should not publish home addresses if the effect of the disclosure would be solely to disclose personal information about an individual, especially if the disclosure would shed no light on the conduct of

151. *See, e.g.*, CAL. GOV'T CODE § 6254.21 (2003) (banning the posting of the home address or telephone number of any elected or appointed official); WIS. STAT. ANN. § 19.33 (2003) (making an elected official the custodian of his or her records).

152. *See, e.g*, WIS. STAT. ANN. § 19.35 (2003).

153. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999).

154. Trans Union Corp. v. FTC, 245 F.3d 809, 818 (D.C. Cir. 2001).

155. 136 F.3d 1055, 1059 (6th Cir. 1998).

156. *Id*. at 1069.

157. *Id*. at 1069-70.

158. *Id*. at 1064. For additional information on the public disclosure of the personal information of police officers, see Adam Liptak, *A Web Site Causes Unease in Police: Its Creator Posts Personal Data on Officers in Washington State*, N.Y. TIMES, Jul. 12, 2003, at A12.

159. *Kallstrom*, 136 F.3d at 1059, 1067.

160. *See* Dep't of the Air Force v. Rose, 425 U.S. 352, 372 (1976).

a public agency or official or on other governmental matters of significance to the public.[161] Instead of creating castes in society, where some groups of people get special treatment, there should be categories of records that are accessible and non-accessible. The safety of one group of people is no more important than that of another group.

ii. Other Confidential Information. Home address information illustrates a wider debate about the extent to which state actors should disclose information about citizens pursuant to open government records requests. Other data items may deserve confidential treatment as well, even if no specific statute were to speak to the specific datum.[162] It would violate the public interest in privacy if state and local government agencies were to disclose information to the public that would otherwise be unobtainable. Especially serious are examples of government records that contain sensitive information. For example, municipal recreation department records often include children's records, which may contain birth dates, emergency phone numbers, and medical conditions.

Generally, the public should not have access to government records if the primary effect of the disclosure would be the dissemination of sensitive personal information about a particular private person, rather than shedding light on the conduct of a government agency or official or on other matters of significance to the public.[163]

161. *See* L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32 (1999). This case involved a First Amendment challenge to a California statute that limited public access to the home address of people who had been arrested. *Id*. at 34, 36. The statute allowed access for "scholarly, journalistic, political, or governmental purpose, or . . . for investigation purposes," but prohibited access that would be used for commercial purposes. *Id*. at 34-35. In the course of holding that the statute was not subject to facial challenge, and remanding for further proceedings, the Court noted that the state "could decide not to give out arrestee information at all without violating the First Amendment." *Id*. at 40. *See also* Mainstream Mktg. Serv. v. FTC, 358 F.3d 1228, 1246 (10th Cir. 2004) (upholding Do Not Call list against a First Amendment challenge); Missouri *ex rel.* Nixon v. American Blast Fax, Inc., 323 F.3d 649, 660 (8th Cir. 2003) (upholding restrictions on junk faxes against First Amendment challenge).

162. *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457-58 (1977) (holding that the president had a constitutionally-protected privacy interest in the records containing his private communications with his family).

163. The common law of "invasion of privacy" informs, to some extent, the public interest in privacy. According to American Jurisprudence, "[t]he right of privacy is not infringed by the publication of matters of public record." 62A AM. JUR. 2d *Public Records* § 107 (2005). Under open government records statutes, however, it is the government, rather than commercial enterprise, disclosing information about individuals. *See*, *e.g.*, WIS. STAT. ANN. § 19.35 (2003). This makes a difference. Most states have adopted a system of categorizing four different kinds of invasions of privacy. The four torts are: (1) "unreasonable publicity" of "private life," (2) "intrusion," such as hidden videotape cameras, (3) "appropriation," such as the commercial use of someone's name, image, or likeness, and (4) "false light" publicity that places someone in a false light in the public eye. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

iii. No Sanctions for Reporting Information the Government Has Published. It is well established that the government may not impose sanctions for re-publication of information that has been obtained through governmental channels. The Supreme Court has repeatedly struck down a number of statutes that prohibited the disclosure of information obtained from government records. *Cox Broadcasting v. Cohn* established that a state may not sanction the press for publishing true information that has been disclosed in public court documents.[164] *Oklahoma Publishing Co. v. Oklahoma County District Court*, held that the state could not prohibit the media from disclosing information about a child when the media obtained the information by attending juvenile court proceedings.[165] In *Smith v. Daily Mail Publishing Co.*, the Court struck down a statute prohibiting the publication of names of juvenile offenders, saying "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.[166]This principle was reiterated in *Florida Star v. B.J.F.*, where a newspaper published the name of a rape victim, which it obtained from a police report.[167] "We hold only that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order . . . ."[168]

These cases support the proposition that once the government makes information public, the government cannot subsequently sanction its further disclosure. However, the cases do *not* establish that the government has an obligation to disclose the information in the first instance. Indeed, in *Cox Broadcasting*, the Court noted that it was not reaching "any constitutional questions which might arise from a state policy not allowing access by the public and press to various kinds of official records . . . ."[169]

There is an important distinction between conditions that might be placed on government records before they are disclosed, and restrictions or sanctions that are imposed after access has already been obtained.[170] The First Amendment prohibits the state from placing post-access restrictions on disclosure, but it does not compel the state to disclose all records in the government's files.[171]

164. 420 U.S. 469, 495-96 (1975).

165. 430 U.S. 308, 311-12 (1977).

166. 443 U.S. 97, 98-99, 103 (1979).

167. 491 U.S. 524, 526 (1989).

168. *Id*. at 541.

169. 420 U.S. at 496 n.26.

170. *See generally* Solove, *supra* note 1 (providing a full analysis of the jurisprudence of "unconstitutional conditions" as they attach to government records).

171. *See supra* notes 165-70 and accompanying text.

Indeed, government agencies, including local governments, may be exposed to lawsuits if the agencies violate the constitution.[172] If public agencies were to disclose personal information, such as home addresses, under all circumstances, they could become subject to constitutional challenges that they may or may not win. The better course is to empower public agencies to comply with requests for government records and still protect individual privacy.

iv. Data Accuracy. A common rationale for collecting information about citizens from government records is that the government data is used for verification, to enhance the quality and accuracy of the data in commercial databases. The first known sampling, however, of individuals' records compiled by two large data aggregators, ChoicePoint and Acxiom, found significant inaccuracy rates in personal data.[173]

The study, organized by Privacy Activism, was based on eleven volunteers, who ordered their "ChoicePoint ScreenNow" background checks, which cost $20 each, and their Acxiom background reports, which cost $5.[174] They found that 100 percent of the ChoicePoint records had at least one error.[175] Over one-third of the eleven participants never received their Acxiom reports, and 67% of the reports received had errors.[176]

ChoicePoint claims to have 17 billion records on individuals and businesses, and sells data to 40 percent of the nation's top 1,000 companies.[177] It also has contracts with major U.S. law enforcement and homeland security agencies.[178] Its overall error rate was 35 percent.[179] Acxiom, another aggregator, primarily serves the financial services industry.[180] Companies can submit rosters of their customers to Acxiom, which can then provide

172. *See, e.g.*, Kallstrom v. City of Columbus, 136 F.3d 1055, 1059 (6th Cir. 1998) (holding that the Fourteenth Amendment prohibits the City of Columbus from disclosing certain personal information contained in police officers' personnel files).

173. *See* LINDA ACKERMAN & DEBORAH PIERCE, PRIVACY ACTIVISM, DATA AGGREGATORS: A STUDY OF DATA QUALITY AND RESPONSIVENESS 1 (2005), http://www.privacyactivism.org/docs/DataAggregatorsStudy.pdf. *See e.g.*, Houston Chronicle Publ'g Co. v. City of Houston, 531 S.W.2d 177, 188 (Tex. Civ. App. 1975) (finding that no effort was made to purge inaccurate or misleading entries on the "rap sheet" in question).

174. ACKERMAN & PIERCE, *supra* note 174, at 2-4.

175. *Id*. at 1.

176. *Id*. at 1, 7.

177. ROBERT O'HARROW, JR., NO PLACE TO HIDE 145 (2005); ChoicePoint Annual Meeting of Shareholders, ChoicePoint, http://www.choicepoint.net/choicepoint/news/feature042903.html (last visited Oct. 2, 2005).

178. O'HARROW, *supra* note 178, at 156.

179. ACKERMAN & PIERCE, *supra* note 174, at 5.

180. 2005 ANNUAL REPORT, ACXIOM CORP. 4 (2005), *available at* http://www.acxiom.com/AppFiles/Download18/2005_Annual_Report-3BFCD5AD-85A1-45ED-A106-AFC876B81142.pdf.

customers' telephone numbers and data on home ownership or estimated income.[181] Acxiom's error rate was 13 percent.[182]

The authors of the study acknowledged its limitations.[183] "It is important to note that due to the small size of the data set, and the non-random distribution of participants, care should be taken in projecting this data to the full population. As participants in the FTC Round-table noted, a detailed national study would be extremely difficult and expensive, and so it is worthwhile beginning with smaller studies such as this."[184]

However, they said their findings could indicate a larger problem.

> The results from the study strongly imply a high rate of serious errors in the information provided by two of the largest data brokers in the United States, as well as a lack of responsiveness to consumers requesting their own information. While the small sample size means we do not consider these results definitive, the figures unequivocally point to a need for a much larger study.[185]

B. Court Records

Court records provide another mother lode of information with commercial value. They are being mined electronically and on paper to obtain information about individuals, for purposes totally unrelated to the reasons the information first landed in the courthouse.[186] As with open government records statutes, the reasons for keeping records open to the public have more to do with supporting our democratic system of government than with the individuals whose records are in the system.

This may seem paradoxical at first glance. Court records have long been presumed open to the public, and the tradition of public access to court case files is rooted in constitutional principles.[187] Upon examination and reflection,

181. O'HARROW, *supra* note 178, at 49-52.

182. ACKERMAN & PIERCE, *supra* note 174, at 5.

183. *Id.* at 2, 5.

184. *Id*. at 5.

185. *Id*. at 8.

186. Beth Givens, *Public Records on the Internet: The Privacy Dilemma*, PRIVACY RIGHTS CLEARINGHOUSE 4, *available at* http://www.cfp2002.org/proceedings/proceedings/givens.pdf.

187. *See* Nixon v. Warner Commc'n, Inc, 98 S. Ct. 1306, 1312 (1978) ("It is clear that courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents."); Soc'y of Prof'l Journalists v. Briggs, 675 F. Supp 1308, 1309 (D. Utah 1987) (acknowledging a constitutional right to access public documents based on *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 583-84 (1980), which stated that the First Amendment is based on access to information and *Press- Enterprise Co. v. Superior Court*, 464 U.S. 501, 518 (1984), which stated "a claim to access cannot succeed unless access makes a positive contribution to this process of self-governance").

however, it is apparent that, as with open government records, the question of what is "public" should be the beginning rather than the end of the analysis.[188]

i. Court Records Are Open to the Public Not Because They Are "Newsworthy," But for the Purpose of Keeping the System Honest. The presumption of public access to court records allows the citizenry to monitor the functioning of our courts, thereby insuring quality, honesty, and respect for our legal system.[189] But it does not follow that every piece of personal information contained within a "public" record in the courthouse needs to be published worldwide on the Internet. Publication of court records should be tailored to serve the court's proper civic purposes, not to broadcast personally identifiable information like Social Security numbers.

The reasons for keeping court records open to the public are several, reflecting the balance of powers among the branches of government and civic principles of government based upon the rights and duties of the individual.[190] For example, in criminal cases, open trials prevent prosecutorial misconduct.[191] A very important aspect of criminal law in this country is the principle of holding law enforcement to its burden of proof.[192] The executive branch, in the person of the prosecutor, is obliged not merely to conduct zealous prosecutions, but to serve the broader interests of justice.[193] Criminal courts are open, therefore, in part to ensure that prosecutorial zeal is checked by rigorous legal standards.

In civil cases, court proceedings are open to the public for a number of reasons. Before damages are awarded, injunctions enforced, or money transferred from one pocket to another, our system demands that the process of adjudication be exposed to scrutiny.

The reasons for keeping the system open to the public have to do with the health and well-being of our legal system, not for the benefit of consumer

188. "Mere speculation about hypothetical public benefits cannot outweigh a demonstrably significant invasion of privacy." U.S. Dep't. of State v. Ray, 502 U.S. 164, 179 (1991). The Supreme Court emphasized in Ray that the disclosure of a list of names pursuant to a FOIA request was not inherently or always a threat to privacy, but "depends upon the characteristics revealed by virtue of being on the particular list, and the consequences likely to ensue." *Id.* at 176 n.12 (quoting Nat'l Ass'n of Retired Fed. Employees v. Horner, 879 F.2d 873, 877 (1989)).

189. *See* Richmond Newspapers v. Virginia, 448 U.S. 555, 575-77 (finding that the First Amendment right of access to criminal trials is predicated on openness, fairness, perception, and confidence in governmental process).

190. *See* Solove, *supra* note 1, at 1173 (listing four functions of government transparency).

191. *See Richmond Newspapers*, 448 U.S. at 569 (stating that open trials assure that proceedings are conducted fairly and discourage perjury and misconduct).

192. *See* U.S. v. Gooding, 25 U.S. 460, 461 (1827) ("In criminal proceedings, the *onus probandi* rests upon the prosecutor, unless a different provision is expressly made by statute.").

193. 27 C.J.S. *District and Prosecuting Attorneys* § 29 (1999) (discussing prosecutorial duties).

profiling or other commercial interests.[194] The Constitution provides for jury trials not only to determine questions of fact, but also to make the community an integral part of the judicial system.[195] Open court records similarly serve an important educational function: not to titillate the masses with news of their neighbors' misfortunes, but to support a functioning democracy.[196] Government records empower citizens to make good political decisions. Court records publish final judgments and liens, facilitating business, and personal and legal affairs.[197]

ii. The Legal System Is Not About the Litigants, but About Self-Government. It is tempting to think that the American court system revolves around the litigants, *i.e.*, the plaintiff and defendant. To the contrary, the jury trial right guaranteed by the Seventh Amendment (civil trials) forms an important part of the American system of self-government.[198]

The core interest underlying the American judicial system is not the interest of the parties, but of the citizens - the jurors and the gallery - who monitor the judges, the witnesses, the prosecutors, the police and the lawyers. Open public trials give the public an opportunity to deter corruption in the system.

> The institution of the jury . . . places the real direction of society in the hands of the governed . . . . . and not in that of the government. . . . . [It] invests the people, or that class of citizens, with the direction of society.
>
> . . . The jury system as it is understood in America appears to me to be as direct and as extreme a consequence of the sovereignty of the people as

194. *See* Globe Newspaper Co. v. Superior Court of Norfolk, 457 U.S. 596, 606 (1982) ("[T]he right of access to criminal trials plays a particularly significant role in the functioning of the judicial process and the government as a whole. Public scrutiny of a criminal trial enhances the quality and safeguards the integrity of the factfinding process, with benefits to both the defendant and to society as a whole."); Neb. Press Ass'n v. Stuart, 427 U.S. 539, 587 (1976) ("[F]ree and robust reporting, criticism, and debate can contribute to public understanding of the rule of law and to comprehension of the functioning of the entire criminal justice system, as well as improve the quality of that system by subjecting it to the cleansing effects of exposure and public accountability.").

195. *See* Gannett Co., Inc. v. DePasquale, 443 U.S. 368, 428 (1979).

196. *Id*. at 429; Anne-Marie Moyes, Note, *Assessing the Risk of Executing the Innocent: A Case for Allowing Access to Physical Evidence for Posthumous DNA Testing*, 55 VAND. L. REV. 953, 986 (2002).

197. John L. McCormack, *Torrens and Recording: Land Title Assurance in the Computer Age*, 18 WM. MITCHELL L. REV. 61, 124 (1992).

198. *See* Edith Guild Henderson, *The Background of the Seventh Amendment*, 80 HARV. L. REV. 289, 295 (1966) (stating that the Seventh Amendment concerning jury trials in civil cases was a principal Antifederalist demand); Charles W. Wolfram, *The Constitutional History of the Seventh Amendment*, 57 MINN. L. REV. 639, 667-669, 678 (1973) (explaining that the Seventh Amendment was a reaction to the powerful government established by the Constitution, and antifederalists sought to protect debtors and litigants from oppressive judges).

> universal suffrage. They are two instruments of equal power, which contribute to the supremacy of the majority.[199]

For this reason, African-Americans and women have struggled for the right to serve on juries, not for the benefit of the parties, but for the sake of being part of the system.[200] The infusion of these groups' knowledge into the system also serves the overarching social purpose of protecting the innocent from erroneous verdicts of liability.[201]

Traditionally, documents that make it through the courthouse door become part of the public record and open to scrutiny. However, this tradition was not intended for the purpose of broadcasting details about the litigants.[202] Government records are made available to the public so that citizens can make political decisions, to instill confidence in the system, to make the government accountable, and to facilitate business, personal and legal affairs.[203]

iii. The Legal System is Not So Much About a "Search for Truth" As About Resolving Conflicts. Very few "facts" are proved to a conclusion in the American system. Only a fraction of lawsuits actually proceed to trial.[204] This means that most of the "facts" recited in pleadings are not tested. Moreover, there is a certain amount of "puffing" that goes into pleadings.[205] If they are disseminated over the Internet, and especially if they are "newsworthy," there are no guarantees whatever that any of the information on the Internet will be reliable. This lack of reliability stands to undermine the perception of fairness and trust in the legal system.

199. ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 293-94 (1945); *see also Gannett*, 443 U.S. at 428-29 (Blackmun, J., concurring and dissenting) (finding that the public should be educated about the manner in which criminal justice is administered); Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002) ("Democracies die behind closed doors.").

200. Nancy S. Marder, *Introduction to the Jury at a Crossroad: The American Experience*, 78 CHI.-KENT L. REV. 909, 921 (2003).

201. *See* Batson v. Kentucky, 476 U.S. 79, 85-87 (1986).

202. For this reason, discovery is not conducted in public domain, but in confidence. Indeed, the government has a substantial interest in controlling and preventing discovery abuse. *See* Rhinehart v. Seattle Times Co., 654 P.2d 673, 690 (Wash. 1982); *see also* Wilk v. Am. Med. Ass'n, 635 F.2d 1295, 1300-01 (7th Cir. 1981) (suggesting a party would not be entitled to a hearing if it brought suit solely to obtain discovery material); Hammock v. Hoffman LaRoche, Inc., 662 A.2d 546, 558 (N.J. 1995) (finding that the public interest in health and welfare may be invoked to prevent abuse of discovery for commercial gain or competitive advantage).

203. Robert Gellman, *Public Records – Access, Privacy, and Public Policy: A Discussion Paper*, 12 GOV'T INFO. Q., 391, 395 (1995).

204. STEPHAN LANDSMAN, THE ADVERSARY SYSTEM: A DESCRIPTION AND DEFENSE 29 (1984).

205. R.J. Gerber, *Victory vs. Truth: The Adversary System and Its Ethics*, 19 ARIZ. ST. L.J. 3, 7 (1987).

Part of this hazard is the nature of the American adversary system.[206] The primary objective of the adversary system is not so much to seek material truth as to resolve disputes in a way that will be acceptable to the parties and to society. If the search for truth were supreme, privileges would not be recognized, and the vast majority of cases would not be resolved on consent.

The difficulty with publishing every data item that comes into the courthouse is that although it would preserve the principle that judicial proceedings should be conducted in public, there is a substantial risk that over-publication will have a chilling effect. When people lose control over information about themselves, they change their behavior in ways that may harm society.[207] The judiciary has recognized this; there is ample precedent for limiting disclosure when a chilling effect looms over litigants.[208] The subpoena power, for example, can easily be used to destroy privacy and confidentiality, hence there are clearly defined restrictions and limitations on its use.[209]

If litigants, jurors, and witnesses lose control over confidential information about themselves, they will similarly adopt privacy-protective behaviors, most likely by refusing to participate in the justice system. This raises a significant risk to public confidence in the court system and to our functioning democracy.

iv. Much of the System is Secret, While Individuals Are Exposed. Personal information about individuals is a valuable commodity in the United States, where large commercial data aggregation companies sell Social Security numbers[210] and create consumer profiles for profit.[211] These companies, like

206. LANDSMAN, *supra* note 205, at 13 (finding that the adversary system evolved with the development of the jury system).

207. *See infra* notes 259-62 and accompanying text.

208. *See, e.g.*, *In re* New York Times Co., 828 F.2d 110, 114 (2nd Cir. 1987); Gaull v. Wyeth Labs. 687 F. Supp 77, 83 (S.D.N.Y. 1988); Kitzmiller v. Dover Area School Dist., 379 F. Supp. 2d 680, 689 (M.D. Penn. 2005).

209. Privileges are recognized where four conditions are met: 1) communications originates in confidence, 2) confidentiality is essential for the relationship, 3) the relationship is fostered in the community, and 4) injury from disclosure outweighs the benefit. 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2285 at 527 (1961) (citing Falsone v. U.S., 205 F.2d 734 (5th Cir. 1953); U.S. v. Funk, 84 F. Supp 967 (E.D. Ky. 1949); O'Toole v. Ohio G.F. Ins. Co., 123 N.W. 795 (Mich. 1909); Baskerville v. Baskerville, 75 N.W.2d 762 (Minn. 1956)).

210. *See, e.g.*, U.S. GENERAL ACCOUNTING OFFICE, SOCIAL SECURITY NUMBERS: PRIVATE SECTOR ENTITIES ROUTINELY OBTAIN AND USE SSNS, AND LAWS LIMIT THE DISCLOSURE OF THIS INFORMATION (2004), http://www.gao.gov/new.items/d0411.pdf [hereinafter GAO REPORT, SOCIAL SECURITY NUMBERS].

211. In Europe, by contrast, information privacy is protected by law. *See* Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/documentprint/0,2744,en_2649_201185_1815186_1_1_1_1,00.html (last visited Jan. 29, 2006).

ChoicePoint and Reed Elsevier, work very hard to extract personal information about people from court records.[212]

Meanwhile, much information about the judicial system itself remains secret. For example, the courts operate with public money, but decisions as to the allocation of budget monies are made in secret.[213] These decisions affect the public, but the public is not informed as to how or why they are made. State courts offer many programs affecting the operation of the judicial system, such as mediation, arbitration, child custody, and pretrial intervention.[214] "All of these programs cost time and money, and affect court personnel, litigants, lawyers and the public."[215] They are adopted in a process that is not publicized.[216] Thus, individuals are exposed to scrutiny, while much of the system itself remains secret.

v. *Courthouse Data Generates Profits for Data Aggregators While Potentially Harming Individuals.* Civil cases are filed because litigants have failed to reach a private compromise. This fact does not transform the litigants' pleadings, or evidence submitted with motion practice, into a commodity that should be public for any and all purposes. Inaccuracies spawn statistics and perceptions that are incorrect.

The judiciary has been wary of discovery abuse for commercial gain (or competitive advantage), and its concerns should extend to other aspects of administering justice.[217] Unhindered access to case files may result in a further increase in identity theft. Marketers may take advantage of compiled records to target advertising at former litigants and witnesses. Personal information that is disclosed for the purposes of litigation could unfairly stigmatize a litigant in his or her future pursuit of employment or educational opportunities.[218]

212. *See* Electronic Privacy Information Center, ChoicePoint, http://www.epic.org/privacy/choicepoint/ (last visited Jan. 29, 2006) (listing ChoicePoint as a company that sells information and listing Reed Elsevier as a "private sector data seller" along with ChoicePoint, Experian, Polk, Seisint and Acxiom).

213. Martin L. Haines, *Privacy in the Courts v. the Public Right to Know*, N.J. LAW., Feb. 2002, at 37.

214. *See, e.g.*, *id.* at 39 (discussing New Jersey).

215. *Id.*

216. Although Judge Haines argues that all of the programs are adopted in a process involving extensive unwritten reports, the author disagrees with this statement and believes instead that many, but not all programs are adopted in such a way. *See id.*

217. Security is also an important aspect of electronic access to court files, as electronic files can be hacked, modified, stolen and misused. *See* Michael Whiteman, *Appellate Court Briefs on the Web: Electronic Dynamos or Legal Quagmire?*, 97 L. LIBR. J. 467, 476-78 (2005) (discussing various privacy concerns related to electronic filing).

218. *See* Illinois v. Rodriguez, 497 U.S. 177, 181-82 (1990) (showing that the fact that information has been disclosed to one individual does not mean that it can be freely disclosed to another – a guest in somebody's home cannot open the door to the police to conduct a search).

vi. To Say "Public is Public" Is Too Simplistic. Just because a piece of information is in a "public record" 'does not mean it can be published for any purpose. The U.S. Supreme Court explained this at length in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.[219] "[There is a] privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public."[220] One need not maintain perfect secrecy in order to maintain a degree of confidentiality. "[T]he fact that an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[221]

The inherent difficulty of obtaining and distributing paper files used to effectively insulate individuals from the harm that could result from misuse of information in government records. The Court referred to the relative difficulty of gathering paper files as "practical obscurity," and recognized that it influenced the privacy equation.[222] "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a [government-created] computerized summary located in a single clearinghouse of information."[223]

It is overly simplistic to say that "public records are public records." As discussed above, court records are not public because of any inherent characteristics; they are public for reasons that have to do with our system of self-government. Moreover, electronic records have attributes that fundamentally change the premises for categorizing information as "public."" The judiciary should resist the temptation to rely on oversimplified arguments that once a document can be found in the public domain it can no longer be considered private.[224] Instead, the courts should consider afresh the reasons for making court records public and draw a distinction among the kinds of documents that should be made available online.

> Litigants do not give up their privacy rights simply because they have walked, voluntarily or involuntarily, through the courthouse door. . . . The mere payment of a filing fee entitles a plaintiff to compel production of intensely personal and confidential information, such as medical records, marital information, religious documents, financial records, and even trade secrets or

219. 489 U.S. 749 (1989).

220. *Id.* at 767.

221. *Id.* at 770.

222. *Id.* at 762.

223. *Id.* at 764.

224. The government may not impose sanctions for publishing information the government itself has already placed in the public domain, but it has no affirmative obligation to publish personally identifiable information about citizens. *See supra* notes 104-09 and accompanying text.

> intellectual property. The defendant, of course, can respond in kind. The loss of privacy through litigation is compounded when the information is disclosed to the media, competitors, political adversaries, and even curious members of the public.[225]

This makes the courts and other state actors the guardians of a "public interest in privacy."" The government has a duty to protect its citizens from incursions upon their privacy interests. Instead, however, the distinction between governmental and commercial interests is fading. Government records are being used to build commercial databases, and governments are purchasing commercial databases, apparently for the purpose of building dossiers on citizens.

IV. IMPLICATIONS FOR CIVIL LIBERTIES

Commercial databases are having an increasing impact on civil liberties, and several recent governmental initiatives have sought to exploit private-sector databases to monitor both legal and illegal activity. As a result, federal statutes have been eviscerated, civil rights compromised, and constitutional protections weakened.

A. The Distinction Between Governmental and Commercial Databases

A current myth about information privacy is that a meaningful distinction can be drawn between governmental and commercial databases. The myth is pervasive for two reasons: 1) we have internalized the metaphor of Big Brother as a governmental entity; and 2) the word "private" sometimes means "non-governmental" (as in "private sector").[226] In reality, however, the distinction is softening, with significant implications for the privacy interests of individuals.[227]

i. Commercial Databases Are Being Used to Eviscerate Statutory Protections. The federal government is using commercial databases to bypass statutory requirements. For example, commercial databases are being used to circumvent the Privacy Act.[228] Federal agencies purchase databases from

225. Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 466 (1991).

226. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHIL. 559, 567-69 (1998).

227. As the Government Accountability Office recently reported, "many federal data mining efforts involve the use of personal information that is mined from databases maintained by public as well as private sector organizations." U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES (2004), *available at* http://www.gao.gov/new.items/d04548.pdf.

228. SENATE MAJORITY TASK FORCE ON THE INVASION OF PRIVACY, NY. SENATE EXECUTIVE SUMMARY 9 (Mar. 2000), http://www.senate.state.ny/Docs/nyspriv00.pdf; 5 U.S.C. § 552a (2004).

companies like ChoicePoint, Dun & Bradstreet, and Lexis Nexis.[229] Commercial airlines have admitted disclosing the travel records of millions of passengers.[230] As noted in *USA Today*, "JetBlue provided the records of 1.1 million passengers to a private company working on an Army security project. By matching the data to Social Security numbers and addresses, the contractor could create detailed dossiers for a controversial air-travel-security plan it was promoting."[231] JetBlue publicly apologized, but even still *USA Today* called the Privacy Act "too porous to protect today's citizens."[232]

The Department of Defense and a private contractor have been building an extensive database of 30 million 16-to-25-year-olds, apparently in violation of the Privacy Act, "which requires that government agencies accept public comment before new records systems are created."[233] The database, which has been in development since 2002, combines names with Social Security numbers, grade-point averages, e-mail addresses, and phone numbers.[234] The Army has acknowledged it has been struggling to meet recruitment goals to replenish the ranks of the all-volunteer services.[235] The Pentagon purchased the names of 3.1 million high school graduating seniors and an additional 4.7 million college students.[236] Drawing information from motor vehicle records, Selective Service registrations and private vendors, the database includes a variety of personal information, including grades, height, weight, and social security numbers.[237]

The Fair Credit Reporting Act ("FCRA"), has been similarly compromised. For example, FCRA provides that records of bankruptcies may be expunged after 10 years.[238] Now that bankruptcy filings are routinely published on the Internet, commercial entities can download and keep the

229. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 600-07 (2004).

230. *1974 Privacy Act Too Porous to Protect Today's Citizens*, USA TODAY, Sept. 29, 2003, at 22A.

231. *Id.*

232. *See id.*

233. Damien Cave, *Age 16 to 25? The Pentagon Has Your Number, and More*, N. Y. TIMES, Jun. 24, 2005, at A18.

234. *Id.* The Joint Advertising and Market Research Studies (JAMRS) recruiting database was established "to provide a single central facility within the Department of Defense to compile, process and distribute files of individuals who meet age and minimum school requirements for military service." Privacy Act of 1974; System of Records, 70 Fed. Reg. 29,486 (May 23, 2005).

235. Cave, *supra* note 234, at A18.

236. *Id.*

237. *Id.* A Department of Defense spokesman explained that "Congress does not want conscription, the country does not want conscription. If we don't want conscription, you have to give the Department of Defense, the military services, an avenue to contact young people to tell them what is being offered." *Id.*

238. 15 U.S.C. § 1681c(a)(1) (2005).

bankruptcy records indefinitely in their proprietary databases.[239] Unless individuals somehow acquire a statutory right to review, correct, and expunge their records, there will be no practical way to clear one's name and credit rating - ever.

ii. Commercial Databases Are Being Used to Violate Civil Rights. State actors have used commercial databases for purposes that have harmed and threaten to harm civil rights such as voting rights,[240] the right to travel,[241] and the right to associate.[242] Thousands of citizens were erroneously deleted from the lists of registered voters in the November 2000 election, when the State of Florida purchased records from ChoicePoint to purge the voter rolls of convicted felons.[243] The data were inaccurate, and the disenfranchised voters had no recourse.

The right to travel will be affected by "Secure Flight," a program implemented by the Transportation Security Agency ("TSA").[244] The purpose of Secure Flight is to match airline passengers against lists of suspected terrorists.[245] In July 2005, however, the Government Accountability Office

239. *See* Letter from Tena Fiery, Research Director of Privacy Rights Clearinghouse, Beth Givens, Director of Privacy Rights Clearinghouse, & Deborah Pierce, Staff Attorney of Electronic Frontier Foundation, to Leander Barnhill, Office of General Counsel of the Executive Office for United States Trustees (Sept. 18, 2000), *available at* http://www.privacyrights.org/ar/bankruptcy091800.htm.

240. *See infra* notes 244-245 and accompanying text.

241. *See* Kent v. Dulles, 357 U.S. 116, 125-26 (1958). The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. *See* Saenz v. Roe, 526 U.S. 489, 500 (1999).

> The right to travel is a part of the "liberty" of which the citizen cannot be deprived without the due process of law under the Fifth Amendment. . . . Freedom of movement across frontiers in either direction, and inside frontiers as well, was a part of our heritage. Travel abroad, like travel within the country, may be necessary for a livelihood. It may be as close to the heart of the individual as the choice of what he eats, or wears, or reads. Freedom of movement is basic in our scheme of values. . . . "Our nation," wrote Chafee, "has thrived on the principle that, outside areas of plainly harmful conduct, every American is left to shape his own life as he thinks best, do what he pleases, go where he pleases."

Kent, 357 U.S. at 125-26.

242. *See, e.g.*, NAACP v. Alabama, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.").

243. Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A6.

244. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, AVIATION SECURITY: SECURE FLIGHT DEVELOPMENT AND TESTING UNDER WAY, BUT RISKS SHOULD BE MANAGED AS SYSTEM IS FURTHER DEVELOPED (2005), *available at* http://www.gao.gov/new.items/d05356.pdf.

245. *See* Letter from Cathleen A. Berrick, Director of Homeland Security and Justice Issues, & Linda D. Koontz, Director of Information management Issues to Congressional Committees 1

reported that TSA was using commercial data from corporations to compile dossiers on passengers, in order to give them a "risk score."[246] This score in theory would determine a prospective passenger's "risk" to airline safety by analyzing their credit rating, how recently they moved, what kind of job they had, and other data.[247] The Government Accountability Office reported that TSA violated the Privacy Act; TSA did not disclose its use of personal information drawn from commercial sources or give the public an opportunity to comment.[248] Indeed, TSA's contractor "collected more than 100 million commercial data records containing personal information . . . without informing the public."[249]

These examples illustrate that commercial databases can be used not only to impair the right to vote and the right to interstate travel, but also to create secret government dossiers on individuals. The loss of anonymity can easily be exploited to burden the First Amendment right to free association and other liberty interests.[250]

iii. Commercial Databases Create Dossiers for the Government. The government has unmatched power to centralize all the private sector data that is being generated for commerce. The ACLU recently reported that the Department of Justice

> has an $8 million contract with ChoicePoint that allows government agents to tap into the company's vast database of personal information on individuals. . . . . The Treasury Department runs a database that collects financial information from thousands of banks and other financial

(July 22, 2005), *available at* http://www.gao.gov/new.items/d05864r.pdf (discussing the results of a review of the Secure Flight Program) [hereinafter Berrick & Koontz Letter].

246. *See* Bruce Schneier, *Secrets and Lies in the 'Friendly Skies'*, ALTERNET, Jul. 27, 2005, http://www.alternet.org/rights/23728. *But see* Berrick & Koontz Letter, *supra* note 246, at 5, 7 (stating that TSA gathered the information to test the accuracy of commercial databases).

247. *See* Schneier, *supra* note 247.

248. *See* Berrick & Koontz Letter, *supra* note 246, at 6-7, 9.

249. *Id.* at 2.

250. Anonymity and pen names have a rich history in the United States. "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." Talley v. California, 362 U.S. 60, 64 (1960). The Federalist Papers were published under the fictitious name "Publius," concealing the identities of the true authors, James Madison, Alexander Hamilton and John Jay. The Federalist Papers, http://www.law.ou.edu/hist/federalist/ (last visited Apr. 1, 2006). Mark Twain was the pen name of Samuel Longhorne Clemens, George Eliot of Mary Ann Evans, and Voltaire of Francois Marie Arouet. Voltaire, http://en.wikipedia.org/wiki/Voltaire (last visited Apr. 1, 2006). "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and the First Amendment in particular: to protect unpopular individuals from retaliation – and their ideas from suppression – at the hand of an intolerant society." McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 356 (1995).

> institutions. . . . . .[251] [In addition, the federal Department of Education] maintains an enormous information bank holding . . . . . educational records on individuals stretching from their primary school years through higher education. Under the USA PATRIOT Act, the FBI can force anyone to turn over records on their customers or clients, giving the government unchecked power to rifle through individuals' financial records, medical histories, Internet use, travel patterns, or any other records.[252]

There is little oversight. Over the past 20 years, the Government Accountability Office ("GAO"),[253] congressional committees, and agency Privacy Act officers have regularly criticized the Office of Management and Budget for not living up to its duty as the executive branch's Privacy Act overseer.[254] In a detailed report, the GAO found major inconsistencies among agencies and said guidance was sorely lacking in the area of "electronic records."[255]

iv. The Databases Skew and Corrupt Data with Far-Reaching Implications. When people are afraid their private information will be misused, they resort to behaviors that have an adverse impact on society at large. The clearest example of this is in the health care industry, where medical patients often use deceit in order to protect themselves.[256] One out of every six Americans now engages in some form of privacy-protective behavior.[257] These behaviors include lying to doctors, asking doctors to lie to

251. Jay Stanley & Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society* 8, ACLU, Jan. 2003, http://www.aclu.org/Files/OpenFile.cfm?id=11572.pdf.

252. *See* Simpson, *supra* note 244, at A1 (reporting that executive branch agencies were purchasing "troves of personal data from the private sector," and quoting government sources for the proposition that DOJ, FBI, USMS, INS, and IRS employees had electronic access to citizens' assets, phone numbers, driving records, and other personal information from their desktop computers). The article reported that ChoicePoint, a publicly-held company and its competitors were supplying citizens' personal information to at least thirty-five federal government agencies. *Id.*

253. The Government Accountability Office was "formerly known as the General Accounting Office. *See* GAO Human Capital Reform Act of 2004, Pub. L. No. 108-271, 118 Stat. 811 (2004); GAO's Name Change and Other Provisions of the GAO Human Capital Reform Act of 2004, www.gao.gov/about/namechange.html (last visited Apr. 1, 2006).

254. *See* U.S. GEN. ACCOUNTING OFFICE, PRIVACY ACT: OMB LEADERSHIP NEEDED TO IMPROVE AGENCY COMPLIANCE 7, 14 (2003), *available at* http://www.gao.gov/new.items/d03304.pdf.

255. *See id.* at 25.

256. *See Confidentiality of Patient Records: Testimony Before the Subcomm. on Health of the House Comm. on Ways & Means*, 106th Cong. (2000), *available at* http://waysandmeans.house.gov/legacy.asp?file=legacy/health/106cong/2-17-00/2-17gold.htm (statement of Janlori Goldman, Director, Health Privacy Project, Inst. for Health Care Research & Policy, Georgetown University) [hereinafter Goldman Statement].

257. *Id.* (quoting a 1999 survey conducted by the California Health Care Foundation).

insurance companies, asking doctors to keep two sets of records, paying out-of-pocket for services (especially psychiatric services) that are covered by insurance, and, in the worst cases, refusing to seek treatment at all, lest the patient's health data be misused.[258] The most poignant example of harm is untreated HIV infection.[259] This has a widespread negative impact because public health data become untrustworthy.[260]

Similarly, the Bureau of the Census has encountered resistance to its constitutional mandate because of citizens' privacy concerns.[261] In order to encourage full compliance with requests for demographic information, census data cannot be used for any purpose other than the statistical purpose for which it was collected and cannot be published in any way that would permit identification of an individual.[262]

v. The Owners of Commercial Databases Exercise and Abuse Power Over Individuals. Most individuals have no choice but to participate in commercial databases in order to get basic services in the community. Commercial databases can be used to create an underclass of people who have difficulty getting jobs, cannot get credit, and for whom life is more expensive because of a low credit score.[263] Data mining companies that perform employee background checks keep permanent records of arrests and criminal sentences that cannot be corrected or expunged.[264] In 2002, pharmaceutical giant Eli Lilly fired many employees 'on the grounds they had criminal records, no matter how remote in time or relevance to the employees' current job

258. *See id.*

259. *See* PRINCETON SURVEY RESEARCH ASSOCIATES FOR THE CALIFORNIA HEALTHCARE FOUNDATION, MEDICAL PRIVACY AND CONFIDENTIALITY SURVEY 20-21 (1999), *available at* http://www.chcf.org/documents/ihealth/topline.pdf (noting that 81 out of 100 national survey respondents believed that unique health identifiers would lead people with AIDS to avoid seeking care for fear of being exposed).

260. *See* Goldman Statement, *supra* note 257, at 3.

261. *See* THOMAS S. MAYER, U.S. BUREAU OF THE CENSUS, PRIVACY & CONFIDENTIALITY RESEARCH AND THE U.S. CENSUS BUREAU RECOMMENDATIONS BASED ON A REVIEW OF THE LITERATURE 2 (2002), http://www.census.gov/srd/papers/pdf/rsm2002-01.pdf.

262. *See* 13 U.S.C. § 9 (1997); *Bureau of the Census, Census Confidentiality and Privacy: 1790-2002*, http://www.census.gov/prod/2003pubs/conmono2.pdf.

263. *See* HENDRICKS, *supra* note 41, at 13. For example, a 38-year-old single mother can lose a job as a secretary, based on a shoplifting conviction at age 19. Even if she had the resources to hire counsel to have her conviction expunged from the official court records, she could not remove the black spot from commercial databases. As a consequence, she may have trouble obtaining loans, getting jobs, and renting a domicile. *See supra* notes 39-41 and accompanying text.

264. *See supra* notes 39-40 and accompanying text. Individuals have no right to correct or review information about themselves where the Privacy Act, FOIA and the Fair Credit Reporting Act do not apply. Commercial databases are proprietary. If a commercial enterprise keeps permanent records of arrests and criminal sentences, there exists no practical way for an individual to challenge the records, much less amend or correct them.

responsibilities.[265] Minority groups are disproportionately represented in the vulnerable population of people who have such records.[266]

The Financial Services Modernization Act, better known as Gramm-Leach-Bliley ("GLB"), repealed old Depression-era legislation[267] that prevented banks, brokers, and insurers from exchanging information with each other about their customers.[268] Under the new legislation, these financial institutions may disclose or sell (for profit) their customers' financial information.[269] This information includes checks, account balances, deposits and withdrawals, and the dates, amounts, and recipients of credit card charges. When consumers fill out loan applications, apply for insurance, or purchase securities, they disclose a tremendous amount of information. Financial institutions are now free to share that information with each other and sell it to unrelated third parties.'[270]

Some companies are collecting blood and tissue samples as well as medical information. Genelex, a genetics company in Redmond, Washington, "has amassed 50,000 DNA samples, many gathered surreptitiously for paternity testing."[271] Whether or not the DNA is collected with the individual's knowledge, the data may be "stored without donors' knowledge. Cells banked for one purpose, such as medical diagnosis, have been shared with or sold to other users for research or profit."[272]

vi. Many Commercial Databases Are Created by Involuntary Participation or Coercion to Obtain Basic Commodities and Services. In order to function in society, one must interact with commercial databases. For example, one must carry auto insurance in order to drive a car legally. One's credit score is even more important, not only for borrowing money, but for an increasing

265. Ann Davis, *Zero Tolerance: Employers Dig Deep Into Workers' Pasts, Citing Terrorism Fears*, WALL ST. J., Mar. 12, 2002, at A1.

266. *See* HENDRICKS, *supra* note 41, at 235-46; *see also* RECOMMENDATIONS OF THE MINNESOTA SUPREME COURT ADVISORY COMMITTEE ON RULES OF PUBLIC ACCESS TO RECORDS OF THE JUDICIAL BRANCH, FINAL REPORT, 12-14, June 28, 2004, *available at* http://www.courts.state.mn.us/cio/public_notices/accessreport.htm.

267. The Glass-Steagall Act of 1932; Act of June 16, 1933, ch. 89, 48 Stat. 162.

268. Glass Steagall Act, http://en.wikipedia.org/wiki/Glass-Steagall_Act.

269. 15 U.S.C. § 6801 et. seq. (2000).

270. *See* STANLEY & STEINHARDT, *supra* note 252, at 6. The risks associated with the re-disclosure of financial information are not limited to legal transactions. Banks and other corporations have a duty of care to their customers to ensure their personal data is not misused in the absence of privacy statutes. Such a duty of care is eclipsed, however, by a culture of few constraints on the treatment of personal data. This leaves corporations and law enforcement ill-equipped to respond to abuses of information. *See* Todd R. Weiss, *Scope of Bank Data Theft Grows to 676,000 Customers*, COMPUTERWORLD, May 20, 2005*; see also* BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD (2003).

271. Dana Hawkins, *Keeping Secrets: As DNA Banks Quietly Multiply, Who is Guarding the Safe?*, U.S. NEWS & WORLD REP., Dec. 2, 2002, at 58.

272. *Id.*

number of ordinary transactions. Prospective employers,[273] landlords,[274] and many others look at credit scores. Perhaps the most troubling recent use of the credit score is by insurance companies to establish rates.[275] In short, one's ability to receive even the most basic services can come down to a number: the credit score.[276]

Medical data can show up in your credit report.[277] This "means your banker, after seeing that credit-card payment you made to the local psychiatrist, might decide he would rather not give you a loan."[278] Under Gramm-Leach-Bliley, financial institutions can sell (or give away) this information unless you opt-out.[279]

Consistent with their obligations to protect the public interest in privacy and the constitutional right to information privacy, governmental agencies, including the judiciary, should carefully weigh and consider the definition of "public" for the purposes of publishing personally identifiable information. Not every data item (such as Social Security Number) and not every record (such as records of minor children) need be separately protected by statute in order for state actors to meet these obligations.

B. National ID Cards

A governmental data-collection program with considerable appeal for many is the creation of a national identification card. In the United States, national ID cards have been proposed - and rejected - for years, for a variety of purposes: to streamline government services, to fight tax evasion, to secure borders, and to make health care more affordable.[280] For the purpose of combating terrorism, this hardy perennial has gained considerable support.[281] A major difficulty with respect to terrorism, however, is that no identification system, no matter how sophisticated, can identify terrorists before they commit crimes.

i. National Databases. A national ID card would be the most visible component of a massive verification and tracking infrastructure. The card

273. Jennifer Bayot, *Use of Credit Records Grows in Screening Job Applicants*, N.Y. TIMES, Mar. 28, 2004, § 10, at 1.

274. Motoko Rich, *A Blacklist For Renters*, N.Y. TIMES, Apr. 8, 2004, at F4.

275. Beth Kobliner, *Borrower Beware: Credit Scorers Are Watching*, N.Y. TIMES, Apr. 21, 2002, § 3, at 8.

276. If one's credit score is too low, one will have difficulty getting a job, obtaining a loan, getting a mortgage, renting an apartment.

277. *See* HENDRICKS, *supra* note 41, at 13.

278. *See* Sean Marciniak, *Medical Data Can Show Up in Credit Reports*, WALL ST. J., Aug. 6, 2003, at D2.

279. *Id*.

280. STANLEY & STEINHARDT, *supra* note 252, at 6.

281. *National ID Cards: 5 Reasons Why They Should Be Rejected*, ACLU, Sept. 8, 2003, http://www.aclu.org/news/NewsPrint.cfm?ID=13501&c=39 [hereinafter *National ID Cards*].

itself would be of no use without a database to verify and monitor the movements of millions of individuals.[282] The database would require constant attention to keep it up to date.[283] To make it work, the United States would need a nationwide architecture, so that every airport gate worker and every police officer would have a card-reading device. It is no wonder technology companies have enthusiastically promoted this kind of system; its maintenance would be spectacularly profitable.[284] Whoever creates and maintains the database must build it to the highest levels of data security, including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization.

Even the most efficient and secure system will not protect the United States against terrorism, however. For foreign nationals, for example, the chain of identification begins and ends with their passports.[285] "Breeder" documents like birth certificates and drivers' licenses will determine the quality of the initial enrollment or registration within the system. If a terrorist with a fake passport were to obtain a national ID card, even one with his or her own biometric attached, the most technologically sophisticated database would be worthless.[286]

Even supposing, for the sake of argument, that the United States had flawlessly designed counterfeit-proof cards that could interface through a secure "reader" to a database system that contained only well-verified lawful information on citizens. Assume further that the information on the cards were accessible only to properly authorized civil authorities who would never dream

282. *Privacy vs. Security: Tread Carefully*, BUS. WK., Nov. 5, 2001, at 124.

283. *See National ID Cards*, *supra* note 282.

284. *See* Jeffrey Rosen, *Silicon Valley's Spy Game*, N.Y. TIMES MAG., Apr. 14, 2002, at 48.

285. *See, e.g.*, Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319, 324 (2002). A foreign national's ability to prove legal residence in the United States fundamentally comes down to that individual's passport. If the passport is counterfeit, it may nevertheless be used to obtain a driver's license, Social Security number, and other identification documents.

286. *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 239-40 (Deborah Russell ed., 2000); BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 193 (2003). The cure for the problem of "breeder" documents is not simply to require more of them. *See, e.g.*, Charles C. Mann, *Homeland Insecurity*, THE ATLANTIC MONTHLY, Sept. 2002, at 81-102. Several of the 9-11 hijackers, for example, had valid drivers' licenses, purchased illegally from employees of Virginia's Department of Motor Vehicles. Jerry Markon, *Va. DMV Official Accused in Fraud Probe*, WASH. POST, July 13, 2005, at B5. The Commonwealth of Virginia responded by requiring more paperwork to get a drivers license, but the solution did not fix the problem. Elaine Rivera, *Hardships Cited In Va. License Law*, WASH. POST, May 12, 2004, at B8. An arrest in July 2005 "marked the second time in two years that a Northern Virginia DMV employee was accused of fraudulently selling licenses for cash. A similar scheme two years ago at the DMV . . . led to the guilty pleas of two employees." Markon, *supra*, at B5.

of using the information for any unauthorized purpose. Unless a terrorist was already in the database and had garnered enough suspicion to merit a full database search, no national ID card would stop him or her at the border.

With a national ID card and its corresponding database infrastructure, every glitch in the system would be costly. For example, if you lose a credit card, you can cancel it and get a new one. If you lose a national ID, by contrast, the consequences are much more significant, not just for you, but for those who rely on the database, such as airport security guards and the police, not to mention the technicians who operate the database. Other countries that use national ID cards have found that their usefulness to police has been marginal.[287] Instead of assisting law enforcement, the cards tend to become essential for all dealings with financial institutions, government benefits, securing employment, renting cars, and entering office buildings.[288]

The venerable history of the Social Security Number illustrates the tendency toward "function creep."[289] The Social Security Number originally ensured that workers paid into the system but soon became a prerequisite for taxation and government services, and found its way into private databases as the key to massive amounts of personal data.[290] This tendency imperils even the most innocuous and best-intentioned identification schemes.

For example, a strong argument in favor of national ID cards is their exculpatory value. An airline passenger could simply flash a "trusted traveler" card at the airport and avoid being detained.[291] This would eliminate the inconvenience of having to register with the government, would be spread across all social groups, and would end ethnic profiling because disfavored groups would not be singled out for negative treatment. If they were very

287. *Is National ID Card the Answer?*, DALLAS MORNING NEWS, Nov. 18, 2001, at 3J.

288. *Id.*

289. *See* Richard Cohen, *IDs All Around*, WASH. POST, Oct. 23, 2001, at A23.

290. *See* GAO REPORT, SOCIAL SECURITY NUMBERS, *supra* note 211, at 4.

291. The Orlando Airport is piloting a new pre-screening program called "Clear," which, for $80 a year, will allow travelers to use an exclusive security line with a promise of no random secondary pat-down. Brian Bergstein, *Voluntary Security ID to Debut at Florida Airport*, AIRPORT BUS. ONLINE, June 6, 2005, http://www.airportbusiness.com/article/article.jsp?id=2274&siteSection=4. To get the identification card for this program, travelers must be vetted by the Department of Homeland Security and submit to fingerprint and iris scans. *Id.* According to the "Clear" program website, "Your Membership will be continuously reviewed by TSA's ongoing Security Threat Assessment Process. If your security status changes, your Membership will be immediately deactivated and you will receive a notification email of your status change as well as a refund of the unused portion of your annual enrollment fee." Clear, How Clear Works, http://www.flyclear.com/clear_howclearworks.html (last visited Jan. 3, 2005). Security expert Bruce Schneier ridicules the program: "Think about it. For $80 a year, any potential terrorist can be automatically notified if the Department of Homeland Security is on to him. Such a deal." Bruce Schneier, *News*, CRYPTO-GRAM NEWSL., Aug. 15, 2005, http://www.schneier.com/crypto-gram-0508.html.

reliable, the cards could be used for writing checks, verifying credit cards, and at traffic stops. They would become ubiquitous, but only for privileged segments of society. For practical purposes, the more significant aspect of a national ID system would be its potential to locate and track people, substantially increasing the state's police power and making it easier for the commercial sector to classify individuals into micro-markets.

ii. Real ID. In 2005, Congress adopted a statute popularly known as "Real ID," which would convert one's drivers' license into a national ID card.[292] Every state will be required to issue a uniform drivers' license, which must include not only a variety of personal data but also a digital photograph of the person (enabling face-recognition software) and possibly some other biometric such as fingerprints or iris scans.[293] The personal data collected by any state motor vehicle agency will be accessible to every state and local official, including police officers and to the federal government through the construction of a massive interconnected database of license holders from all 50 states.[294]

The federalized drivers' license must contain a standard "machine readable" element, most likely in the form of an RFID[295] chip or the sort of computer chip found in "smart" credit cards.[296] In practical terms, this means that a single cheap and widely available machine (such as a bar code scanner or RFID reader) will be able to read and store the data on all of the hundreds of millions of drivers' licenses in the country.[297] When a drivers' license is used for any type of identification (including private purchases) it can, and will, be scanned and the data collected.[298] Banks, merchants, and health care providers will ask for the card and harvest the data.[299] Picture, address, date of birth and other data on the license will then be sold to data aggregators like ChoicePoint.[300] This will in turn result in the creation of one or more massive and detailed private databases (in addition to the government database) that will cover virtually every American over the age of 16 and will contain a vast array of information from address and picture to purchasing and lifestyle habits. Consistent with current practice, federal and state agencies will buy access to these private databases, giving government entities easy access to

292. H.R. 418, 109th Cong. §§ 1, 202 (2005); *see also* H.R. 1268, 109th Cong. § 202 (2005).
293. H.R. 418, 109th Cong. § 202(b); H.R. 1268, 109th Cong. § 202(b).
294. *See* H.R. 1268, 109th Cong. § 202(d)(12).
295. RFID is an acronym for "radio frequency identification."
296. H.R. 418, 109th Cong. § 202(b)(9); H.R. 1268, 109th Cong. § 202(b)(9).
297. *See* STANLEY & STEINHARDT, *supra* at note 252, at 12.
298. *See id*. at 12-13.
299. *See id*. at 12.
300. *See id*. at 7.

even more data, far more than they themselves have the statutory authority to collect.[301]

As things stand today, a national ID system promises to provide the worst of both worlds: a system that enables surveillance of the population in general but provides zero increased protection against terrorists.[302]

C. Generalized Surveillance

The public interest in privacy should protect individuals against disclosure by their government of personal information about them. As such, the public interest in privacy imposes certain limits on governmental action. This limitation on governmental power should extend as well to generalized surveillance of the population.

Generalized and passive surveillance can be the condition of life in a tyrannical police state, as memorably portrayed in Orwell's *1984*.[303] It can also be merely the result of gradual desensitization in the United States, where consumer profiling is routine, panoptical television sets are marketed as highly desirable, and people relish the thought of being on television.

The Fourth and Fifth Amendments have never been invoked against generalized and passive surveillance of whole populations.[304] There are criminal penalties and civil remedies for abuses of technology that have

301. *See* STANLEY & STEINHARDT, *supra* at note 252, at 8.

302. Indeed, as currently proposed, a centralized database may do more harm than good to innocents. The FBI published a notice on July 28, 2005, outlining plans to create a records system that would encompass the governments terrorist "watch list" information, operational support records, and records related to complaints or inquiries from individuals. Notice to Establish System of Records, 70 Fed. Reg. 43715 (July 28, 2005). As envisioned, the system will be used to make important determinations about individuals, such as whether they may fly on airplanes, enter the United States, or be arrested. *Id.* The FBI proposes to exempt the system from requirements that agencies maintain only accurate timely, complete, relevant and necessary information about individuals, as mandated by the Privacy Act of 1974. Proposed Rule, 70 Fed. Reg. 43661 (July 28, 2005). Under the FBI's proposed rule, citizens would not be able to access or correct this information, and they will have no judicially enforceable right of redress for negative determinations made on the basis of the system. *Id.* The Department of Justice Inspector General reported in June 2005 that

> Our review of the consolidated watch list identified a variety of issues that contribute to weaknesses in the completeness and accuracy of the data, including variances in the record counts between [two versions of the database], duplicate records, missing or inappropriate handling instructions or categories, missing records, and inconsistencies in identifying information between [the terrorist screening database] and source records.

DEPARTMENT OF JUSTICE, INSPECTOR GENERAL, AUDIT DIVISION, AUDIT REPORT NO. 05-27, REVIEW OF THE TERRORIST SCREENING CENTER CHPT. 7 (June 2005).

303. *See* Nissenbaum, *supra* note 227, at 569.

304. *But see* Laird v. Tatum, 408 U.S. 1, 12-13 (1972) (holding that the First Amendment did not support a challenge to generalized passive surveillance).

become old-fashioned, like wiretapping.[305] However, new surveillance technologies are far less heavy-handed, so they seem less intrusive. Further, they can be adopted incrementally for purposes that, ostensibly at least, are quite benign, and indeed beneficial.

One of the difficulties in mounting legal arguments against group surveillance is the distinction in the United States between the public sector and the private sector. The Constitution places limits only on governmental powers.[306] Accordingly, the Fourth and Fifth Amendments protect against overreaching by the state.[307] When private corporations install cameras and "profile" consumers, few Americans perceive an assault on their rights. We have grown accustomed to the presence of hidden cameras in banks and convenience stores. We have adopted the habit of using surveillance as a means for social control, to maintain order and to create a sense of safety and security on private property.[308] One result of this desensitization is that now, outside the confines of our own homes, our "expectation of privacy" is almost gone.

However, as I have argued, it is wrong to assume there is a category of information about people that is "up for grabs," to be used by anyone for any person. Philosopher and privacy scholar Helen Nissenbaum calls this the problem of "privacy in public."[309] For example, a woman was raped and badly beaten in New York's Central Park in 1989. The case became famous as a racially charged example of prosecutorial misconduct.[310] Even though the rape occurred in a public place, and the trials of the accused rapists were public events, the victim maintained a measure of privacy as to her identity. [311] Even in more mundane situations, moreover, there does exist a right to maintain a measure of confidentiality in public. As Nissenbaum points out, for example, it is within one's rights to say "none of your business" to a stranger who asks your name, even in a public square or sidewalk.[312]

It is equally wrong to say that an aggregation of information violates no privacy interest so long as its individual components, taken individually, reveal

305. *See, e.g.*, 18 U.S.C. § 2511 (2005).

306. *See generally* U.S. CONST.

307. U.S. CONST. amends. IV, V.

308. *See* STANLEY & STEINHARDT, *supra* at note 252, at 1-3.

309. Nissenbaum, *supra* note 227, at 559.

310. *A Crime Revisited: Excerpts From District Attorney's Report on Re-examination of Jogger Case*, N.Y. TIMES, Dec. 6, 2002; Dwyer, J, *Likely U-Turn by Prosecutors in Jogger Case*, N.Y. TIMES, Oct. 12, 2002, at A1; McFadden, RD, *History is Shadow in Present in Jogger Case*, N.Y. TIMES, Sept. 7, 2002, at B1; Rashbaum, WK, *Convicted Killer and Rapist Says He Attacked Central Park Jogger*, N.Y. TIMES, June 12, 2002, at B2.

311. The rape victim has subsequently published a book. *See* TRISHA MELLI, I AM THE CENTRAL PARK JOGGER (2003).

312. Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAVIOR 207, 214 (1997).

little. George Kateb makes the case that data mining and video surveillance erode our integrity as individuals.[313] When the world is divided between those who watch and those who are the subject of scrutiny, the watchers are empowered, and the people on the wrong end of the camera are stripped of dignity:

> [O]ne is insulted, and insulted deeply, because one loses all possibility of innocence. . . . . [O]ne is crudely treated as interesting and even as presumptively or potentially guilty, no matter how law abiding one is. . . . . One is placed under constant suspicion just by being placed under constant watchfulness and subjected to the implicit interrogation that exists when the accumulated information on oneself is seen as a set of integrated answers that add up to a helpless, an unauthored autobiography. Such a loss of innocence . . . . . is so massive that the insult involved constitutes an assault on the personhood or human status of every individual.[314]

The public interest in privacy recognizes that citizens are more than the sum of the data elements they disclose to the state. Just as public surveillance constitutes a form of tyranny,[315] there is a fundamental privacy violation when the government permits or encourages data mining by commercial enterprises.

V. POLICY RECOMMENDATIONS

To protect the public interest in privacy, the government must fulfill its obligation to safeguard from public access the personal information with which it has been entrusted. Until recently, open government records were difficult to access, due to what the Supreme Court called the "practical obscurity" of paper storage.[316] Finding information about an individual used to involve making personal visits to local offices to locate records. Electronic formats and Internet publication have fundamentally changed the relationship between individuals, their information, and the government. The assumptions underlying these relationships deserve fresh inquiry, and new policies should be adopted to govern these relationships. [317]

A. Open Government Records

The greatest threat to privacy comes from government in secret. The best way to protect individual privacy is to make the government accountable to its

313. George Kateb, *On Being Watched and Known*, 68 SOCIAL RES. 269, 275 (2001).

314. *Id.* at 274-75.

315. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 135 (2004).

316. U.S. v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989).

317. For a work in progress on how to apply the principles of fair information practices to commercial data brokers, see Daniel J. Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection (Version 1.1)*, GWU Law School Public Law Research Paper No. 132, Mar. 8, 2005, http://ssrn.com/abstract=681902.

citizens, and open government records statutes serve this purpose. State legislatures should draft open government records statutes to incorporate provisions that reveal the inner workings of government and simultaneously protect individual privacy: to that end, the following recommendations offer a set of policies to be considered and adopted by agencies in the executive and legislative branches of government.

i. Government Agencies Must Notify Individuals That Their Personal Information May Be Disclosed to the Public Pursuant to Open Government Records Requests. The first and most important recommendation is to put the public on notice that their personal information in government records may be disclosed. Many people are unaware that their personal information may become public when they make disclosures for the purpose of doing business with state and local government agencies.[318] For example, if they have an "unlisted" telephone number, they may not expect that their addresses and phone numbers will be disclosed pursuant to an open government records request. All governmental agencies should provide notice that information may be disclosed.

ii. Government Agencies Must Limit the Personal Information They Collect from Individuals. Public agencies should only collect the data they need to serve their statutorily mandated functions and refrain from collecting extraneous personal information. Indeed, they should be able to identify the purposes for which they collect each item of personal information about individuals.

Moreover, state and local government agencies should re-examine the information they collect from individuals to determine whether the information is relevant and necessary to perform the agencies' mandated functions. For example, to collect Social Security numbers for fishing licenses may be convenient for the agency but serve no essential governmental function; if so, the practice should be abolished. If the personal information is not necessary for the agencies' mandated functions, the agencies should not collect it.

Government agencies should adopt the principles of fair information practices. There should be a way for an individual to find out what information about him is in a record and how it is used. There should be a way for him to correct or amend a record of identifiable information about him. If a public agency collects personal information for one purpose, it should not use the information for other purposes or re-disclose the information without notice to the affected individuals.

For most categories of government records, closer study will be required to determine whether government agencies should publish personally identifiable information. Vital records, for example, deserve fresh scrutiny. Records of

318. Sandra Byrd Peterson, Note, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163, 168-69 (1995).

births, deaths, marriages and other vital statistics, long presumed to be public records, are now being reconsidered in many jurisdictions, questioning whether they are appropriate for Internet publication.[319]

Licensing records similarly deserve a fresh look. Dog licenses, hunting and fishing licenses, and many species of permit applications necessarily collect home address information. There may be good reasons to disclose home addresses and other particulars about applicants, but none appear at first glance.[320] The New Jersey Division of Consumer Affairs recently stopped publishing the home addresses of licensed professionals on its web site, although it still discloses addresses of record (including home addresses) upon request.[321]

State legislatures should consider the following factors to determine whether personal information such as home addresses should be exempted from government records:

- the type of record requested;
- the potential for harm in any subsequent nonconsensual disclosure;
- the injury from disclosure to the relationship in which the record was generated;
- the adequacy of safeguards to prevent unauthorized disclosure;
- the degree of need for access; and
- whether there is an express statutory mandate, articulated public policy or other recognizable interest militating toward access.[322]

iii. Public Agencies Should Program Their Computer Systems and Applications to Collect But Not Disclose Personal Information. In the future, most requests for government records will likely be answered in electronic form, making computer systems and application design a technological answer to ensuring that data items like Social Security numbers and home addresses are not disclosed when redaction is required. As new computer systems and applications are phased in, they should be designed to flag the data fields for personal information and automatically redact this information when required to respond to open government records requests.

319. *See, e.g.*, N.H. REV. STAT. ANN. § 5-C:4 (2005) (effective through Jan. 1, 2006 and amended by H.R. 383, 2005 Leg., Reg. Sess. (N.H. 2005)) (privacy requirements for vital records); CAL. GOVT. CODE § 6254 (West 2005), (exempting vital records from disclosure under California Public Records Act).

320. Home address and telephone should ordinarily be redacted from disclosures under open government records statutes, except in the case of title search records voter registration records, and records where disclosure would serve the purpose of shedding light on government. This will not foreclose the news media, professional investigators, or title search companies from obtaining residential street addresses. In order to obtain home address information, requestors may obtain common law access to government records.

321. *See generally* New Jersey Division of Consumer Affairs, http://www.state.nj.us/lps/ca/home.htm (last visited Oct. 20, 2005).

322. U.S. v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).

This will require the state to identify a set of data items to be redacted from every record released to the public, such as home address, home telephone number, and financial and medical information. In addition, they must identify categories of records to be exempted from public disclosure, such as records concerning minor children.

iv. Individuals Should Be Permitted to "Opt-Out" of Having Their Personal Information Disclosed to the Public Pursuant to Open Government Records Requests. It may be appropriate in some cases to give individuals a means to indicate that they do not want their personal information to be disclosed to the public.[323] For example, they should be permitted in appropriate cases to file an "address of record" as an alternative to their home address. In many cases government agencies collect address information from residents not for the purpose of establishing residency but for other purposes, such as future contact.[324] Citizens who do not want their home addresses to be disclosed should, in appropriate cases, have the option of providing an address of record in lieu of home address.

v. Legislatures Should Give State and Local Agencies Adequate Funding to Comply with Requests for Government Records So As Not to Burden Requestors or Records Custodians with the Expense of Redaction and Other Requirements. To redact personal information such as home addresses from paper records is very burdensome. Redaction is labor intensive, time consuming, and costly.[325] In the future, it should be cheap and easy to program government computers so that inappropriate personal information is not disclosed electronically. Most requests for government records will in the future probably ask for electronic copies of electronic records. Many current and old records are still on paper, however, and most are archived or difficult to access.[326] Some requests are for dozens of boxes or thousands of documents stored at remote locations or in media that are difficult to retrieve.[327]

323. In 1999, for example, Congress amended the Drivers Privacy Protection Act, changing it from an "opt-out" law to an "opt-in" law, meaning that state departments of motor vehicles could not sell personal data for commercial purposes without the individuals' consent. Nevertheless, following the June 2000 effective date of the opt-in provision, data brokers continued to purchase millions of records from the Florida government for a penny each. The data brokers knew that the law had changed (having lobbied against it), but Fidelity Bank, a Florida savings and loan, bought from the Florida DMV names and addresses of individuals who had registered new or used cars. Florida has patched its statute, and Fidelity Bank has been held liable for liquidated damages. Kehoe v. Fid. Fed. Bank and Trust, 421 F.3d 1209, 1210-11 (11th Cir. 2005).

324. *See* Solove, *supra* note 1, at 1142-49.

325. David K. Isom, *Electronic Discovery Primer for Judges*, 2005 FED. CTS. L. REV. 1, §§ II-H, II-I (2005).

326. Solove, *supra* note 1, at 1139.

327. *See, e.g.*, Courier Post v. Lenape Reg'l High Sch. Dist., 821 A.2d 1190, 1195-96 (N.J. Super. Ct. Law Div. 2002) (offering the following factors to be considered to determine whether requestors should bear the costs for retrieving and inspecting government records: 1) The volume

As a general proposition, the expense of redacting personal information should not be borne by requestors but should instead be considered part of the cost of providing governmental services. This proposition places a very significant burden on governmental agencies and may be staggering for local governments, in staff time, technical equipment, and workspace. For this reason, every government agency should consider and articulate its reasons for collecting and disclosing personal information and receive appropriate funding support.

B. Privacy and Fair Information Practices

In order to adopt statutes that will protect the public interest in individual privacy, legislatures will have to identify categories of government records that should be kept confidential or from which personal information should be redacted. Some categories of government records clearly belong in the public domain, and some categories, just as clearly, do not. Records custodians need clear guidelines to determine whether personal information should be disclosed from different categories of records. Fortunately, legal precedents and many current state government resources are available to develop such guidelines.[328]

i. Public Domain and Private Information. It is commonly understood that many records are in the public domain – and should be - such as real property records. In many cases, however, citizens give their personal information to state and local government agencies expecting that the agencies will not give this information to anyone else.[329] For many records, like applications for fishing licenses and recreational softball leagues, citizens currently expect that the government will not publish their home addresses or unlisted telephone numbers, much less sensitive personal information.

Real property records should remain in the public domain. Generally, public agencies should allow access to information where the information is to be used for the purposes of facilitating the transfer of title to real property, such as title searching, the issuance of title insurance, mortgage origination, and other common activities related to the sale and financing of property. Government records that contain this information include property deeds, mortgages, municipal tax assessment records, tax liens, and judgment liens.[330]

of government records involved; 2) the period of time over which the records were received by the government unit; 3) whether some or all of the records sought are archived; 4) the amount of time required for a government employee to locate, retrieve and assemble the documents for inspection or copying; 5) the amount of time, if any, required to be expended by government employees to monitor the inspection or examination; and 6) the amount of time required to return the documents to their original storage space).

328. Solove, *supra* note 1, at 1162-64.

329. *Id.* at 1140; Peterson, *supra* note 321, at 168-69.

330. [329] Solove, *supra* note 1, at 1145.

From other categories of records, by contrast, personal information should routinely be withheld from public disclosure. Such categories include, for example, records containing information about minor children and records containing medical information, such as municipal recreation department records.[331]

ii. Definition of "Personal Information." To distinguish between records that properly belong in the public domain from the confidential data they should protect in the interest of privacy, legislatures must define "personal information" and charge records custodians with responsibility to ensure that personal information is not released to the public. For example, the Federal Privacy Act defines such records as

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.[332]

More simply, the Organisation for Economic Co-operation and Development guidelines define "personal data" as "any information relating to an identified or identifiable individual (data subject)."[333]

iii. Specific Privacy Legislation. The federal government enacted the Privacy Act as a companion to the FOIA, and the Supreme Court has

331. Judicial process will continue to be available, allowing litigants, the press, and other interested parties to inspect records that have been closed, especially in cases that involve public officials or public figures. Personal information that is routinely redacted would still be available to the public through common law access to government records. A court should make such a determination only after a public hearing of which reasonable notice has been given, and at which any interested person has a right to be heard and to contest.

332. 5 U.S.C. § 552a(a)(4) (West 2004). "Personally identifying information" could similarly be defined to mean any name, number or other information that may be used, alone or in conjunction with any other information, to identify a specific individual and includes, but is not limited to, the name, address, telephone number, date of birth, social security number, official state issued identification number, employer or taxpayer number, place of employment, employee identification number, demand deposit account number, savings account number, credit card number, mother's maiden name, unique biometric data, such as fingerprint, voice print, retina or iris image or other unique physical representation, or unique electronic identification number, address or routing code of the individual.

333. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/documentprint/0,2744,en_2649_201185_1815186_1_1_1_1,00.html; *see also* Declaration on Transborder Data Flows, OECD, Apr. 1985, http://www.oecd.org/documentprint/0,2744,en_2649_201185_1888153_1_1_1_1,00.html. For a comparison of U.S. privacy law to the OECD guidelines, see Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999).

interpreted the statutes together.[334] State legislatures could similarly enact specific privacy legislation to accompany open government records statutes.

iv. Omnibus Fair Information Practices Statutes. Every state in the European Union, Canada, and other countries have adopted fair information practices statutes.[335] This approach is available to the United States as well. Such statutes, at a minimum, would require all government agencies to (1) compile an index of all databases containing personal information; (2) permit individuals access to the non-exempt personal information collected about them; and (3) provide individuals the opportunity to verify the accuracy of that personal information maintained by the agency.[336]

C. Courthouse Records

The public interest in privacy applies with respect to courthouse records just as it applies to government records of the executive branch. Generally, courthouse records fall under the aegis of state supreme courts rather than a body of statutes.[337] Accordingly, while similar recommendations apply to both, the proper domain for codifying rules that apply to courthouse records is not legislation but the rules of court. The following guidelines would serve to safeguard the public interest in individual privacy with respect to courthouse records.

i. Redaction. The courts should redact from online records all Social Security numbers and other personal information that could facilitate identity theft or financial fraud. This is consistent with the Supreme Court's decision in *United States Dep't of Justice v. Reporters Committee for Freedom of the Press*:

> [W]e hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no 'official information' about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted.'[338]

334. *See, e.g.*, U.S. Dept. of Def. v. FLRA, 510 U.S. 487, 490-91 (1994).

335. *See* Canada Privacy Act, R.S.C., ch. P 21, §§ 1-2 (1985); OECD Privacy Statement Generator (2000), http://www.oecd.org/documentprint/0,2744,en_2649_34255_28863271_1_1_1_1,00.html.

336. *See* Canada Privacy Act, R.S.C., ch. P 21, §§ 10, 12 (1985); A few American statutes embrace these principles, but cover narrow segments of personal information. *See, e.g.*, 15 U.S.C. §§ 1681-1681x (1970) (Fair Credit Reporting Act); 5 U.S.C. § 552a (1974) (Privacy Act of 1974).

337. Michael Caughey, *Keeping Attorneys from Trashing Identities: Malpractice as a Backstop Protection For Clients Under the United States Judicial Conference's Policy on Electronic Court Records*, 79 WASH. L. REV. 407, 411 (2004).

338. 489 U.S. 749, 780 (1989).

ii. Limit Commercial Access to Courthouse Records. No benefit accrues to individuals who are forced to disclose information about themselves as a result of being hailed into court.[339] Litigants, jurors, and witnesses should be entitled to a measure of protection, instead of having their personal information mined for the commercial benefit of enterprises with which the individuals have no relationship.

The courts may constitutionally require that businesses be explicit about what they intend to do with the personal information they obtain from the judicial branch. In *Los Angeles Police Department v. United Reporting Publishing Corp.*, for example, the Supreme Court upheld a statute that limited commercial access to arrest records.[340] The statute permitted public access for scholarly, journalistic, political, or governmental purposes.[341] The Court concluded that the government may selectively grant access to public record information.[342] In *Seattle Times v. Rhinehart*, the Court stated that the government may condition the receipt of discovery information on nondisclosure.[343] Criminal records that merit special protection include presentence reports, plea agreements, unexecuted warrants, and pre-indictment documents.

iii. Security. The judiciary must adopt state-of-the-art security measures to prevent hackers and information brokers (including the judiciary's own outsourcing contractors) from culling sensitive information from its electronic files.

iv. Notice to the Public. The Rules of Court should be amended to account for privacy and security. The courts must put litigants, witnesses, and jurors on notice that personal information about them may be sold and/or published worldwide on the Internet. The rules should establish liability and consequences for releasing restricted information, as well as remedies for providing erroneous or incomplete information derived from court records.[344]

v. Acknowledge Individuals. Privacy protection should extend to persons, not corporations. To a limited extent, anonymity is already permitted: grand jury secrecy protects the interests of an innocent accused,[345] and some litigants

339. For this reason, the "information bargain" does not apply to court records, or government records of any kind. That is to say, the benefits that individuals may obtain from supermarket discount cards, for example, do not apply to interactions with the government.

340. 528 U.S. 32, 34, 41 (1999).

341. *Id.* at 35.

342. *Id.* at 41.

343. *Id.*

344. The rules should also provide remedies and consequences for improperly withholding public information.

345. *See, e.g.*, Douglas Oil v. Petrol Stops Nw., 441 U.S. 211, 219 (1979).

(such as rape victims and minors) are permitted to use their initials only.[346] The principles that protect the privacy interests of individuals who must participate in the court system should extend to electronic court records.

vi. Limit Fees. Court records should not be sold to generate revenue for the judicial branch. In this country, personally identifiable information is treated as a commodity, and the data-mining industry generates substantial revenues.[347] The judiciary could easily sell court records for profit to companies that collect information to do background checks and the like. This would be highly inappropriate. The courts are created to serve the entire population of the state. Their costs should not be borne exclusively by litigants, witnesses, and others who have involuntarily come into contact with the justice system.

> Release of information on computer tape in many instances is far more revealing than release of hard copies, and offers the potential for far more intrusive inspections. Unlike paper records, computerized records can be rapidly retrieved, searched, and reassembled in novel and unique ways, not previously imagined. For example, doctors can search for medical-malpractice claims to avoid treating litigious patients; employers can search for workers-compensation claims to avoid hiring those who have previously filed such claims; and credit companies can search for outstanding judgments and other financial data. Thus, the form in which information is disseminated can be a factor in the use of and access to records.[348]

CONCLUSION

Congress, state legislatures, and the judiciary must empower federal, state, and local government agencies to protect the public interest in privacy and thereby fulfill their constitutional and statutory obligations. State and local government agencies should evaluate and articulate their reasons for collecting individually identifiable information about citizens.

In some instances, government agencies need information about individuals in order to provide services to those individuals. In such cases, disclosures about the individuals will reveal nothing about governmental

346. *See, e.g.*, Fla. Star v. B.J.F., 491 U.S. 524, 527 n.2 (1989) (noting that the court would use the rape victims initials for privacy interests); J.K. v. Kucharski, 661 N.W.2d 216 (Mich. 2003) (using a minor's initials in a termination of parental rights case); State *ex rel.* T.W. v. Ohmer, 133 S.W.3d 41, 42 (Mo. 2004) (en banc) (using a minor's initials in a termination of parental rights case).

347. *See* Solove, *supra* note 1, at 1149-51.

348. Higg-A-Rella, Inc. v. County of Essex, 660 A.2d 1163, 1172 (N.J. 1995).

operations. Accordingly, in those instances, personally identifiable information should not be routinely disclosed.[349]

The public interest in privacy similarly attaches to court records. The judiciary should not yield to the demands of profit or even of tradition without a fresh evaluation of its obligation to protect the personal information it has obtained from individuals who are under compulsion to the system.

349. In other cases, the information may be gathered for the purpose of evaluating governmental operations, and disclosure would be appropriate. *See* U.S. v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980).