2002

Access and Aggregation: Privacy, Public Records, and the Constitution

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

Access and Aggregation: Public Records, Privacy and the Constitution

Daniel J. Solove†

CONTENTS

† Assistant Professor, Seton Hall Law School; J.D. Yale, 1997. I would like to thank Mark Alexander, Carl Coleman, Howard Erichson, Timothy Glynn, Rachel Godsil, Ted Janger, Raymond Ku, Erik Lillquist, Michael Risinger, Marc Rotenberg, Richard Solove, Richard St. John, Charles Sullivan, and Michael Sullivan. I would also like to thank Peter Choy and Eli Weiss for their research assistance, and the Seton Hall Law School faculty scholarship fund for its financial support for this project.

INTRODUCTION

Imagine that the government had the power to compel individuals to reveal a vast amount of personal information about themselves—where they live, their phone numbers, their physical description, their photograph, their age, their medical problems, all of their legal transgressions throughout their lifetimes whether serious crimes or minor infractions, the names of their parents, children, and spouses, their political party affiliations, where they work and what they do, the property that they own and its value, and sometimes even their psychotherapists' notes, doctors' records, and financial information.

Then imagine that the government routinely poured this information into the public domain—by posting it on the Internet where it could be accessed from all over the world, by giving it away to any individual or company that asked for it, or even by providing entire databases of personal information upon request. In an increasingly "wired" society, with technology such as sophisticated computers to store, transfer, search, and sort through all this information, imagine the way that the information could be combined or used to obtain even more personal information.

Imagine the ease with which this information could fall into the hands of crafty criminals, identity thieves, stalkers, and others who could use the information to threaten or intimidate individuals. Imagine also that this information would be available to those who make important decisions about an individual's life and career—such as whether the individual will get a loan or a job. Also imagine that in many cases, the individual might not be able to explain any concerns raised by this information or even know that such information was used in making these decisions.

Imagine as well that this information would be traded among hundreds of private-sector companies that would combine it with a host of other information such as one's hobbies, purchases, magazines, organizations, credit history, and so on. This expanded profile would then be sold back to the government in order to investigate and monitor individuals more efficiently.

Stop imagining. What I described is what is currently beginning to

occur throughout the United States by the use of federal, state, and local public records, and the threat posed to privacy by public records is rapidly becoming worse.

For decades, federal, state, and local governments have been keeping records about their citizens. 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 information. Federal agencies maintain records pertaining to immigration, bankruptcy, social security, military personnel, and so on. 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, psychiatrists' notes, drug prescriptions, diseases and other disorders); and identifying information (mother's maiden name, Social Security number). This list is far from complete. Many of these records are open for public inspection.

Until recently, public records were difficult to access. For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records. But with the Internet revolution, public records can be easily obtained and searched from anywhere. Once scattered about the country, now public records are consolidated by private sector entities into gigantic databases. Recently, the federal court system has proposed to make court records available electronically, sparking a considerable debate over privacy because highly sensitive information such as one's Social Security number, medical and psychological records, financial information, and even details about one's marital relationship are sometimes lodged in court records.

A complicated web of state and federal regulation governs the accessibility of these records. This regulation was formulated to balance two important, yet sometimes conflicting, interests. One of these interests is transparency, the need to expose government bureaucracy to public scrutiny. The Federal Freedom of Information Act is an attempt to promote such transparency. Access to court records, in the words of Jus-

tice Holmes, ensures "that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed."[1]

The other interest is privacy. Increasingly, as more personal information is collected, stored, and consolidated in government databases, the threat to privacy is imminent. Federal, state, and local governments have been one of the principal suppliers of personal information to the private sector. A growing number of large corporations are assembling dossiers on practically every individual by combining information in public records with information collected in the private sector such as one's purchases, spending habits, magazine subscriptions, web surfing activity, and credit history. Increasingly, these dossiers of fortified public record information are sold back to government agencies for use in investigating people.

In this Article, I argue that the regulation of public records in the United States must be rethought in light of the new technologies in the Information Age, and I advance a theory about how to reconcile the tension between transparency and privacy.

First, I contend that information privacy must be reconceptualized in the context of public records to abandon the longstanding notion that there is no claim to privacy when information appears in a public record. This view, which I term the "secrecy paradigm," understands privacy as depending upon whether information is secret or non-secret. The secrecy paradigm fails to account for the realities of the Information Age, where information is rarely completely confidential. I suggest that privacy must be understood as an expectation of a limit on the degree of accessibility of information.

Second, I critique the widespread view that one has a privacy interest only in information that is embarrassing or harmful to one's reputation. Much of the personal information contained in public records (i.e., one's race, marital status, party affiliation, property values, and so on) is relatively innocuous. However, as I explain, it is the totality of the information, aggregated together, that presents the problem. Consolidating various bits of information, each in itself relatively unrevealing, can, in the aggregate, begin to paint a portrait of a person's life. I refer to this as a "digital biography." A growing number of private sector organizations are using public records to construct digital biographies on millions of individuals. I argue that we should be concerned about the ways in which our digital biographies are being used. These uses are resulting in a growing dehumanization, powerlessness, and vulnerability for indi-

1. Cowley v. Pulsifer, 137 Mass. 392, 394 (1884).

viduals. Therefore, viewed in light of my theory of information privacy, the regulation of public record regimes must be substantially rethought.

I contend that the appropriate balance between transparency and privacy can be reached by limiting access and uses of certain information rather then making public records unavailable to the public. If the secrecy paradigm is abandoned and privacy is understood as an expectation in the limitation of the degree of accessibility of information, then commercial access and use restrictions as well as a federal baseline of regulation for all public records would help significantly in addressing the problem.

A potential hurdle to the adoption of these solutions is the First Amendment. Although the First Amendment establishes a right to access certain court proceedings and records, I contend that this right does not and should not extend to other types of public records. In fact, based upon developing strands of Supreme Court jurisprudence, the Constitution imposes certain limitations and responsibilities on the government's collection and use of personal information.

Next, I analyze the implications of such a solution for the First Amendment's protection of freedom of speech and the press. This issue is quite complicated, as there is a significant tension between two lines of Supreme Court jurisprudence. One line of cases holds that when the government makes information publicly available in a public record, the press cannot be sanctioned for publishing it.[2] Another line of cases, however, establishes that the government may selectively grant access to public record information and suggests that the government may condition the receipt of such information on nondisclosure.[3] In an extensive navigation of these potentially conflicting precedents, I conclude that access and use restrictions of public record information will generally not run afoul of the First Amendment.

Part I of this Article provides an introduction to the history of public records and how these records are regulated. Part II describes how privacy in this context should be reconceptualized, taking into account the problems of access and aggregation. Part III examines the constitutional issues.

I. THE PROBLEM OF PUBLIC RECORDS

From the beginning of the twentieth century, we have witnessed a

2. *See, e.g.*, Fla. Star v. B.J.F., 491 U.S. 524 (1989); Cox Broad. Corp. v. Cohn Publ'g Co., 420 U.S. 469 (1975).

3. *See, e.g.*, Los Angeles Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32 (1999); *cf.* Rust v. Sullivan, 500 U.S. 173 (1991) (finding that prohibiting abortion counseling or referral as a condition for receipt of Title X funds does not violate the First Amendment).

vast proliferation in the number of government records kept about individuals as well as a significant increase in public access to these records. These trends together have created a problematic state of affairs—a system where the government extracts personal information from the populace and places it in the public domain, where it is hoarded by private sector corporations that assemble dossiers on almost every American citizen. In this Part, I will explore public record systems, examining the types of public records maintained by governments and the regulatory regime that governs access to these records. This regulatory regime has not adequately matured to respond to the realities of modern information flow.

A. AN OVERVIEW OF PUBLIC RECORD-KEEPING

1. Federal, State, and Local Public Records

Public record-keeping is largely a product of the twentieth century. Before the mid-nineteenth century, few public records were collected, and most of them were kept at a very local level.[4] During the late nineteenth century and early twentieth century, state and local governments increasingly began to keep records of their citizens.[5] In the 1940s, 50s, and 60s, the expansion of the bureaucratic network of regulation, licensing, and entitlements at the federal, state, and local levels resulted in a massive escalation of public records.[6]

Today, a welter of public records is kept by federal, state, and local governmental entities. States maintain a smorgasbord of public records, covering one's life from birth to death.[7] Birth records can contain one's name, date of birth, place of birth, full names and ages of one's parents, and mother's maiden name.[8] In particular, a person's mother's maiden name is an important piece of information because many financial institutions and other entities use it as a password to access more sensitive data. Shortly after birth, the federal government stamps an individual

4. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 12 (2000).

5. Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1906-07 (1981).

6. *See* DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE 73 (Tim May ed., 2001); ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY 220-23 (1972). For a discussion of the expansion of government entitlements and licensing, see Charles A. Reich, *The New Property*, 73 YALE L.J. 733, 733-37 (1964).

7. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1403 (2001).

8. *See, e.g.*, CAL. HEALTH & SAFETY CODE § 102425(a)(1)-(11) (West Supp. 2002).

with a Social Security number, which will be used throughout her life to identify her and consolidate records about her.[9] States also maintain other records relating to one's personal life, such as records about one's marriage, divorce, and death. These records are often referred to collectively as "vital records." Records of marriages, which are public in most states,[10] contain maiden name, the date and place of birth of both spouses, as well as their residential addresses.[11]

Beyond vital records, states keep records for almost every occasion an individual comes into contact with the state bureaucracy. When a person obtains a license to drive, the state records and publicizes information such as her name, address, phone number, Social Security number, medical information, height, weight, gender, eye color, photograph, and date of birth.[12] Additionally, accident reports and traffic citation records are made publicly available by many states.

Individuals who register to vote must surrender information into a public record. Voting records can reveal one's political party affiliation, date of birth, place of birth, e-mail address, home address, telephone number,[13] and sometimes one's Social Security number.[14] In many states, this information is publicly available.[15]

One's profession and employment often generate a number of records. A number of professions require state licensing, such as doctors, lawyers, engineers, insurance agents, nurses, police, accountants, and teachers.[16] If an individual is injured at work, worker's compensation records may disclose one's date of birth, type of injury, and Social Security number.[17] If a person is a public employee, many personal details

9. *See* Solove, *supra* note 7, at 1402.

10. *See, e.g.*, CAL. HEALTH & SAFETY CODE § 103150 (West 1996).

11. *See, e.g.*, *id.* § 103175 (West Supp. 2002).

12. *See* BD. OF GOVERNORS OF THE FED. RESERVE SYS., REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD 6 n.5 (March 1997), *available at* http://www.federalreserve.gov/boarddocs/RptCongress/privacy.pdf; *see also* Joan Biskupic, *High Court to Hear Driver Privacy Case*, WASH. POST, May 18, 1999, at A8.

13. *See* CAL. ELEC. CODE §§ 2102, 2150(a)(1)-(10) (West Supp. 2002); CAROLE A. LANE, NAKED IN CYBERSPACE: HOW TO FIND PERSONAL INFORMATION ONLINE 274 (1997).

14. EDMUND J. PANKAU, CHECK IT OUT! 16 (1998).

15. Some states are beginning to restrict access to voter records for certain purposes, although the permissible purposes remain quite broad. In California, for example, voter records are openly available to any political candidate, to any committee for or against any initiative or referendum, and "to any person for election, scholarly, journalistic, or political purposes." CAL. ELEC. CODE § 2194 (West Supp. 2002). Therefore, any person or entity with even a tangential relationship to the political process can obtain this information.

16. *See* Solove, *supra* note 7, at 1403.

17. *See* LANE, *supra* note 13, at 275. Seven states make workers' compensation records publicly accessible. *See* PUBLIC RECORDS ONLINE: THE NATIONAL GUIDE TO

are released to the public by way of personnel records, including one's home address, phone number, Social Security number, salary, sick leave, and sometimes even e-mail messages.[18] In Massachusetts, government officials are required by law to maintain "street lists" containing the names, addresses, dates of birth, veteran statuses, nationalities, and occupations of all residents.[19] These lists, which organize residents by the streets they live on, are made available to the police,[20] to all political committees and candidates, and to businesses and other organizations.[21]

One's home and property are also a matter of public record. Property tax assessment records contain a detailed description of one's home, including number of bedrooms and bathrooms, amenities such as swimming pools, the size of the house, and the value.[22] These records are public.[23] Other property ownership records unveil lifestyle information such as whether one owns a boat, and if so, its size and type.[24]

Often, any contact with law enforcement officials will yield a record. Arrest records can contain one's name, occupation, physical description, date of birth, and the asserted factual circumstances surrounding the arrest.[25] Police records also contain information about victims of crime.

Court records are potentially the most revealing records about individuals. Whenever a person comes into contact with the judicial system, information is released into a public record. In almost all states, court records are presumed to be public.[26] Although current practice and exist-

PRIVATE & GOVERNMENT ONLINE SOURCES OF PUBLIC RECORDS 21 (Michael L. Sankey et al. eds., 3d ed. 2001).

18. *See, e.g.*, IND. CODE ANN. § 5-14-3-4(b)(8)(A)-(C) (Michie 2001) (first version) (requiring disclosure of particular information in public employees' personnel records including salary, education, prior work experience, and any disciplinary troubles); Braun v. City of Taft, 201 Cal. Rptr. 654, 660-61 (Cal. Ct. App. 1984) (permitting disclosure of an employee's Social Security number, home address, and birth date); Eskaton Monterey Hosp. v. Myers, 184 Cal. Rptr. 840, 843 (Cal. Ct. App. 1982) (permitting disclosure of a state employee's personnel file, which contained education and training experience); Moak v. Phila. Newspapers, Inc., 336 A.2d 920, 921, 924 (Pa. Commw. Ct. 1975) (permitting disclosure of payroll records that contained employees' names, gender, date of birth, annual salary, and other personal data). *But see* IDAHO CODE § 9-340C(1) (Michie Supp. 2001) (exempting personnel records from public disclosure).

19. *See* MASS. ANN. LAWS ch. 51, § 4 (Law. Co-op. Supp. 2001)

20. *Id.*

21. *Id.* § 6; *see also* Pottle v. Sch Comm. of Braintree, 482 N.E.2d 813, 817 (Mass. 1985).

22. *See, e.g.*, CAL. REV. & TAX. CODE § 408.3 (West 1998).

23. *See id.* § 408.3(a) ("Property characteristics information maintained by the assessor is a public record and shall be open to public inspection.").

24. *See* LANE, *supra* note 13, at 274-75.

25. *See, e.g.*, CAL. GOV'T CODE § 6254(f)(1) (West Supp. 2002).

26. *See infra* text accompanying notes 114-17; *see, e.g.,* CAL. R. 243.1(c) ("Unless

ing physical constraints limit the extent to which personal information in court documents can be accessed, new technologies are on the verge of changing this reality.[27]

In civil cases, such as suits for personal injury, medical malpractice, product liability, and so on, court files may contain vast quantities of data, such as medical history, mental health data, tax returns, and other financial information.[28] For example, in an ordinary civil lawsuit over an automobile accident, the plaintiff must submit medical information, including any pre-existing conditions that might affect her recovery or be responsible for her symptoms. This data could even include psychological information. To establish damages, the plaintiff must also reveal details about her lifestyle, activities, and employment. If this information is contained in a document filed with the court or is mentioned in a hearing or at trial, it can potentially become accessible to the public unless protected by a protective order. In addition to plaintiffs, civil defendants must also yield personal information in many instances.

Witnesses and other third parties who are involved in cases can have deeply personal details snared by discovery and later exposed in court documents. If a person serves as a juror, her name, address, spouse's name, occupation, place of employment, and answers to voir dire questions may become part of the court record.[29] Additionally, some courts have held that the public may have access to questionnaires given to jurors as part of voir dire.[30] Voir dire questions can involve sensitive matters such as whether a juror was the victim of a crime, the juror's political and religious beliefs, any medical and psychological conditions that

confidentiality is required by law, court records are presumed to be open."). Not all court records are public; in most states, adoption records, grand jury records, and juvenile criminal court records are not public. *See, e.g.,* David S. Jackson, *Privacy and Ohio's Public Records Act*, 26 CAP. U. L. REV. 107, 120 (1997); *see also* The Federal Judiciary, *Frequently Asked Questions, Filing a Case, Q: How Can I Check on the Status of My Case? Can I Review Case Files?*, *at* http:/www.uscourts.gov/faq.html (last visited June 29, 2002). Beyond pleadings and motions (which are, for the most part, always contained in the court file), other documents (such as exhibits) and transcripts may or may not be contained in the file. For example, typically a trial transcript will only be contained in the court file if an appeal is taken. The availability of other documents, such as exhibits, in the court file is controlled by local practice. Local practices vary greatly depending on limited storage capacities in clerks' offices. Often, exhibits are kept by the parties.

27. *See infra* Part I.A.3.

28. LANE, *supra* note 13, at 246.

29. *See, e.g.*, Unabom Trial Media Coalition v. United States Dist. Court, 183 F.3d 949, 950 (9th Cir. 1999); United States v. Antar, 38 F.3d 1348, 1358-59 (3d Cir. 1994) (noting that a public right of access to voir dire proceedings exists); People v. Mitchell, 592 N.W.2d 798 (Mich. Ct. App. 1999) (holding that the press has a "qualified right of access" to jurors' names and addresses).

30. Lesher Communications, Inc. v. Superior Court, 274 Cal. Rptr. 154, 156-57 (Cal. Ct. App. 1990).

might affect the juror's performance, and other private details.[31]

Beyond ordinary civil lawsuits, special civil proceedings such as appeals from the denial of social security benefits release much information into court records, such as a person's disability, work performance, Social Security number, birth date, address, phone number, and medical records.[32] In federal bankruptcy courts, any "paper filed . . . and the dockets of a bankruptcy court are public records and open to examination by an entity at reasonable times without charge."[33] Information involved in bankruptcy proceedings includes one's Social Security number, account numbers, employment data, sources of income, expenses, debts owed, and other financial information.[34] Additionally, in certain circumstances, employees of a company that declares bankruptcy can have their personal information divulged in public bankruptcy records.[35]

In some states, family court proceedings are public. For example, a divorce proceeding can unmask the intimacies of marital relationships. As one state court held, "[a] private citizen seeking a divorce in this State must unavoidably do so in a public forum, and consequently many private family and marital matters become public."[36]

For criminal cases, there is even less privacy. Beyond the personal details about a defendant released at trial or in the government's indictment or charging papers, conviction records are made public.[37] Information about victims—their lifestyles, medical data, and occupation—can also be found in court records. Presentence reports prepared by probation officers about convicted defendants facing sentence are used by judges in arriving at the appropriate sentence. These reports contain identifying information about the defen-

31. In practice, juror information is rarely sought out except in high profile cases.

32. A person may appeal from the denial of social security benefits pursuant to 42 U.S.C. § 405(a) (1994 & Supp. V 1999), *amended by* Act of Dec. 21, 2001, Pub. L. No. 107-90, 115 Stat. 878. If social security information is disclosed in court filings, confidentiality is lost. 20 C.F.R. § 401.180 (2001).

33. 11 U.S.C. § 107(a) (2000).

34. Mary Jo Obee & William C. Plouffe, Jr., *Privacy in the Federal Bankruptcy Courts*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1011, 1020 (2000).

35. *See* Jerry Markon, *Curbs Debated As Court Records Go Public on Net*, WALL ST. J., Feb. 27, 2001, at B1. Normally, bankruptcy filings only include personal information about a company's top officials. However, an Internet furniture retailer included information in its bankruptcy petition about all employees "to blunt criticism from creditors that it had recklessly burned through cash." *Id*. At the request of creditors, a court-appointed trustee posted the information on the retailer's website. *Id*.

36. *In re* Keene Sentinel, 612 A.2d 911, 915-16 (N.H. 1992); *see also* Barron v. Fla. Freedom Newspapers, Inc., 531 So. 2d 113, 119 (Fla. 1988) ("[P]arties seeking a dissolution of their marriage are not entitled to a private court proceeding just because they are required to utilize the judicial system.").

37. *See* LANE, *supra* note 13, at 213.

dant's prior criminal conduct, social history, character, family environment, education, employment and income, and medical and psychological information.[38] Although in many states and in federal court, presentence reports remain confidential, in some states, such as California, the presentence report becomes part of the court file after sentencing.[39]

Community notification laws for sex offenders, often referred to as "Megan's Laws," require the maintenance of databases of information about prior sex offenders and disclosure of their identities and where they live.[40] In 1996, Congress passed a federal Megan's Law restricting states from receiving federal anti-crime funds unless they agree to "release relevant information that is necessary to protect the public" from released sex offenders.[41] As a result, all fifty states enacted some version of Megan's Law.[42] Sex offender records often contain the sex offender's Social Security number, photograph, address, prior convictions, and places of employment.[43] Some states have placed their sex offender records on the Internet.[44] Several states fail to identify the particular crime the offenders are charged with, lumping all of them under the label sex offender, even where some might be rapists while others could be listed for sodomy, public masturbation, or indecent exposure.[45]

In a move broader than Megan's Law, some localities are widely disseminating records about individuals arrested, but not yet convicted, of certain crimes. For example, in 1997 Kansas City initiated "John TV," broadcasting on a government-owned television station the names, photographs, addresses, and ages of people who had merely been arrested (not convicted) for soliciting prostitutes.[46] Other cities have initiated

38. *See, e.g.*, CAL. PENAL CODE § 1203.10 (West 1982); CAL. CT. R. 4.411.5(a)(6).

39. *See, e.g.,* CAL. PENAL CODE § 1203d (West Supp. 2002) ("The report shall be filed with the clerk of the court as a record in the case at the time the court considers the report.").

40. *See* Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (holding that New Jersey's Megan's Law does not violate the constitutional right to information privacy because of compelling governmental interest in preventing sex offenses); Russell v. Gregoire, 124 F.3d 1079, 1093-94 (9th Cir. 1997) (holding that Washington's Megan's Law does not violate the constitutional right to information privacy because the information compiled and disclosed is already public).

41. 42 U.S.C. § 14071(e)(2) (1994 & Supp. V 1999), *amended by* Act of Oct. 28, 2000, 42 U.S.C.S. § 14071 (Law. Co-op. Supp. 2001).

42. Jane A. Small, *Who Are the People In Your Neighborhood? Due Process, Public Protection, and Sex Offender Notification Laws*, 74 N.Y.U. L. REV. 1451, 1459 (1999).

43. *See, e.g. Paul P.*, 170 F.3d at 398; *Russell*, 124 F.3d at 1082.

44. *See, e.g.*, Fla. Dep't of Law Enforcement, *Sexual Offenders/Predators Search System*, *at* http://www.fdle.state.fl.us/Sexual_Predators (last visited March 12, 2002) ; N.C. State Bureau of Investigation, *North Carolina Sex Offender & Public Protection Registry*, *at* http://sbi.jus.state.nc.us/sor/ MainText.htm (1998).

45. *See* Small, *supra* note 42, at 1456, 1463-64.

46. Edward Walsh, *Kansas City Tunes In as New Program Aims at Sex Trade: 'John*

similar programs.[47] Additionally, a growing number of states are furnishing online databases of all of their current inmates and parolees.[48]

2. The Government-Madison Avenue Connection

For a long time, private sector companies have relied upon public records to obtain personal information about individuals for marketing purposes. In the burgeoning Information Age, marketing thrives upon personal information, giving rise to an entire industry devoted to the collection of personal information. I have discussed the history and current collection and use of personal information by the private sector in more detail elsewhere.[49]

Much of the information collected by the private sector comes from public records and personal information held by the government. For example, beginning in the nineteenth century, advertisers began using census data as a marketing device.[50] In 1970, the United States began selling its census data on magnetic tapes.[51] Often at the behest of marketers, the Census Bureau increasingly sought data about people's lifestyles. To do this, the Census Bureau required a subset of households to fill out a long questionnaire asking dozens of questions.[52] These questions included such information as how much rent people pay, what products they own, their occupation, their marital history, and their income.[53] The connection between the Census Bureau and marketers has been a very close one. Presidents have frequently appointed former marketers to serve as the head of the Census Bureau.[54] In 1981, a group of ten companies made a pact with the Census Bureau for it to undertake a special

TV,*'* WASH. POST, July 8, 1997, at A3.

47. *Id.*

48. D. Ian Hopper, *Database, Protection, Or a Kind of Prison?: Web Registries of Inmates, Parolees Prompt a Debate*, WASH. POST, Dec. 29, 2000, at A31.

49. *See* Solove, *supra* note 7, at 1403-09.

50. ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 30-31 (1992).

51. *See* DICK SHAVER, THE NEXT STEP IN DATABASE MARKETING 29 (1996); *see also* LARSON, *supra* note 50, at 41.

52. *See, e.g.*, ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER 270 (2d ed. 1996); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 127 (1971).

53. *See* MILLER, *supra* note 52, at 127. The 2000 Census long form asks for information on sex, age, race, education, employment, income, value and physical description of residence, vehicles owned, as well as other information. *See* U.S. Census Bureau, 2000 Long Form Questionnaire (Form D-2) *available at* www.census.gov/dmd/www/pdf/do2p.pdf (approved for use by the public through Dec. 31, 2000).

54. Since the 1970s, the Census Bureau has been run by a former director of marketing at General Motors, an executive at a political polling firm, a research manager for Sears, and a past president of the American Marketing Association. LARSON, *supra* note 50, at 44.

tabulation of census data by zip code—with the companies enjoying exclusive access to the results.[55] The questions asked by the census are often quite helpful to marketers and the Census Bureau has been accused of being too influenced by the needs and wants of corporate America.[56]

For decades, many states have been selling their public records to the highest bidder.[57] Colorado used to sell its motor vehicle information for about $4.4 million a year.[58] Florida offered to sell copies of its motor vehicle information for $33 million.[59] New York earned $17 million in one year from such sales.[60] In 1994, the Federal Government, alarmed at this practice, passed the Driver's Privacy Protection Act, restricting such disclosures of information from motor vehicle records.[61]

Increasingly, there is a two-way information flow between the private and public sectors. In other words, not only is the government supplying information to the private sector, but the private sector is assisting the government in generating information about individuals. Currently, government agencies such as the FBI and IRS are purchasing public record collections aggregated by private sector companies and combined with other data gathered by the private companies.[62] A private company called ChoicePoint, Inc. has amassed a database of ten billion records and has contracts with at least thirty-five federal agencies to share the data with them.[63] In 2000, the Justice Department signed an $8 million contract with ChoicePoint, and the IRS reached a deal with the company for between $8 and $12 million.[64] ChoicePoint collects information from public records from around the country and then combines it with information from private detectives, the media, and credit reporting firms.[65] This data is indexed by people's Social Security numbers.[66] The Health Care Financing Administration (now the Center for Medicare and Medicaid Services) uses ChoicePoint's data to help it identify fraudulent

55. *Id.* at 44-45.

56. *Id.* at 44-46.

57. *See* Rajiv Chandrasekaran, *Governments Find Information Pays,* WASH. POST, Mar. 9, 1998, at A1.

58. Robert Kowalski, *Privacy Bills Up Next: Should Sale of Driver's License Info Continue?*, DENVER POST, May 5, 1997, at 1A.

59. Larry Rohter, *Florida Weighs Fees for its Computer Data: Some See Profits; Others, Too High a Price*, N.Y. TIMES NAT'L, Mar. 31, 1994, at B9.

60. *See* Biskupic, *supra* note 12, at A8. Wisconsin receives $8 million annually from the sale of motor vehicle data. *See* Travis v. Reno, 163 F.3d 1000, 1002 (7th Cir. 1998).

61. 18 U.S.C. §§ 2721-2725 (2000).

62. *See* 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 A1.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

Medicare claims by checking health care provider addresses against ChoicePoint's list of "high-risk and fraudulent business addresses."[67] ChoicePoint claims that it has records on almost everybody with a credit card.[68]

ChoicePoint's information is not only used by government agencies but also by private sector employers to screen new hires or investigate existing employees.[69] The information in ChoicePoint's collection is a mixture of fact and fiction.[70] There are a number of errors in the records.[71] Richard Smith of the Privacy Foundation obtained his report and discovered numerous errors, including the false facts that he had been previously married and that his wife had a son three years before they met.[72] A ChoicePoint report also erroneously indicated that a woman was a convicted drug dealer and shoplifter, resulting in the termination of her employment.[73] ChoicePoint also had a hand in the 2000 Presidential Election problems in Florida. ChoicePoint supplied Florida officials with a list of 8000 "ex-felons" to eliminate from their voter lists.[74] However, many of the 8000 were not guilty of felonies, only misdemeanors, and were legally eligible to vote.[75] Although the error was discovered prior to the election and officials tried to place the individuals back on the voter rolls, the error might have led to some eligible voters being turned away at the polls.[76]

3. The Impact of Technology

For a long time, public records have been accessible only in the various localities in which they were kept. A person or entity desiring to find out about the value of an individual's home would have to travel to the town or county where the property was located and search through the records at the local courthouse. Depending upon local practice, the seeker of a record might be able to obtain a copy through the mail. Court records, such as bankruptcy records, would typically be obtained by visiting a courthouse or engaging in a lengthy correspondence with the

67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *See* Richard Smith, *My FBI File*, *at* http://www.privacyfoundation.org/ commentary/tipsheet.asp (May 11, 2001).
73. *See* Simpson, *supra* note 62, at A1.
74. *See* Gregory Palast, *Florida's Flawed "Voter-Cleansing" Program*, Salon.com, *at* http://www.salonmag.com/politics/feature/2000/12/04/voter_file/ index.html (Dec. 4, 2000).
75. *Id.*
76. *See id.*

clerk's office.[77] The seeker of a record could not obtain records en masse; records could only be obtained for specific individuals.

This reality, however, is rapidly changing. As records are increasingly computerized, entire record systems rather than individual records can be easily searched, copied, and transferred. Private sector organizations sweep up millions of records from record systems throughout the country and consolidate those records into gigantic record systems. Many websites now compile public records from across the country.[78] There are more than 165 companies offering public record information over the Internet.[79] These companies have constructed gigantic databases of public records that were once dispersed throughout different agencies, offices, and courthouses, and with the click of a mouse, millions of records can be scoured for details.[80]

The increasing digitization of documents and the use of electronic filing will soon result in much greater accessibility to court records online. A recent proposal to make court records electronic and available over the Internet has garnered significant attention. A majority of courts post only court rulings and schedules on their websites. Only a handful of courts now post complaints and other legal documents.[81] A few states have begun to require electronic copies of records to be filed or to convert existing records into electronic format. For example, in New Jersey, bankruptcy records (including a debtor's bankruptcy petition) are scanned into electronic format and can be accessed through the Internet.[82] Some companies are beginning to make digital images of records available over the Internet.[83]

Recently, the federal court system announced plans to develop a system for placing court filings online. The existing system, called PACER (Public Access to Court Electronic Records), includes only basic docketing information such as the names of the parties, attorneys, general type of action, and a list of documents filed. The system under develop-

77. *See* Obee & Plouffe, *supra* note 34, at 1012.

78. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1156-57 (1997).

79. *See* PUBLIC RECORDS ONLINE, *supra* note 17, at 8.

80. For example, KnowX.com states that it has amassed millions of public records, which are updated regularly. *See* http://www.knowx.com (last visited June 29, 2002). Search Systems contains over 6000 searchable public record databases. *See* http://www.pac-info.com (last visited June 29, 2002). Locateme.com permits its users to search public records such as driver registrations, voter registrations, and credit headers. *See* http://www.locateme.com (last visited June 29, 2002).

81. *See* Joanna Glasner, *Courts Face Privacy Conundrum*, WIRED NEWS, Feb. 26, 2001, *at* http://www.wired.com/news/politics/0,1283,41967,00.html.

82. U.S. Bankruptcy Court for the Dist. of N.J., *Case Information*, *at* http://www.njb.uscourts.gov/caseinfo/ (last visited March 12, 2002).

83. *See* http://www.courthousedirect.com (last visited June 29, 2002).

ment, called Case Management/Electronic Case Files ("CM/ECF"), is designed to be in place by 2005.[84] The system will make full case files accessible via the Internet.[85] Currently, nine courts use the CM/ECF system.[86] Anybody is permitted to view, print, and download any document filed in the system. The courts, however, have not developed comprehensive policies to deal with privacy concerns.[87]

Beyond greater accessibility, technology may also lead to the retention of greater amounts of personal information in public records. Under current practice, due to storage space constraints, clerks' offices often do not maintain copies of exhibits and other documents related to trials. However, as court documents such as pleadings and exhibits are filed in digital format, they will become easier to store. Further, under current practice, transcripts are typically produced only when a case is appealed. New technology enables transcripts of court proceedings to be made instantaneously without having to be transcribed. The increased use of such technology could result in the existence of more transcripts of trials, which can potentially include personal information about many parties and witnesses.

In sum, the increasing digitization of documents enables more documents to be retained by eliminating storage constraints, increases the ability to access and copy documents, and permits the transfer of documents en masse. Personal information in public records, once protected by the practical difficulties of gaining access to the records, is increasingly less obscure.

B. THE REGULATION OF PUBLIC RECORDS

As it currently stands, public records law is a complicated and diverse hodge-podge of various statutes, court practices, and common law rights that vary from state to state and leave much personal information unprotected. Our information regulatory infrastructure is disconnected, often outdated, and inadequate to meet the challenges of the new technologies of the Information Age. This section provides a brief overview of the law that governs public records.

84. *See* Administrative Office of the U.S. Courts, *News Release*, *at* http://privacy.uscourts.gov/Press.htm (Feb. 16, 2001).

85. *See* Brian Krebs, *Public Hearing Over Online Court Documents Planned,* NEWSBYTES, Feb. 20, 2001, *at* http://www.newsbytes.com/news/ 01/162183.html.

86. *See* Office of Judges Programs of the Admin. Office of the United States Courts, *Privacy and Access to Electronic Case Files in the Federal Courts* at 6, *at* http://www.uscourts.gov/privacyn.htm (Dec. 15, 1999).

87. *Id.*

1. The Common Law, Court Records, and Protective Orders

At common law, English courts rarely encountered cases involving an individual seeking to gain access to government documents.[88] In certain limited circumstances, English courts recognized that the public could inspect certain government records.[89] If an individual were denied the ability to inspect, she could seek to enforce her right through mandamus; however, there were severe restrictions on the ability to use mandamus to obtain access to records. Individuals could not bring mandamus on their own and had no right to access government documents for their own personal purposes.[90] There was a narrow exception to this rule, however, when the seeker of a record needed to obtain it for use in litigation. Courts would generally "not issue the extraordinary writ of mandamus to enforce a private right of inspection, unless the purpose was to use it in some pending or prospective suit."[91] In contrast, access to court records, as opposed to other public records, was broader. When documents were introduced into evidence, individuals were permitted access.[92]

Early U.S. courts followed the English practice.[93] In many jurisdictions, an individual seeking to inspect non-court records for the general public interest (to expose graft or corruption, or to bring government activities into the sunlight), could not bring suit in her own name; only the Attorney General could bring an action on her behalf.[94] However, if the person had a "special interest" in examining the records (for example, to provide evidence in a legal proceeding), the individual could bring a petition for mandamus on her own.[95] As one court articulated the rule in 1882,

> The individual demanding access to, and inspection of public writings must not only have an interest in the matters to which they relate, a direct, tangible interest, but the inspection must be sought for some specific and legitimate purpose.[96]

88. *See* HAROLD L. CROSS, THE PEOPLE'S RIGHT TO KNOW 25 (1953).

89. *See, e.g.*, Nowack v. Fuller, 219 N.W. 749, 750-51 (Mich. 1928). *See generally* William Ollie Key, Jr., *The Common Law Right to Inspect and Copy Judicial Records: In Camera or On Camera*, 16 GA. L. REV. 659 (1982).

90. *Nowack*, 219 N.W. at 750-51.

91. *Id.* at 751.

92. *See* CROSS, *supra* note 88, at 135; Key, *supra* note 89, at 666.

93. *See* CROSS, *supra* note 88, at 26.

94. *Nowack*, 219 N.W. at 751.

95. *See id.* at 751; CROSS, *supra* note 88, at 25-26; Comment, *Public Inspection of State and Municipal Documents: "Everybody, Practically Everything, Anytime, Except . . . ."*, 45 FORDHAM L. REV. 1105, 1108 (1977).

96. Brewer v. Watson, 71 Ala. 299, 305 (1882). Some jurisdictions, such as Michigan and Rhode Island, recognized a broader right to access than the English rule early on. *See* Burton v. Tuite, 44 N.W. 282, 285 (Mich. 1889); *In re* Caswell, 29 A. 259, 259 (R.I.

In several jurisdictions, the common law evolved to abandon the view that access to documents was limited only to litigation purposes.[97] The "interest" required for inspection was expanded to include the interest in redressing public wrongs and monitoring government functions.[98] Under the modern common law rule in many jurisdictions, a person can inspect public records when the purpose is not improper and access is not harmful to others.[99] One of the most commonly mentioned improper purposes for accessing public records was "to satisfy idle curiosity or for the purpose of creating a public scandal."[100] Therefore, government officials could deny access to information based on the person's reason for seeking the information.[101] Today, however, this discretion has been significantly reduced by state and federal freedom of information laws.

In contrast to public records, the right to inspect court records was generally broader and was shaped by the supervisory authority of the courts.[102] The courts had a long tradition of permitting open access to court records, and access was rarely limited based on the purposes for which the records were sought.[103]

In 1978, in *Nixon v. Warner Communications, Inc.,*[104] the Supreme Court took notice of the right to inspect and copy both public records and court records: "It is clear that the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents."[105] The *Nixon* Court noted that "[i]n

1893).

97. *See* CROSS, *supra* note 88, at 26.

98. *See id.* at 27; *Public Inspection, supra* note 95, at 1108.

99. *See* CROSS, *supra* note 88, at 29. As one court explained, "We cannot find any valid basis in our society for the imposition of the requirement of the interest stated in the common-law rule as a prerequisite to the right to inspect public records." City of St. Matthews v. Voice of St. Matthews, Inc., 519 S.W.2d 811, 815 (Ky. Ct. App. 1974).

100. *Voice of St. Matthews*, 519 S.W.2d at 815; Husband, C. v. Wife, C., 320 A.2d 717, 723 (Del. 1974) (characterizing the common law approach as permitting access to judicial records if a person "has an interest therein for some useful purpose and not for mere curiosity").

101. *See, e.g.*, Mans v. Lebanon Sch. Bd., 290 A.2d 866, 867 (N.H. 1972); *see also* Matthew D. Bunker et al., *Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology*, 20 FLA. ST. U. L. REV. 543, 556 (1993) ("Most states depended on the discretion of agencies, or on the common law, to provide public access to government records until they were inspired by the federal FOIA to codify the concept of open government. The common law had varied among states, with most courts requiring a person requesting a record to have a legitimate interest in, and a useful purpose for, the requested record.").

102. *See* Key, *supra* note 89, at 668 ("Consistent with state court decisions, federal courts historically allowed, absent sensitive circumstances, anyone to inspect and copy judicial records for any purpose.").

103. *See* CROSS, *supra* note 88, at 135-36.

104. 435 U.S. 589 (1978).

105. *Id*. at 597.

contrast to the English practice, American decisions generally do not condition enforcement of this right on a proprietary interest in the document or upon a need for it as evidence in a lawsuit."[106] The Court explained that the right to access public records is justified by "the citizen's desire to keep a watchful eye on the workings of public agencies, and in a newspaper publisher's intention to publish information concerning the operation of government."[107]

The right of access to court records differs from the right to access other public records. As the *Nixon* Court noted, the common law right of access applies to court records; however, the right is not absolute.[108] The Court observed that "[e]very court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes."[109] The Court noted that public access has been denied where records would have been used to promote scandal by revealing embarrassing personal information, to serve as "reservoirs of libelous statements for press consumption," or to harm a litigant's business.[110] The decision over whether to permit access "is one best left to the sound discretion of the trial court, a discretion to be exercised in light of the relevant facts and circumstances of the particular case."[111] Thus, the common law protects privacy in the context of court records by giving judges discretion over access to their records and proceedings.[112]

In the federal court system, pursuant to Federal Rule of Civil Procedure 26(c), judges have discretion "for good cause shown" to issue protective orders to shield information from disclosure where it might cause a party "annoyance, embarrassment, oppression, or undue burden or expense."[113] Rule 26(c) was part of the original version of the Federal Rules of Civil Procedure adopted in 1938.[114] The Federal Rules explicitly provided for protective orders because the Rules significantly expanded pretrial discovery to encompass almost all information that could

106. *Id*. (citation omitted).

107. *Id*. at 598 (citations omitted).

108. *Id.*; *see also* United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997) (citing *Nixon* for the proposition that right of access is not absolute); United States v. Amodeo, 71 F.3d. 1044, 1047-50 (2d Cir. 1995) (applying a balancing test to determine if public access is proper).

109. *Nixon*, 435 U.S. at 598.

110. *Id*.

111. *Id*. at 599.

112. Judicial discretion over access is, of course, constrained by the First Amendment. *See infra* Part III.A.

113. FED. R. CIV. P. 26(c).

114. *Id.*

be of help in the preparation of the case.[115] This broad expansion created a new threat to privacy, as the Rules did not differentiate between private and non-private information. To protect privacy, as well as other interests such as trade secrets, Rule 26(c) was designed to limit the use of discoverable information beyond the context of the litigation.[116] Most states have modeled their discovery provisions, including protective orders, on the Federal Rules of Civil Procedure.[117]

Federal courts have held that there is a presumption in favor of access to court records.[118] When seeking a protective order, the party seeking to maintain the confidentiality of a record has the burden of overcoming the presumption in favor of access.[119] Courts balance a party's interest in privacy against the public interest in disclosure.[120] If a court decides to deny access, it "must set forth substantial reasons."[121]

Generally, documents disclosed to parties in discovery but not filed in court are not subject to the common law right of access.[122] According to the Supreme Court in *Seattle Times Co. v. Rhinehart*,[123] "pretrial depositions and interrogatories are not public components of a civil trial. Such proceedings were not open to the public at common law, and, in general, they are conducted in private as a matter of modern practice."[124]

Courts retain discretion to issue special orders to keep certain proceedings and information confidential. A court will sometimes, under very limited circumstances, seal court proceedings such as trials.[125] Courts can seal court records if the parties' desire for confidentiality outweighs the need for public access.[126] A trial court can permit a plain-

115. *See* Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 447 (1991).

116. *Id.*

117. Seattle Times Co. v. Rhinehart, 467 U.S. 20, 29 (1984).

118. *See, e.g.*, United States v. El-Sayegh, 131 F.3d 158, 159 (D.C. Cir. 1997); Pansy v. Borough of Stroudsburg, 23 F.3d 772, 782 (3rd Cir. 1994); *SEC v. Van Waeyenberghe*, 990 F.2d 845, 848 (5th Cir. 1993); Anderson v. Cryovac, Inc., 805 F.2d 1, 13 (1st Cir. 1986).

119. FTC v. Standard Fin. Mgmt. Corp., 830 F.2d 404, 408-10 (1st Cir. 1987).

120. *See, e.g.*, *Nixon*, 435 U.S. at 602.

121. *See, e.g.*, United States v. Beckham, 789 F.2d 401, 413 (6th Cir. 1986).

122. *Rhinehart*, 467 U.S. at 33.

123. *Id*.

124. *Id.* (citations omitted).

125. *See, e.g.*, Unabom Trial Media Coalition v. United States Dist. Court for E. Dist. of Cal., 183 F.3d 949, 951 (9th Cir. 1999). The court must find that those excluded have "a reasonable opportunity to state their objections" and the court must make the following specific factual findings: that "(1) closure serves a compelling interest; (2) there is a substantial probability that, in the absence of closure, this compelling interest would be harmed; and (3) there are no alternatives to closure that would adequately protect the compelling interest." *Id*.

126. *See* Pansy v. Borough of Stroudsburg, 23 F.3d 772, 786 (3d Cir. 1994); CAL. CT.

tiff to proceed anonymously with the use of a pseudonym.[127] Courts can also permit anonymous juries when jurors might otherwise be placed in danger.[128] These decisions, however, are within the discretion of the trial court,[129] and courts differ greatly in the exercise of their discretion. For example, one court permitted a woman raped at a train station who sued Amtrak to keep her identity secret because of the potential embarrassment she would suffer if the fact she was raped became widely disclosed.[130] In contrast, another court held that a victim of sexual assault could not sue her assailant for civil damages under a pseudonym because "[f]airness requires that she be prepared to stand behind her charges publicly" and because she was "seeking to vindicate primarily her own interests."[131]

In sum, under modern American common law, there is a limited right to access public records so long as one's purpose is not improper. For court records, the common law right to access follows the supervisory authority of the courts, and judges have significant discretion in granting or denying access.[132]

2. Freedom of Information Laws

State legislatures gradually replaced or supplemented the court-created right of the nineteenth and early twentieth centuries with open records statutes, which generally mandated open access.[133] These statutes are often entitled or referred to as "freedom of information," "open ac-

R. 243.1(d)(1)-(5) (providing that a court may seal records if there is an "overriding interest that overcomes the right of public access to the record" and the sealing is "narrowly tailored" and "[n]o less restrictive means exist to achieve the overriding interest").

127. *See, e.g.,* Doe v. Shakur, 164 F.R.D. 359, 360 (S.D.N.Y. 1996); Doe v. Bell Atl. Bus. Sys. Servs., Inc., 162 F.R.D. 418, 420 (D. Mass. 1995); *see also* James v. Jacobson, 6 F.3d 233, 238-42 (4th Cir. 1993); Doe v. Frank, 951 F.2d 320, 322-24 (11th Cir. 1992). The use of pseudonyms is rare and reserved only for exceptional cases. "It is the exceptional case in which a plaintiff may proceed under a fictitious name." *Id.* at 323.

128. Reporters Comm. for the Freedom of the Press, *Court Access: The Privacy Paradox*, *at* http://www.rcfp.org/pp_pt3.html (last visited June 29, 2002).

129. *See Pansy*, 23 F.3d at 786.

130. *See* Doe v. Nat'l R.R. Passenger Corp., No. CIU.A. 94-5064, 1997 WL 116979, at *1 (E.D. Pa. Mar. 11, 1997).

131. *Shakur*, 164 F.R.D. at 361; *see also Bell Atl. Bus. Sys. Servs.*, 162 F.R.D. at 422 (D. Mass. 1995) (rejecting use of pseudonym for plaintiff alleging a sexual assault by her supervisor at work and that she might have been infected with HIV).

132. *See, e.g.*, United States v. McVeigh, 119 F.3d 806, 811-15 (10th Cir. 1997).

133. *See* Roger A. Nowadzky, *A Comparative Analysis of Public Records Statutes*, 28 URB. LAW. 65, 69-70 (1996); Jason Lawrence Cagle, Note, *Protecting Privacy on the Front Page: Why Restrictions on Commercial Use of Law Enforcement Records Violate the First Amendment*, 52 VAND. L. REV. 1421, 1422 n.2 (1999). While some states' FOIAs replaced the common law, courts in some states have held that the state's FOIA operates as an additional right of access to the common law. *See id.*

cess," "right to know," or "sunshine" laws. States were initially slow in enacting statutory public access rights; by 1940, only twelve states had open records statutes.[134]

In 1946, the federal Administrative Procedures Act (APA) contained a limited provision for disclosure of government records.[135] However, under § 3 of the APA, information could be withheld if it involved "any function of the United States requiring secrecy in the public interest" or was "required for good cause to be held confidential."[136]

In 1966, Congress passed the Freedom of Information Act (FOIA), dramatically reforming public access to government records. According to the Senate Report for FOIA, the APA was "full of loopholes which allow agencies to deny legitimate information to the public" and that information was often "withheld only to cover up embarrassing mistakes or irregularities."[137] When he signed the FOIA into law, President Lyndon Johnson declared,

> This legislation springs from one of our most essential principles: A democracy works best when the people have all the information that the security of the Nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest.[138]

As Fred Cate observes, the FOIA serves three purposes: "first and most important, ensure public access to the information necessary to evaluate the conduct of government officials; second, ensure public access to information concerning public policy; and third, protect against secret laws, rules and decisionmaking."[139]

Under FOIA, "any person" (including associations, organizations, and foreign citizens) may request "records" maintained by an executive agency.[140] FOIA does not apply to records kept by Congress or the Judiciary.[141] Requesters of records do not need to state a reason for requesting records.[142]

---

134. *See Public Inspection*, *supra* note 95, at 1107.

135. 5 U.S.C. § 1002 (1946).

136. *Id.*, *superceded by* the Freedom of Information Act, 5 U.S.C. § 552 (2000). For a discussion of the ineffectiveness of the APA, see Bunker et al., *supra* note 101, at 552-53.

137. S. REP. NO. 89-813, at 3 (1965). The House Report likewise noted that under § 3 of the APA, "[g]overnment agencies whose mistakes cannot bear public scrutiny have found 'good cause' for secrecy." H.R. REP. NO. 89-1497 (1966), *reprinted in* 1966 U.S.C.C.A.N. 2418, 2423.

138. 2 PUBLIC PAPERS OF THE PRESIDENTS OF THE UNITED STATES: LYNDON B. JOHNSON 699 (1967), *quoted in* H.R. REP. No. 104-795, at 8 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3448, 3451.

139. Fred H. Cate et al., *The Right to Privacy and the Public's Right to Know: The "Central Purpose" of the Freedom of Information Act*, 46 ADMIN. L. REV. 41, 65 (1994).

140. 5 U.S.C. § 552(a)(3)(A) (2000).

141. *See id.* § 552(f).

142. *See, e.g.*, United States Dep't of Justice v. Reporters Comm. for Freedom of the

Today, all fifty states have open records statutes, a majority of which are modeled after the FOIA.[143] Like the federal FOIA, state FOIAs are justified by a strong commitment to openness and transparency.[144]

Many states, following FOIA, eliminated the common law requirement of requesters establishing an interest in obtaining the records.[145] Indeed, the federal FOIA and many state FOIAs allow information to be obtained by anybody for any reason.[146] Most state FOIAs contain a presumption in favor of disclosure.[147]

Open access laws never mandate absolute disclosure. They contain exemptions, typically (although not always) including an exemption to protect individual privacy. The federal FOIA contains nine enumerated exemptions to disclosure, two of which pertain to privacy. Exemption 6 exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[148] Exemption 7(C) exempts from disclosure "records or information compiled for law enforcement purposes . . . [which] could reasonably be expected to constitute an unwarranted invasion of personal privacy.[149] If possible, private information can be deleted from records, and the redacted records disclosed to the requester.[150]

The federal FOIA does not require that a person be given notice that

Press, 489 U.S. 749, 771 (1989).

143. Jackson, *supra* note 26, at 111; Nowadzky, *supra* note 133, at 65-66.

144. *See, e.g.*, DEL. CODE ANN. tit. 29, § 10001 (1997) (stating that "it is vital that citizens have easy access to public records in order that the society remain free and democratic"); 5 ILL. COMP. STAT. ANN. 140/1 (1) (West 1993) (stating that the right to inspect public records "is necessary to enable the people to fulfill their duties of discussing public issues fully and freely"); *see also* IOWA CODE ANN. § 22.2(1) (2001); N.C. GEN. STAT. § 132-6(a) (1999); Mans v. Lebanon Sch. Bd., 290 A.2d 866, 867 (N.H. 1972).

145. *See, e.g.*, N.C. GEN. STAT. § 132-6(b) (1999).

146. *See Reporters Comm.*, 489 U.S. at 771 (stating that the federal FOIA provides the same access rights to the general public as it does to those asserting a particular interest in a document); Nowadzky, *supra* note 133, at 78 (noting that many state FOIAs eliminated the requirement of demonstrating need or stating purpose); *see also* IOWA CODE ANN. § 22.2(1) (2001); N.C. GEN. STAT. § 132-6(b) (1999) ("No person . . . shall be required to disclose the purpose or motive for the request."); State Employees Ass'n v. Dep't of Mgmt. and Budget, 404 N.W.2d 606, 616 (Mich. 1987) (holding that Michigan's FOIA does not require a person to justify her request for access); *Mans*, 290 A.2d at 867 (describing the elimination of common law discrimination based on the purpose of the record seeker in New Hampshire's Right to Know Law).

147. Nowadzky, *supra* note 133, at 66 & n.6 (conducting a comprehensive survey of all state FOIAs as to the presumption of disclosure).

148. 5 U.S.C. § 552(b)(6) (2000).

149. *Id.* § 552(b)(7)(C).

150. *See id.* § 552(b).

his or her personal information is encompassed within a FOIA request.[151] Even if an individual finds out about the request, she has no right under FOIA to prevent or second-guess an agency's decision to disclose the records. FOIA does not require that the government withhold information.[152] It is up to the government agency to assert and to litigate the individual's privacy interest.[153]

State FOIA privacy exemptions come in myriad shapes and sizes. Many state sunshine laws contain a privacy exemption similar to that found in the FOIA,[154] applying when disclosure would constitute a "clearly unwarranted" invasion of privacy."[155] However, not all state FOIAs have a privacy exemption. Pennsylvania's Right to Know Act[156] does not contain a privacy exemption; it prohibits only access to records "which would operate to the prejudice or impairment of a person's reputation or personal security."[157] As one court stated, "the phrase 'personal security' does not mean 'personal privacy.'"[158] Ohio's Public Records Act does not contain any privacy exemption.[159]

The privacy exemptions in state FOIAs have often been expanded or constricted by judicial interpretation.[160] In applying FOIA privacy exemptions, many states go along with the federal FOIA approach and bal-

151. Heather Harrison, Note, *Protecting Personal Information from Unauthorized Government Disclosures*, 22 MEMPHIS ST. U. L. REV. 775, 787 (1992).

152. Cate et al., *supra* note 139, at 49; Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 593 (1995).

153. In contrast, companies seeking to protect trade secrets can initiate actions on their own to protect their information in what is known as a "reverse-FOIA" lawsuit. *See* Harrison, *supra* note 151, at 783.

154. Jackson, *supra* note 26, at 114.

155. *See, e.g.,* D.C. CODE ANN. § 2-534(a)(2) (Lexis 2001) (applying a privacy exception where disclosure "would constitute a clearly unwarranted invasion of personal privacy"); MICH. COMP. LAWS ANN. § 15.243(1)(a) (1994) (stating that the privacy exception applies "where the public disclosure of the information would constitute a clearly unwarranted invasion of an individual's privacy").

156. PA. CONS. STAT. ANN. §§ 66.1-66.4 (2000).

157. *Id.* § 66.1(2).

158. Kanzelmeyer v. Eger, 329 A.2d 307, 310 (Pa. Commw. Ct. 1974).

159. *See* 1 OHIO REV. CODE ANN. § 149.43(A)(1) (Anderson Supp. 2001) (listing exceptions to disclosure); *see also* State *ex rel.* Plain Dealer Pub. Co. v. Cleveland, 661 N.E.2d 187, 193-95 (Ohio 1996) (Resnick, J., concurring) (criticizing the lack of a privacy exception in Ohio's Public Records Act).

160. For example, in *In re Rosier*, 717 P.2d 1353, 1358 (Wash. 1986), the court expanded the scope of the personal privacy exception under Washington's Public Disclosure Act to encompass anything that is connected to an individual or that reveals something "unique" about an individual. A number of states have held that certain forms of public record information (such as names and addresses) are not "private" because they do not involve intimate or embarrassing details. *See supra* notes 155, 159 and accompanying text.

ance interests of privacy against the interests of public access.[161] However, states have adopted widely differing approaches often stemming from vastly different judicial conceptions of privacy.

It is critical to note that the federal FOIA was passed before the rise of computer databases. In 1996, due to the development of modern computer technology, Congress passed the Electronic Freedom of Information Amendments (E-FOIA)[162] which amended the FOIA to enable any person to access electronic documents (including e-mail messages) in the same way he or she could access paper documents.[163] Agencies must establish an index to the documents they possess and make the index available on the Internet.[164] Further, agencies must establish "electronic reading rooms" where people can read documents online.[165] The electronic reading room must contain documents that are likely to be requested multiple times.[166] As states computerize their records, these computer databases are often encompassed within the broad definition of "public records" in many state FOIAs.[167] Some states explicitly include computerized information in their definitions of public records.[168]

3. Privacy Acts

The federal Privacy Act was borne out of fears of computerized databases. Beginning in the 1960s and 1970s, social commentators began to voice privacy concerns about computerized databases.[169] People feared the eventual creation of a national database using the Social Security number as the primary identifier.[170] Throughout the mid-1960s and 1970s, Congress devoted a significant amount of attention to the prob-

161. Nowadzky, *supra* note 133, at 79. At least one state has rejected such an approach, opting to apply the exception by determining solely whether such information is private (but adopting a rather narrow conception of privacy). *See* State Employees Ass'n v. Dep't of Mgmt. & Budget, 404 N.W.2d 606, 611-13 (Mich. 1987).

162. Pub. L. No. 104-231, 110 Stat. 3048 (1996) (codified as amended at 5 U.S.C. § 552(a)(2) (2000)).

163. 5 U.S.C. § 552(a)(2) (2000).

164. *Id.*

165. *Id.*

166. *Id.*

167. Nowadzky, *supra* note 133, at 70.

168. *Id.* at 70, 75 & n.16.

169. *See, e.g.*, MYRON BRENTON, THE PRIVACY INVADERS 14 (1964); MILLER, *supra* note 52; NOMOS XII: PRIVACY (J. Ronald Pennock & J.W. Chapman eds., 1971); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); WESTIN & BAKER, *supra* note 6, at 3-5; Kenneth L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 359-63 (1966). *See generally* Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968).

170. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 95 (1995).

lem.[171] In 1973, the Department of Health, Education, and Welfare (HEW) issued a profoundly influential report about computer databases, condemning the trend toward making the Social Security number a universal identifier.[172] The report noted a growing public "distrust" with computer record-keeping systems[173] and no "coherent or conceptually unified approach to balancing the interests of society and the organizations that compile and use records against the interests of individuals who are the subjects of records."[174] The report recommended that a code of Fair Information Practices should be enacted:

> • There must be no personal data record-keeping systems whose very existence is secret.
>
> • There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> • There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
>
> • There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> • Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[175]

In 1974, after years of apprehension over computer databases, Congress finally passed the Privacy Act.[176] The Privacy Act, embodying the Fair Information Practices, gives individuals the right to access and correct information about themselves held by federal agencies and restricts federal agencies' collection, use, and disclosure of personal information. According to the Act, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . ."[177] Agencies can only maintain information about individuals that is "relevant and necessary" to accomplish a particular purpose of the agency.[178] When collecting personal information, agencies must inform individuals about the purposes for which the information is to be used, and the effects on the

171. *Id.* at 71-74.

172. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 108-35 (1973) [*hereinafter* HEW 1973 REPORT].

173. *See id*. at 28.

174. *Id*. at 35.

175. *Id.* at 41-42.

176. *See* REGAN, *supra* note 170, at 8.

177. 5 U.S.C. § 552a(b) (2000).

178. *Id.* § 552a(e)(1).

individual for not providing any of the requested data.[179] Agencies must ensure "security and confidentiality of records."[180] Further, individuals can review their records upon request[181] and ask an agency to correct inaccurate data.[182] The Privacy Act authorizes individuals to bring civil actions if agencies do not correct an individual's record, fail to give an individual access to her record, maintain a shoddy record that results in an adverse determination against an individual, or fail to comply with any provision of the Privacy Act that results in an adverse effect on an individual.[183]

Additionally, the Privacy Act gives citizens certain rights regarding the use of their Social Security numbers. Unlike the rest of the Privacy Act, which applies only to federal agencies, § 7 of the Privacy Act makes it "unlawful for any Federal, State or local government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."[184]

The Privacy Act, however, failed to bring the growing uses of Social Security numbers under control. The use of the Social Security number continued to escalate after the Privacy Act.[185] The reason for this failure arose in part because the Privacy Act's Social Security number provisions are limited only to the public sector.[186] As a result, Social Security numbers are frequently collected by private sector entities, and it is currently legal for these entities to sell or disclose Social Security numbers. Further, Congress frequently made exceptions to the Act to expand the uses of SSNs.[187]

In addition to the problems with its regulation of Social Security numbers, the Privacy Act has other significant limitations. The Privacy

179. *Id.* § 552a(e)(3).

180. *Id.* § 552a(e)(10).

181. *Id.* § 552a(d)(1).

182. *Id.* § 552a(d)(2).

183. *Id.* § 552a(g)(1).

184. *Id.* § 552a note.

185. *See* U.S. GEN. ACCOUNTING OFFICE, REP. TO THE CHAIRMAN, SUBCOMM. ON SOC. SEC., COMM. ON WAYS AND MEANS, HOUSE OF REPRESENTATIVES: SOCIAL SECURITY: GOV'T AND COMMERCIAL USE OF THE SOC. SEC. NUMBER IS WIDESPREAD 4, 7-12 (1999).

186. *See id.* at 78; *see also Use and Misuse of Social Security Numbers: Hearing Before the Subcomm. on Soc. Sec. of the House Comm. on Ways and Means*, 106th Cong. (2000) (testimony of Marc Rotenberg, director of the Electronic Privacy Information Center) (urging new legislation to protect widespread uses of Social Security numbers).

187. PHILIPPA STRUM, PRIVACY 50-51 (1998); Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 569 (1998).

Act is limited only to the public sector.[188] The Act applies only to federal, not state and local agencies. Further, the Act has been eroded by about a dozen exceptions.[189] For example, agencies can disclose information without the consent of individuals to the Census Bureau, to law enforcement entities, to Congress, and to consumer reporting agencies.[190] When FOIA requires that information be released, the Privacy Act does not apply.[191] Nor does the Privacy Act apply to court records.[192]

The broadest exception is that information may be disclosed for any "routine use" if disclosure is "compatible" with the purpose for which the agency collected the information.[193] The "routine use" exception has repeatedly been criticized as being a gigantic loophole.[194] For example, in 1977, the federal government began matching its computer employee records with the records of people receiving federal benefits to detect fraud.[195] Records in different government benefit programs were also compared.[196] Through this automated investigatory technique, the government investigated millions of people quickly, efficiently, and secretly. This sharing of records between different government agencies, ordinarily a violation of the Privacy Act, was justified under the "routine use" exception.[197] In 1988, Congress finally passed a law regulating this practice,[198] but the law has been strongly criticized as providing scant sub-

188. Although privacy advocates in Congress wanted the Act to extend to the private sector, President Ford threatened to veto the law if it extended beyond public records. Sandra L. Macklin, *Students' Rights in Indiana: Wrongful Distribution of Student Records and Potential Remedies*, 74 IND. L.J. 1321, 1325 (1999).

189. *See* STRUM, *supra* note 187, at 50-51.

190. 5 U.S.C. § 552a(b)(1)-(12) (2000).

191. *See id.* § 552a(t)(2); Martin v. Office of Special Counsel, Merit Sys. Prot. Bd., 819 F.2d 1181, 1184 (D.C. Cir. 1987).

192. 5 U.S.C. §§ 551(1)(B), 552(f); *see also* United States v. Frank, 864 F.2d 992,1013 (3d Cir. 1988); Warth v. Dep't of Justice, 595 F.2d 521, 522-23 (9th Cir. 1979).

193. 5 U.S.C. §§ 552a(b)(3).

194. *See* Schwartz, *supra* note 152, at 585-87 (describing criticism of the "routine use exemption" and advancing his own criticisms).

195. *See* REGAN, *supra* note 170, at 86. As Priscilla Regan has noted, surprisingly, the Fourth Amendment implications of computer matchings have not been litigated. *See id.* at 90.

196. *See* Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 198-99 (Philip E. Agre & Marc Rotenberg eds., 1997).

197. *See* REGAN, *supra* note 170, at 87.

198. *See* Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a (a)(8)-(13), (e)(12), (o)-(r), (u) (2000)). The CMPPA requires agencies to formulate procedural agreements before exchanging computerized record systems and establishes Data Integrity Boards within each agency to oversee matching, requires agencies to perform a cost-benefit analysis of proposed matching endeavors, and requires agencies to notify individuals of the termination of benefits due to computer matching and permit them an opportunity to refute the termination. *Id.*

stantive guidance and having little practical effect.[199] As Robert Gellman correctly notes with regard to the "routine use" exception, "[t]his vague formula has not created much of a substantive barrier to external disclosure of personal information."[200]

Although the Privacy Act requires an individual's permission before his or her records can be disclosed, redress for violations of the Act is virtually impossible to obtain.[201] The Privacy Act provides individuals with a monetary remedy for disclosures of personal information only if the disclosure was made "willfully and intentionally."[202] This restriction on recovery of damages fails to redress the most common form of mistakes—those due to carelessness. This leaves little incentive to bring suit.[203] For example, in *Andrews v. Veterans Administration,*[204] the Veterans Administration released inadequately redacted personnel records of nurses resulting in what the court called a "substantial" violation of nurses' privacy. However, the agency could not be sued under the Privacy Act because it acted negligently, not willfully.[205] Paul Schwartz aptly notes that "individuals who seek to enforce their rights under the Privacy Act face numerous statutory hurdles, limited damages, and scant chance to effect an agency's overall behavior."[206]

Although several states have promulgated statutes protecting privacy in certain narrow contexts, less than a third have enacted a general privacy law akin to the Privacy Act.[207] As Paul Schwartz observes, most

199. *See* U.S. GEN. ACCOUNTING OFFICE, COMPUTER MATCHING: QUALITY OF DECISIONS AND SUPPORTING ANALYSES LITTLE AFFECTED BY 1988 ACT 3 (1993) ("[T]he implementation of these new procedures does not appear to have had major effects on the most important review process. . . ."); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 101 (1996); Schwartz, *supra* note 152, at 588 (the CMPPA "creates no substantive guidelines to determine when matching is acceptable"); INFO. POL'Y COMM., NAT'L INFO. INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE: DRAFT FOR PUBLIC COMMENT 10, *at* http://www.iitf.doc.gov/ipc/privacy.htm (1997).

200. Gellman, *supra* note 196, at 198.

201. *See id*. (pointing out that there is no administrative process in place to challenge agencies' disclosures); Harrison, *supra* note 151, at 787 (noting that "some persons who may have had their privacy violated by unauthorized agency actions received no remedy for their injury"); Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 975 n.118 (1991) (stating that the "individual's ability to be made whole" has been "crippled" under the Privacy Act).

202. 5 U.S.C. § 552a(g)(4) (2000).

203. Coles, *supra* note 201, at 975 n. 118.

204. 838 F.2d 418 (10th Cir. 1988).

205. *Id.* at 425.

206. Schwartz, *supra* note 152, at 596.

207. *See id.* at 605. For a compilation of state privacy laws, see ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 3-66 (1997).

states lack "omnibus data protection laws" and have "scattered laws [that] provide only limited protections for personal information in the public sector."[208]

4. Access and Use Restrictions

Confronted with increased information trade, some states have attempted to restrict access to personal information in public records as well as certain uses of personal information obtained from public records. In the last decade, a number of states have enacted access restrictions for some of their public records, often excluding access for the commercial uses of soliciting business or marketing services or products. For example, Georgia amended its public records law in 1991 making it unlawful to access law enforcement or motor vehicle accident records "for any commercial solicitation of such individuals or relatives of such individuals."[209] In 1992, Louisiana restricted access to accident records for commercial solicitation purposes.[210] Kentucky, in response to "a public groundswell [that] developed against the release of accident reports to attorneys and chiropractors,"[211] amended its public records law in 1994 to restrict access for these and other commercial uses.[212] In 1996, Florida restricted the access of driver information in traffic citations from those seeking it for commercial solicitation purposes.[213] Colorado prohibited access to criminal justice records unless those seeking access signed a statement that such records would not be used "for the direct solicitation of business for pecuniary gain."[214] California recently restricted access to arrest records by providing that the records "shall not be used directly or indirectly to sell a product or service . . . and the requester shall execute a declaration to that effect under penalty of perjury."[215] Almost half of the states prohibit the commercial use of voter registration records.[216]

208. Schwartz, *supra* note 152, at 605.

209. GA. CODE ANN. § 35-1-9 (Harrison 1998).

210. LA. REV. STAT. ANN. § 32:398(H) (West Supp. 2002).

211. Amelkin v. McClure, 168 F.3d 893, 896 (6th Cir. 1999).

212. KY. REV. STAT. ANN. § 189.635 (Michie Supp. 2001).

213. FLA. STAT. ANN. § 316.650(11) (West 2001). The law explicitly noted that it did not apply to media publication or "when used to inform a person of the availability of driver safety training." *Id*.

214. COLO. REV. STAT. § 24-72-305.5 (2001).

215. CAL. GOV'T CODE § 6254(f)(3) (West Supp. 2002).

216. *See* Rajiv Chandrasekaran, *Government Finds Information Pays*, WASH. POST, Mar. 9, 1998, at A1. For example, California provides that voter registration lists may only be released to candidates, political committees, or for "election, scholarly, journalistic, political, or governmental purposes." CAL. ELEC. CODE § 2194(a)(2) (West Supp. 2002). Florida prohibits the use of lists of registered voters for any use other than uses "related to elections, political or governmental activities, voter registration, or law enforcement." FLA. STAT. ANN. § 98.095(2) (West Supp. 2002).

The federal government also has certain access restrictions for its public records. Pursuant to the Federal Election Campaign Act (FECA), reports of contributors to political committees are "available for public inspection . . . except that any information copied from such reports . . . may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes."[217]

In sum, although in certain contexts laws are beginning to limit access to public records for some purposes, the vast majority of public records remain virtually unrestricted in access.

5. Restrictions on State Information Practices

In a rare instance, the federal government has directly regulated the states' use of public records. In 1994, Congress passed the Driver's Privacy Protection Act (DPPA) to curtail the practice of many states of selling their motor vehicle records to marketers.[218] Pursuant to DPPA, "A State department of motor vehicles . . . shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record . . . ." [219]

Originally, DPPA provided that if an individual did not opt out, then information could be used for any purpose. In 1999, Congress amended DPPA, changing the opt-out provision to an opt-in requirement, forcing states to require a driver's consent before disclosing personal information to marketers.

In *Reno v. Condon*,[220] the Supreme Court concluded that DPPA was a proper exercise of Congress' authority to regulate interstate commerce:

> The motor vehicle information which the States have historically sold is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized solicitations. The information is also used in the stream of interstate commerce by various public and private entities

217. 2 U.S.C. § 438(a)(4) (2000). Although the FEC occasionally uses decoy names to check to see if candidates are engaging in improper uses of the records, the FEC has not, according to critics, done much to investigate reports of abuse. *See* Chandrasekaran, *supra* note 216, at A1.

218. Pub. L. No. 103-322, 108 Stat. 2099 (1994) (codified as amended at 18 U.S.C. §§ 2721-25 (2000)).

219. 18 U.S.C. § 2721(a) (2000) ("Under the amended DPPA, States may not imply consent from a driver's failure to take advantage of a state-afforded opportunity to block disclosure, but must rather obtain a driver's affirmative consent to disclose . . . personal information for use in surveys, marketing, solicitations, and other restricted purposes . . . .").

220. 528 U.S. 141, 144-45 (2000).

for matters related to interstate motoring.[221]

The Court correctly recognized that information is an essential aspect of commerce and that it is a matter appropriately within Congress's power to regulate. Further, the Court concluded that DPPA does not "require the states in their sovereign capacity to regulate their own citizens"[222] because DPPA "regulates the States as the owners of databases" and does not require them to enact regulation or to assist in enforcing federal statutes concerning private individuals.[223]

Although DPPA is an important first step in bringing state public records systems under control, DPPA applies only to motor vehicle records and does not forbid the dissemination of all the other public records states maintain.

6. Conclusion: The Regulatory Regime of Public Records

As illustrated above, states vary significantly in what information they make publicly available. Often such decisions are made by agencies and bureaucrats or left to the discretion of the courts. Decisions as to the scope of access—whether one must obtain a record by physically going to a local agency office, by engaging in correspondence by mail, or by simply downloading it from the Internet—are often made by local bureaucrats. Frequently, it is up to the individual to take significant steps to protect privacy, such as overcoming the presumption of access to court records. In many instances, individuals are never even given notice or an opportunity to assert a privacy interest when records containing their personal information are disclosed.

Differing protection of personal information with no minimum floor of protection presents significant problems in today's age of increasing mobility and information flow.[224] There is no federal law establishing a baseline for the regulation of public records. Thus, personal information is regulated by a bewildering assortment of state statutory protections, which vary widely from state to state. As Paul Schwartz notes, "[s]tate data protection law in the United States is largely unchartered territory."[225] "Some data protection exists in every state," he observes, "but no two states have adopted precisely the same system of regulation."[226]

This chaotic state of affairs is troublesome in an Information Age

221. *Id*. at 148.

222. *Id*. at 151.

223. *Id*.

224. *See* Bruce D. Goldstein, Comment, *Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection*, 41 EMORY L.J. 1185, 1205-06 (1992) (critiquing the lack of uniformity in state public records laws).

225. Schwartz, *supra* note 152, at 604.

226. *Id.*

where information so fluidly passes throughout the country and is being made more widely available by the Internet and through private companies. The privacy protection that currently exists for public records is largely designed for a world of paper records and has been slow to adapt to an age where information can be downloaded from the Internet in an instant.

II. ACCESS AND AGGREGATION: RETHINKING PRIVACY AND PUBLIC RECORDS

A. THE TENSION BETWEEN TRANSPARENCY AND PRIVACY

A 1998 episode of a television newsmagazine illustrates one way that the tension between transparency and privacy can arise.[227] A man, imprisoned for murder, obtained under a state FOIA the address of a former girlfriend.[228] When she learned that her ex-boyfriend obtained her address, the woman became quite scared because her ex-boyfriend was prone to losing his temper and held a grudge against her.[229] She lived in fear, knowing that someday he would be released and might come after her.[230] The prisoner, however, claimed that he was the father of her child and needed the address because he wanted to file a paternity suit.[231] This story illustrates why it is important for people to be able to obtain certain information about others, yet also demonstrates the dangers and threat to privacy caused by the ready availability of information.

There are at least four general functions of transparency: (1) to shed sunshine on governmental activities and proceedings; (2) to find out information about public officials and candidates for public office; (3) to facilitate certain social transactions, such as selling property or initiating lawsuits; and (4) to find out information about other individuals for a variety of purposes. I will discuss each in turn.

First, and perhaps most importantly, transparency provides the public with knowledge about the government and an understanding of how it functions.[232] By promoting awareness of the workings of government, transparency serves a "watchdog" function. Open access to government

227. *Dateline* (NBC television broadcast, Oct. 30, 1998).
228. *Id.*
229. *Id.*
230. *Id.*
231. *Id.*
232. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 572 (1980) (discussing the benefits to the public of conducting open criminal trials).

proceedings ensures that they are conducted fairly.[233] Public access exposes the government to public scrutiny and enables a check on abuse and corruption.[234] "Sunlight is said to be the best of disinfectants," declared Justice Brandeis, "electric light the most efficient policeman."[235] As courts have observed, making arrest records public provides "valuable protection against secret arrests and improper police tactics,"[236] and preserves "the integrity of the law enforcement and judicial processes"[237] by ensuring that the public can prevent abuse of the government's power to arrest individuals.[238] Open access to public court records "allows the citizenry to monitor the functioning of our courts, thereby insuring quality, honesty, and respect for our legal system."[239] As James Madison observed, "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."[240] According to Justice Oliver Wendell Holmes:

> It is desirable that the trial of [civil] causes should take place under the public eye not because the controversies of one citizen with another are of public concern, but because it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed.[241]

Access to court records permits people to examine the information considered by courts making decisions affecting the public at large. Issues raised in a product liability case could have significance for millions of others who use a product. Information about how certain types of cases are resolved—such as domestic abuse cases, medical malpractice cases, and others—is important for assessing the competency of the judicial system for resolving important social matters. Scholars and the me-

233. *Id.* at 569.

234. *Id.*

235. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY 92 (1932).

236. Wainwright v. City of New Orleans, 392 U.S. 598, 606 (1968) (per curiam) (Warren, C.J., dissenting) (quotations omitted); *see also* Davis v. North Carolina, 310 F.2d 904, 910 (4th Cir. 1962) (en banc) (Haynsworth, J., dissenting) (recycling on the police record to examine police tactics); Engrav v. Cragun, 769 P.2d 1224, 1228 (Mont. 1989); Houston Chronicle Publ'g Co. v. City of Houston, 531 S.W.2d 177, 186 (Tex. App. 1975) (discussing the legitimate interests for disclosure of police records).

237. United States v. Hickey, 767 F.2d 705, 708 (10th Cir. 1985).

238. United States v. Ross, 259 F. Supp. 388, 390 (D.D.C. 1966).

239. *In re* Cont'l Ill. Sec. Litig., 732 F.2d 1302, 1308 (7th Cir. 1984).

240. Letter from James Madison to W.T. Barry (Aug. 4, 1822), *in* 9 THE WRITINGS OF JAMES MADISON 103 (Gaillard Hunt ed., 1910).

241. Cowley v. Pulsifer, 137 Mass. 392, 394 (1884).

dia need to look beyond a judicial decision or a jury verdict to scrutinize records and evidence in a case. The ability to identify jurors enables the media to question them about the reasons for their verdict. Courts and commentators have pointed out that the Watergate Scandal might never have been uncovered if the original bail hearing had been closed to the press because reporters Bob Woodward and Carl Bernstein would not have been suspicious that expensive attorneys were representing the burglars.[242]

The second function of transparency is to enable the scrutiny of public officials or candidates for public office. Information about a politician's criminal history might be informative to many voters. Information about a politician's property may provide insight into the politician's wealth, a factor that might shape the politician's values and public decisions. Some voters may find a politician's divorce records and marital history illustrative of a politician's character. Other possibly informative information about a politician could include that she was sued many times or sued others many times; that she once declared bankruptcy; that she never voted in any elections; that she was formerly registered in another political party; that she owns property in other states; and so on. Open access to public records enables voters to find out such information to make more informed choices at the polls.

Third, transparency facilitates certain social transactions. Access to public records is an essential function for the sale and transfer of property, as it enables people to trace ownership and title in land. Public record information is useful in locating witnesses for judicial proceedings as well as locating heirs to estates. Further, access to public records can allow individuals and entities to track down individuals they want to sue and to obtain the necessary information to serve them with process.

The fourth function of transparency is to enable people to find out information about individuals for various other purposes. Public records can help verify individual identity, investigate fraud, and locate lost friends and classmates. Public records enable law enforcement officials to locate criminals and investigate crimes, and can assist in tracking down deadbeat parents.[243] Public records can permit people to investigate babysitters or child care professionals. Employers can use public record information to screen potential employees, such as examining the past driving records of prospective truck drivers or taxicab drivers. Criminal history information might be relevant when hiring a worker in a

242. United States v. Chagra, 701 F.2d 354, 363 n.25 (5th Cir. 1983); G. Michael Fenner & James L. Koley, *Access to Judicial Proceedings: To* Richmond Newspapers *and Beyond*, 16 HARV. C.R.-C.L. L. REV. 415, 436 n.109 (1981).

243. *See* Chandrasekaran, *supra* note 216.

child care facility or when hiring a kindergarten teacher.[244]

Transparency, however, can come into tension with privacy. Can both of these important values be reconciled? Before turning to this question, I must first address how the privacy problem that public records contribute to should be understood. Commentators have long struggled over defining what privacy is and why it is important, especially in the context of information collection and use.[245] We must rethink certain longstanding notions about privacy before we can reach an appropriate balance between transparency and privacy.

B. CONCEPTUALIZING PRIVACY AND PUBLIC RECORDS

1. Access: The Public is Private

One of the longstanding conceptions of privacy is that it involves secrecy and is lost once information is disclosed. I call this the "secrecy paradigm." According to this paradigm, an invasion of privacy consists of concealed information being unveiled or released in some way to others. Another central form of invasion is being watched or listened to both surreptitiously or in the open. The harms caused by these invasions of privacy are self-censorship and reputational damage.[246]

This paradigm is so embedded in our privacy discourse that privacy is often represented visually by a roving eye, an open keyhole, or a person peeking through Venetian blinds. Further, this paradigm explains why the Big Brother metaphor has become so widely used for depicting privacy problems.[247] Much of privacy law has developed around this paradigm. For example, in Fourth Amendment jurisprudence, the Supreme Court has routinely held that there is no expectation of privacy whenever it is possible that something can be seen or heard from a public vantage point, even if that perception is through a sensory enhancement device.[248] Accordingly, the Court has held that there is no expectation of

244. I am not contending that all of these purposes are desirable uses of public record data, especially since many of them constitute significant invasions of an individual's privacy. However, many people view these purposes as highly beneficial.

245. *See, e.g.*, JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992) ("Exploring the concept of privacy resembles exploring an unknown swamp."); MILLER, *supra* note 52, at 25; Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schoeman ed., 1984) (stating that "nobody has a clear idea" of what the right to privacy means); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 422 (1980) (stating that commentators have urged looking past the rhetoric to truly understand privacy law).

246. Solove, *supra* note 7, at 1394-99.

247. *Id.* at 1396.

248. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth

privacy when the government uses a sophisticated aerial camera to photograph objects that cannot be seen by the naked eye,[249] or when third parties have access to information.[250]

Along with this paradigm, privacy is often understood as an exclusive status or domain. Information is categorized as either public or private. When information is private, it is hidden, and as long as it is kept secret, it remains private. On the other hand, when information is public, it is in the public domain available for any use, and a person can no longer claim that the information is private. Understood this way, information has a particular status; it can either be in one domain or another. The law often treats information in this black-and-white manner; either it is wholly private or wholly public.

In the Information Age, this paradigm is outmoded, and it could lead to the practical extinction of privacy. Unless we live as hermits, there is no way to exist in modern society without leaving information traces wherever we go. Life today is fueled by information, and it is virtually impossible to live as an Information Age ghost, leaving no trail or residue. Does this mean that privacy is no longer possible? The answer to this question is yes only if we adhere to the dichotomous conception of privacy as a status, with information being in either a secret private realm or an open public realm.

In order to protect privacy in the Information Age, we must abandon the secrecy paradigm. Privacy involves an expectation of a certain degree of accessibility of information. Under this alternative view, privacy entails control over and limitations on certain uses of information, even if the information is not concealed. Privacy can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible. Our expectation of limits on the degree of accessibility emerges from the fact that information in public records has remained relatively inaccessible for much of our history. When people lived in small towns and everybody knew each other's business, there was no large-scale system of record-keeping in place. Today, people have a lot more anonym-

Amendment protection.").

249. Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986). This term, in *Kyllo v. United States*, 533 U.S. 27 (2001), the Supreme Court held that there are certain limits to how much technological enhancement of normal perception is permissible when it concluded that thermal sensors violated the Fourth Amendment.

250. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40 (1988) (holding there is no reasonable expectation of privacy in garbage because trash collectors had access to it); Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding that no reasonable expectation of privacy in pen register of phone numbers dialed from a person's home telephone existed because the phone company could record this information); United States v. Miller, 425 U.S. 435, 442-43 (1976) (holding there is no reasonable expectation in financial records because banks had access to them).

ity in the sense that they often conduct many day-to-day activities among strangers. The majority of Americans live in larger communities and frequently move to different places throughout their lifetimes.[251] According to Janna Malamud Smith,

> Control over private behavior, previously in the hands of the family, the community or neighborhood, and the church, is now redistributed, with more power granted on the one hand to individuals, and on the other, at a greater distance, to the bureaucracies and institutions that attempt to keep track of vast numbers of mobile people . . . .[252]

We know that our lives will remain private not in the sense that the information will be completely shielded from public access, but in the sense that for the most part, it will be lost in a sea of information about millions of people. Our personal information remains private because it is a needle in a haystack, and usually nobody will take the time to try to find it. This anonymity is rapidly disappearing as access to information is increasing.

In limited contexts, some courts are beginning to abandon the secrecy paradigm, although most of privacy law still clings to it. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[253] the Court held that the release of FBI "rap sheets" was an invasion of privacy within the privacy exemption of FOIA. The FBI rap sheets contained the date of birth, physical description, and a history of arrests, charges, and convictions on over twenty-four million people.[254] FOIA exempts law enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[255] The reporters claimed that the events summarized in the rap sheet were not private because they had previously been publicly disclosed.[256] The Court rejected this argument:

> In an organized society, there are few facts that are not at one time or another divulged to another. Thus, the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. . . . Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole . . . .[257]

As the Court further remarked, "there is a vast difference between the public records that might be found after a diligent search of courthouse

251. About 75% of people live in cities or in suburbs to urban areas. JANNA MALAMUD SMITH, PRIVATE MATTERS: IN DEFENSE OF THE PERSONAL LIFE 65 (1997).

252. *Id.*

253. 489 U.S. 749 (1989).

254. *Id.* at 751-52.

255. 5 U.S.C. § 552(b)(7)(C) (2000).

256. *Reporters Comm.*, 489 U.S. at 762-63.

257. *Id*. at 763-64 (citations omitted).

files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[258]

In cases involving the privacy torts,[259] a few courts have recognized a privacy interest in information exposed to the public. For example, in *Nader v. General Motors Corp.*,[260] Ralph Nader, a prominent public figure and outspoken critic of consumer safety, criticized the safety of General Motors' automobiles for many years.[261] General Motors, attempting to discredit Nader's reputation, interviewed his friends and acquaintances to learn the private details of his life, kept him under surveillance, tapped his telephone and eavesdropped into his conversations, and hired prostitutes to entrap him into an illicit relationship.[262] Of particular relevance, General Motors hired a person to "shadow" Nader in public—to follow him around and watch him engage in day-to-day activities.[263] The court held that generally observation in public did not constitute an action for the tort of intrusion upon seclusion.[264] This tort protects against the intentional intrusion into one's "solicitude or seclusion" or "his private affairs or concerns" that "would be highly offensive to a reasonable person."[265] Because the tort requires an invasion of "seclusion," courts have typically rejected intrusion suits when plaintiffs have been in public places.[266] Nevertheless, in *Nader*, the court concluded that "overzealous" watching such as "shadowing" could rise to a level as to constitute a violation of privacy (even though all the activities watched occurred in public).[267]

Likewise, in cases involving the tort of public disclosure of private facts, a few courts have held that information once public can be private under certain circumstances. The tort of public disclosure permits a person to sue when one makes public "a matter concerning the private life of another" in a way that "(a) would be highly offensive to a reasonable per-

258. *Id.* at 764.

259. The privacy torts are often referred to collectively as "invasion of privacy" and consist of (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or "publicity"; and (4) appropriation. RESTATEMENT (SECOND) OF TORTS § 652A (1977). The torts were inspired by the famous article by Samuel D. Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

260. 255 N.E.2d 765 (N.Y. Ct. App. 1970).

261. *Id.* at 767.

262. *Id.*

263. *Id.* at 771.

264. *Id.*

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

266. *See, e.g.*, Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 482-83 (D. Me. 1987) (holding that no intrusion occurred when photographers harassed and insulted the plaintiff in a public place).

267. *Nader*, 255 N.E.2d at 771.

son and (b) is not of legitimate concern to the public."[268] In *Daily Times Democrat v. Graham,*[269] a woman who went to a county fair had her dress inadvertently blown up by air jets on the platform she was standing on.[270] A local newspaper photographer snapped a photo of the woman at that moment, and it was published on the front page of the newspaper.[271] The woman sued for a violation of the public disclosure tort.[272] The newspaper argued that the picture was taken in public and therefore, she had no claim to privacy.[273] The court, however, held that merely because a person is involuntarily placed in an embarrassing pose in public does not eliminate privacy.[274]

In *Melvin v. Reid*,[275] which is frequently referred to as "The Red Kimono" case, a former prostitute who was once criminally prosecuted for murder had left the prostitution business long ago and led a normal life.[276] A motion picture company produced the film "The Red Kimono," depicting her life story and using her maiden name.[277] She sued under the tort of public disclosure.[278] The court held that, although she could not claim that the facts about her life were private because they were in the public record, there was no need for the movie to use her real name.[279]

Likewise, in *Briscoe v. Reader's Digest Ass'n*,[280] an article in Reader's Digest Magazine about hijacking disclosed that the plaintiff had hijacked a truck.[281] The crime occurred eleven years before the article; Briscoe had rehabilitated himself and his new friends, family, and young daughter were not aware of his previous life of crime.[282] The court held that although the article was newsworthy and the facts of Briscoe's crime could be disclosed, Briscoe could sue for the use of his name, which had no relevance to the article at all.[283]

Generally, however, most courts still adhere to the secrecy paradigm

268. RESTATEMENT (SECOND) OF TORTS § 652D (1977).
269. 162 So. 2d 474 (Ala. 1964).
270. *Id.* at 476.
271. *Id.*
272. *Id.* at 475.
273. *Id.* at 477-78.
274. *Id.* at 478.
275. 297 P. 91 (Cal. Dist. Ct. App. 1931).
276. *Id.* at 91.
277. *Id.*
278. *Id.*
279. *Id.* at 93.
280. 483 P.2d 34 (Cal. 1971).
281. *Id.* at 36.
282. *Id.*
283. *Id.* at 39-40.

and do not recognize a privacy interest when information is exposed to the public. As a result, most courts have rejected the *Reid* and *Briscoe* approach.[284] In *Forsher v. Bugliosi*,[285] the court noted that "California courts have refrained from extending the *Briscoe* rule to other fact situations."[286] The court considered *Briscoe* "an exception to the more general rule that 'once a man has become a public figure, or news, he remains a matter of legitimate recall to the public mind to the end of his days.'"[287] The *Forsher* decision was in line with the Restatement for the tort of public disclosure: "There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public. Thus there is no liability for giving publicity to facts about the plaintiff's life which are matters of public record."[288] Likewise for the tort of intrusion upon seclusion, the Restatement provides that "there is no liability for the examination of a public record concerning the plaintiff."[289] Further, *Briscoe* seems foreclosed by the Supreme Court's decision in *Cox Broadcasting Corp. v. Cohn*,[290] which held that when information is disclosed in documents open to the public, the press cannot be punished for publishing it.[291]

In a number of cases, courts applying the constitutional right to information privacy have become mired in the secrecy paradigm. Courts have refused to find a constitutional right to information privacy for data that has previously been disclosed or exist in a public record. In *Scheetz v. Morning Call, Inc.*,[292] a court held that a husband and wife had no constitutional right to information privacy in a police report disclosed to the press containing the wife's allegations of spousal abuse.[293] Although her complaint to the police did not result in charges, "[t]he police could have brought charges without her concurrence, at which point all the information would have wound up on the public record, where it would have been non-confidential."[294] In *Cline v. Rogers,*[295] the court held that the

284. Westphal v. Lakeland Register, 2 Media L. Rep. (BNA) 2262, 2263 (Fla. Cir. Ct. 1977); Roshto v. Hebert, 439 So. 2d 428, 431 (La. 1983); Montesano v. Donrey Media Group, 668 P.2d 1081, 1088 (Nev. 1983); Jenkins v. Bolla, 600 A.2d 1293, 1296-97 (Pa. Super. Ct. 1992).

285. 608 P.2d 716 (Cal. 1980).

286. *Id.* at 726.

287. *Id.* (quoting William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 418 (1960)).

288. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

289. *Id.* § 652B cmt. c.

290. 420 U.S. 469 (1975).

291. *Id.* at 495.

292. 946 F.2d 202 (3d Cir. 1991).

293. *Id.* at 207.

294. *Id.*

295. 87 F.3d 176 (6th Cir. 1996).

constitutional right to information privacy did not apply to the disclosure of police records because "one's criminal history is arguably not a private 'personal matter' at all, since arrest and conviction information are matters of public record."[296] In *Walls v. City of Petersburg*,[297] the court upheld against a constitutional right to information privacy challenge a questionnaire asking public employees the criminal histories of their family members, their complete marital history, including marriages, divorces, and children, and any outstanding debts or judgments against them.[298] The court reasoned that there was no privacy interest in this information because the data was already available in public records.[299]

Courts have also adhered to the secrecy paradigm in challenges to Megan's Laws, which mandate the disclosure of personal information about convicted sex offenders after they have completed their prison sentences. In *Russell v. Gregoire*,[300] convicted sex offenders challenged Washington's sex offender law, which provided for disclosure of their picture, name, age, date of birth, crimes, and vicinity of residence to government agencies, schools, and even to the media in certain instances.[301] The plaintiffs contended that Megan's Law was unconstitutional under the constitutional right to information privacy, but the court held that the information was not private because it was "already fully available to the public."[302]

In *Paul P. v. Verniero*,[303] plaintiffs challenged New Jersey's Megan's Law.[304] Disclosure would be to law enforcement officials, schools, and community organizations for certain offenders and disclosure to all members of the public for the most severe offenders.[305] The plaintiffs argued that the statutorily required disclosure of their names, physical descriptions, and home addresses violated the constitutional right to information

296. *Id*. at 179; *see also* Doe v. City of New York, 15 F.3d 264, 268 (2d Cir. 1994) ("[A]n individual cannot expect to have a constitutionally protected privacy interest in matters of public record.").

297. 895 F.2d 188 (4th Cir. 1990).

298. *Id.* at 190-95. Additionally, the questionnaire asked whether they had sexual relations with a person of the same sex. The court's conclusion that no privacy interest existed for this information was based on a different rationale than the other questions. The court concluded that under the "controlling" Supreme Court decision in *Bowers v. Hardwick*, 478 U.S. 186 (1986), there was no right to keep one's sexual orientation private. *Walls*, 895 F.2d at 193. It is unclear how *Bowers* controls on this proposition.

299. *Walls*, 895 F.2d at 193-94.

300. 124 F.3d 1079 (9th Cir. 1997).

301. *Id.* at 1082.

302. *Id*. at 1094.

303. 170 F.3d 396 (3d Cir. 1999).

304. *Id.* at 398.

305. *Id.* at 399.

privacy.[306] The court explicitly rejected the logic of *Reporter's Committee*, but recognized that the plaintiffs were entitled to privacy protection with regard to their address information.[307]

In sum, courts are deeply divided about whether to adhere to the secrecy paradigm. The Supreme Court clings to this paradigm in its Fourth Amendment jurisprudence but has abandoned it in its FOIA cases.[308] Courts applying privacy torts have occasionally departed from the paradigm, but generally follow it.[309] Unless the secrecy paradigm is abandoned, people will lose any ability to claim a privacy interest in the extensive personal information in public records.

2. Aggregation: The Digital Biography

Another longstanding notion of privacy is that it protects against disclosure of particularly sensitive or intimate information. According to this view, information that we should protect as private must be embarrassing or harmful to one's reputation. However, the information in public records often consists of fairly innocuous details—such as one's birth date, address, height, weight, and so on. Eugene Volokh epitomizes this view when he writes,

> [M]any of the proposals to restrict communication of consumer transactional data would apply far beyond a narrow core of highly private information, and would cover all transactional information, such as the car, house, food, or clothes one buys. I don't deny that many people may find such speech vaguely ominous and would rather that it not take place, and I acknowledge that some people get extremely upset about it. . . . If such relatively modest offense or annoyance is enough to justify speech restrictions, then the compelling interest bar has fallen quite low . . . .[310]

A number of courts have rejected claims that certain information falls within state FOIA privacy exceptions because the information does not pose immediate harm to one's reputation or security. One court reasoned that "[n]ames and addresses are not ordinarily personal, intimate, or embarrassing pieces of information."[311] Another court held that pay-

306. *Id.* at 398.

307. *Id.* at 400-01, 405. *But see* Doe v. Portiz, 662 A.2d 367, 411 (N.J. 1995) (following the conception from *Reporters Committee* when examining the constitutionality of Megan's Law and noting that "a privacy interest is implicated when the government assembles . . . diverse pieces of information into a single package and disseminates that package to the public, thereby ensuring that a person cannot assume anonymity").

308. *See supra* notes 248-50, 253-58 and accompanying text.

309. *See supra* notes 260-308 and accompanying text.

310. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1117 (2000).

311. State Employees Ass'n v. Dep't of Mgmt. & Budget, 404 N.W.2d 606, 615 (Mich. 1987) (quoting Tobin v. Mich. Civil Serv. Comm'n, 331 N.W.2d 184, 189 (Mich.

roll records of the Philadelphia Police Department that contained each employee's name, payroll number, gender, date of birth, annual salary, and other personal data were subject to disclosure because the records did not harm the officer's reputation.[312] Information about teacher salaries, according to one court, did not fall within the sunshine law privacy exception because "[t]he salaries of public employees and schoolteachers are not 'intimate details . . . the disclosure of which might harm the individual.'"[313]

If the release of certain information in public records does not make one blush or reveal one's deepest secrets, then what is the harm? I contend that the nature of the harm stems from what I call the "aggregation problem." Viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities. The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined. Even information in public records that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information. For example, although one's Social Security number does not in and of itself reveal much about an individual, it provides access to one's financial information, educational records, medical records, and a whole host of other information.

In a parable, *The Circular Ruins*, Jorge Luis Borges describes a person who aspires to dream a man in "painstaking detail" so as to create an imaginary being so real that he can move from the world of dreams into the world of reality.[314] The person begins by imagining the man's heart and then adds details each night:

> He dreamed the heart warm, active, secret—about the size of a closed fist, a garret-colored thing inside the dimness of a human body that was still faceless and sexless . . . . Each night he perceived it with greater clarity, greater certainty. . . . On the fourteenth night, he stroked the pulmonary artery with his forefinger, and then the entire heart, inside and out. . . . Before the year was out he had reached the skeleton, the eyelids.[315]

Eventually, the person completes his goal and has assembled enough details to create a dreamed being so realistic that the being be-

1982)).

312. Moak v. Phila. Newspapers, Inc., 336 A.2d 920, 924 (Pa. Commw. Ct. 1975).

313. Mans v. Lebanon Sch. Bd., 290 A.2d 866, 868 (N.H. 1972) (quoting H.R. REP. NO. 1497, at 11 (1966)) (discussing federal FOIA); *see also* Pottle v. Sch. Comm. of Braintree, 482 N.E.2d 813, 816-17 (Mass. 1985) (holding that payroll records containing names, salaries, overtime pay, and addresses of policemen and school employees were not private within the meaning of Massachusetts's FOIA privacy exception because the information was not intimate).

314. JORGE LUIS BORGES, *The Circular Ruins*, *in* COLLECTED FICTIONS 96, 97 (Andrew Hurley trans., 1998).

315. *Id*. at 98.

comes real.[316] At the end of the parable, the dreamer realizes that he is but the dreamed person of another.[317]

Borges's parable illustrates the power of aggregating details. In the Information Age, personal data is being combined to create a "digital biography" about us. Information that appears innocuous can sometimes be the missing link, the critical detail in one's digital biography, or the key necessary to unlock other stores of personal information. There are several aspects of this digital biography that raise alarm.

To the extent that the digital biography is accurate, our lives are not only revealed and recorded, but also can be analyzed and investigated. Our digital biographies are being assembled by companies like ChoicePoint, which are amassing personal information in public records along with other information.[318] Collectively, millions of biographies can be searched, sorted, and analyzed in a matter of seconds. This enables automated investigations of individuals on a nationwide scale by both the government and the private sector. Increasingly, private sector entities are conducting investigations which can have profound consequences on people's lives–such as their employment and financial condition. Employers are resorting to information brokers of public record information to assist in screening job applicants and existing employees. For example, the firm HireCheck serves over 4000 employers to conduct background checks for new hires or current employees.[319] It conducts a national search of outstanding warrants, a Social Security number search to locate age, past and current employers, and former addresses, a driver record search, a search of worker's compensation claims "to avoid habitual claimants or to properly channel assignments," a check of civil lawsuit records, as well as searches for many other types of information.[320] These investigations occur without any external oversight, and individuals often do not have an opportunity to challenge the results.[321]

Although the digital biography contains a host of details about a person, it captures a distorted persona, one who is constructed by a variety of external details. The digital biography falls short of the perfection achieved by the dreamer in Borges's parable. The problem, as Arthur Miller observed decades ago, is that an "individual who is asked to provide a simple item of information for what he believes to be a single pur-

316. *Id.* at 99.

317. *Id.* at 100.

318. *See supra* text accompanying notes 63-68.

319. Hire Check, *Welcome to Hirecheck*, *at* http://www.hirecheck.com/ flashintro/index.html (last viewed July 1, 2002).

320. Hire Check, *Background Screening*, *at* http://www.hirecheck.com/ ProductsAndServices/background Screening.html (last viewed July 1, 2002).

321. *Id.*

pose may omit explanatory details that become crucial when his file is surveyed for unrelated purposes."[322] Further, although the data in public records combined with the information marketers glean about us can be quite revealing, it still cannot penetrate into our thoughts and often only partially captures who we are. W.H. Auden's 1940 poem, *The Unknown Citizen*, depicts the situation with eerie foresight:

> He was found by the Bureau of Statistics to be
> One against whom there was no official complaint,
> And all the reports on his conduct agree
> That, in the modern sense of an old-fashioned word, he was a saint,
> For in everything he did he served the Greater Community.
> Except for the War until the day he retired
> He worked in a factory and never got fired,
> But satisfied his employers, Fudge Motors, Inc.
> Yet he wasn't a scab or odd in his views,
> For his Union reports that he paid his dues,
> (Our report on his Union shows it was sound)
> And our Social Psychology workers found
> That he was popular with his mates and liked a drink.
> The Press are convinced that he bought a paper every day
> And that his reactions to advertisements were normal in every way.
> Policies taken out in his name prove that he was fully insured,
> And his Health-card shows he was once in hospital but left it cured.
> Both Producers Research and High-Grade Living declare
> He was fully sensible to the advantages of the Instalment Plan
> And had everything necessary to the Modern Man,
> A phonograph, a radio, a car and a frigidaire.
> Our researchers into Public Opinion are content
> That he held the proper opinions for the time of year;
> When there was peace, he was for peace; when there was war,
> he went.
> He was married and added five children to the population,
> Which our Eugenicist says was the right number for a parent of
> his generation,
> And our teachers report that he never interfered with their education.
> Was he free? Was he happy? The question is absurd:
> Had anything been wrong, we should certainly have heard.[323]

322. MILLER, *supra* note 52, at 34.

323. W.H. AUDEN, *The Unknown Citizen*, *in* COLLECTED POEMS 201 (Edward Mendelson ed., 1976). Used by permission of Random House, Inc. Copyright 1940 and re-

This poem aptly captures how day-to-day information both reveals and distorts. Auden illustrates how our lives are captured to a significant degree by the information we leave behind. Yet the information about our property, our professions, our purchases, our finances, and our medical history does not tell the whole story. We are more than the bits of data we give off as we go about our lives. Our digital biography is revealing of ourselves but in a rather standardized way. It consists of bits of information pre-defined based on the judgment of the government or some entity about what categories of information are relevant or important. We are partially captured by details such as our age, race, gender, net worth, property owned, and so on, but only in a manner that standardizes us into types or categories. Indeed, database marketers frequently classify consumers into certain categories based on stereotypes about their values, their lifestyle, and their purchasing habits.[324] Our digital biography is thus an unauthorized biography, only partially true and very reductive. We must all live with such unauthorized biographies about us, the complete contents of which we often do not get to see. Although certainly a more extensive dossier might be less reductive in capturing our personalities, it would have greater controlling effects on an individual's life.

Our digital biographies are not only reductive but are often inaccurate. In today's bureaucratized world, one of the growing threats is that we will be subject to the inadvertence, carelessness, and mindlessness of bureaucracy. A scene from the movie *Brazil* illustrates this problem by way of dark humor.[325] The movie opens with an exhausted bureaucrat swatting a fly, which inconspicuously drops into a typewriter, causing a jam, and resulting in a mistyped letter in a person's last name on a form.[326] The paper is a form authorizing the arrest and interrogation of suspected rebels. In the next scene, the innocent man whose name was wrongly typed on the form peacefully sits with his family when suddenly scores of armor-clad police storm into his tiny apartment and haul him away.[327]

These dangers are not merely the imaginary stuff of movies. The burgeoning use of databases of public record information by the private sector in screening job applicants and investigating existing employees demonstrates how errors can potentially destroy a person's career. Even before the ready accessibility of public records, significant problems

newed 1968 by W.H. Auden.

324. *See* Solove, *supra* note 7, at 1424.

325. BRAZIL (Universal Pictures 1985).

326. *Id.*

327. *Id.*

emerged from the use of such information. For example, in *Paul v. Davis*,[328] the police distributed flyers with names and photographs to various stores erroneously listing the plaintiff as an active shoplifter.[329] The plaintiff almost lost his job and was afraid to enter stores.[330] In a more recent example involving computerized information, a Maryland woman wrongly arrested for a burglary was not cleared from the state's criminal databases.[331] Her name and Social Security number also migrated to a Baltimore County database relating to child protective services cases.[332] She was fired from her job as a substitute teacher, and only after she could establish that the information was in error was she rehired.[333] When she later left that job to run a day care center for the United States' military, she was subject to questioning about the erroneous arrest.[334] Later on, when employed at as a child care director at a YMCA, she was terminated when her arrest record surfaced in a background clearance check; she could not have the error expunged in sufficient time, so the job was given to another person.[335] Only after several years was the error cleared from the public records.[336] In another example, as described earlier, the errors in the data supplied by ChoicePoint to the Florida elections officials possibly resulted in the loss of many people's right to vote.[337] To the extent that our digital biographies are increasingly relied upon to make important decisions, the problems that errors can cause will only escalate in frequency and magnitude.

Beyond these difficulties, our digital biographies greatly increase our vulnerability to a variety of dangers. For example, a website called the "Nuremberg Files" posted information about doctors working in abortion clinics, including names, photos, Social Security numbers, home addresses, descriptions of their cars, and information about their families.[338] The website drew a black line through the names of murdered doctors and shaded wounded doctors' names in gray.[339] Fearing for their lives and the lives of their families, the doctors sued to shut the website down, but the Ninth Circuit held that the website had a First Amendment

328. 424 U.S. 693 (1976).
329. *Id.* at 695.
330. *Id.* at 696-97.
331. Eugene L. Meyer, *Md. Woman Caught in Wrong Net; Data Errors Link Her To Probes, Cost 3 Jobs*, WASH. POST, Dec. 15, 1997, at C1.
332. *Id*.
333. *Id.*
334. *Id*.
335. *Id*.
336. *Id*.
337. *See supra* note 76 and accompanying text.
338. *See* CHARLES J. SYKES, THE END OF PRIVACY 42-43 (1999).
339. *Id.* at 43-44.

right to publish the information.[340] The Nuremberg Files case illustrates the dangers created from the increased access to public record information.

As public record information becomes more readily available, criminals can use it to gain access to a person's financial accounts. For example, one industrious criminal gained access to the financial accounts of a number of individuals on *Forbes* Magazine's list of the 400 richest people in America such as Oprah Winfrey and George Lucas.[341] One of the most rapidly escalating forms of crime is identity theft.[342] Identity theft occurs when an individual's personal information is stolen to open new bank accounts, acquire credit cards, obtain loans, and so on. In fact, the FBI stated that identity theft is the fastest-growing form of white-collar criminal activity in the United States.[343] Identity thieves frequently obtain personal information necessary for their criminal activity through information brokers, who sell reports about individuals based on public record data combined with other information.[344] Identity theft creates severe hardship for victims, who must spend countless hours—estimated at about 175 hours over two years—to mend the damage to their credit.[345]

Public record information also proves useful for stalkers. In 1989, a fan obsessed with actress Rebecca Shaeffer located her home address with the help of a private investigator who obtained it from California

340. *See* Planned Parenthood v. Am. Coalition of Life Activists, 244 F.3d 1007, 1019-20 (9th Cir. 2001).

341. Jayson Blair & William K. Rashbaum, *Man Broke Into Accounts of Celebrities, Police Say*, N.Y. TIMES, Mar. 21, 2001, at B3.

342. Robert O'Harrow, Jr., *Identity Thieves Thrive in Information Age: Rise of Online Data Brokers Makes Criminal Impersonation Easier*, WASH. POST, May 31, 2001, at A1. According to estimates by the Federal Office of the Comptroller of the Currency, there are half a million victims of identity theft each year. *Id*. For a detailed discussion of identity theft, see Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem,* 80 TEX. L. REV. 89 (2001). According to LoPucki, the problem of identity theft is not caused by the widespread accessibility of personal information but by the private sector's use of Social Security numbers, addresses, and mothers' maiden names as passwords. *See id*. at 108-14. Accordingly, LoPucki proposes a system where people publicly register their identities and provide data for identification. *See id.* at 114-35. I agree with LoPucki that restrictions must be placed on the way that the private sector maintains the security of personal information. *See* Solove, *supra* note 7, at 1460. However, as described herein, there are other problems associated with the widespread disclosure of personal information. Even if LoPucki's solution combats the identity theft problem, it can contribute to these other problems.

343. Jennifer S. Lee, *Fighting Back When Someone Steals Your Name*, N.Y. TIMES, Apr. 8, 2001, § 3, at 8.

344. O'Harrow, *supra* note 342.

345. *See* Lee, *supra* note 343.

motor vehicles records.[346] The fan murdered her outside her home.[347] This killing spurred Congress to pass the DPPA, which restricts the states' ability to release motor vehicle records.[348] Ironically, however, the Act provided an exception permitting the disclosure of personal information to private investigators without an individual's consent.[349]

At a more abstract level, the existence of digital biographies alters the nature of the society we live in. In 1971, in his highly influential work on privacy, Arthur Miller warned of the "possibility of constructing a sophisticated data center capable of generating a comprehensive womb-to-tomb dossier on every individual and transmitting it to a wide range of data users over a national network."[350] On a number of occasions, the federal government has flirted with the idea of creating a national database of personal information. The Johnson Administration contemplated creating a National Data Center that would combine information collected by various federal agencies into one large computer database, but the plan was scrapped after a public outcry.[351] Again, in the early 1970s, an official in the General Services Administration proposed that all of the federal government's computer systems be connected in a network called FEDNET.[352] Responding to a public outcry, Vice President Gerald Ford stopped the plan.[353]

Although these proposals have been halted due to public outcries, we have been inching toward a system of de facto national identification for some time and are precariously close to having one.[354] The Immigration Reform and Control Act of 1986 requires new employees to supply identification and proof of United States citizenship before obtaining a new job.[355] In a recent effort to track down parents who fail to pay child support, the federal government has created a vast database consisting of

346. Lessley Anderson, *Watching the I-Detectives*, INDUS. STANDARD, Nov. 30, 1998, *available at* http://www.thestandard.com/article/0,1902,2581, 00.html.

347. *See id.*

348. *See* REGAN, *supra* note 170, at 102.

349. 18 U.S.C. § 2721(b)(8) (2000).

350. MILLER, *supra* note 52, at 39.

351. *See, e.g.,* SYKES, *supra* note 338, at 44. In 1965, the Ruggles Committee issued a report urging that decentralized data among federal agencies be consolidated. *See* SMITH, *supra* note 4, at 309 Due to a large public outcry, the proposal was abandoned. *See id*. at 310-11; *see also* Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 404 (1968).

352. SMITH, *supra* note 4, at 311.

353. *Id.*

354. *See* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 39 (2002). *See generally* AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

355. Immigration Reform and Control Act of 1986, Pub. L. No. 99-603 100 Stat. 3359 (1986) (codified as amended at 8 U.S.C. §§ 1324a-1365 (2000)).

information about all people who obtain a new job anywhere in the nation. The database contains their Social Security numbers, addresses, and wages.[356] The ready availability of one's Social Security number and the ability to combine it with a host of other information about individuals will make increasingly more possible a reality where typing an individual's name into a searchable database will pull up a "womb-to-tomb" dossier.

Such a reality can pose significant dangers. "Identity systems and documents," observes Richard Sobel, "have a long history of uses and abuses for social control and discrimination."[357] Slaves were required to carry identifying papers to travel; identification cards were used by the Nazis in locating Jews; and the slaughter of Tutsis in Rwanda was aided by a system of identifiers.[358] In addition to facilitating the monitoring and control of individuals, such a dossier may make a person a "prisoner of his recorded past."[359] Records of personal information can easily be used by government leaders and officials for improper monitoring of individuals. Indeed, such data can be used for whatever task is at hand—a tool available to anyone in power in government for use to further the current passion or whim of the day. In 1942, the Census Bureau used its data from the 1940 census to assist in the effort to intern Japanese-Americans during World War II.[360] Currently, we do not know the full consequences of living in a dossier society, but we are rapidly moving toward becoming such a society without sufficient foresight and preparation.

The problems and dangers illustrated above are not merely the product of the actions of the government. Rather, these troubles are caused by the way that both public and private sector entities are using personal information. The issue concerns more than isolated threats and harms, but is fundamentally about the structure of our society. Not only are public records altering the power that the government can exercise over people's lives, but they are also contributing to the growing power of private sector entities. Elsewhere, I described the problem of private sector collection and use of personal information, and I argued that Franz Kafka's *The Trial* is an appropriate metaphor to conceptualize this prob-

356. *See* Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996) (codified as amended at scattered sections of 7, 8, 21, 25 & 42 U.S.C. (2000)). *See generally* Robert O' Harrow, Jr., *Uncle Sam Has All Your Numbers*, WASH. POST, June 27,1999 at A1.

357. Sobel, *supra* note 354, at 48.

358. *See id.* at 50-53.

359. HEW 1973 REPORT, *supra* note 172, at 112.

360. *See* LARSON, *supra* note 50, at 53-54.

lem.[361] In *The Trial*, a bureaucratic court system has assembled a dossier of information about the protagonist, Joseph K., and suddenly arrests him one morning. K. is never informed of the reason for his arrest, and he embarks on a frustrating quest to find out why he has been arrested and the nature of the proceedings against him. His information is in the hands of an entity that is obscure, unaccountable, and uncontrolled.

Like *The Trial*, the current collection and use of personal information are used to make decisions affecting an individual's life, yet individuals often have no way to participate and no notice about what is happening. Although people may be aware that dossiers are being assembled about them, they have no idea what information the dossiers contain or how the dossiers are being used. For example, the HEW Report in 1973 aptly observed

> There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays, an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.[362]

This reality creates a sense of unease, vulnerability, and powerlessness—a deepening sense that one is at the mercy of others, or, perhaps even more alarming, at the mercy of a bureaucratic process that is arbitrary, irresponsible, opaque, and indifferent to people's dignity and welfare.

The problem with information collection and use today is not merely that individuals are no longer able to exercise control over their information; it is that their information is subjected to a bureaucratic process that is itself out of control.[363] Without this process being subject to regulation and control and without individuals having rights to exercise some dominion over their information, individuals will be routinely subjected to the ills of bureaucracy.

Public records contribute to this privacy problem because they are often a principal source of information for the private sector in the construction of their databases. Marketers stock their databases with public record information, and the uses to which these databases are put are manifold and potentially limitless. The personal information in public records is often supplied involuntarily and typically for a purpose linked to the reason why particular records are kept. The problem is that, often

361. *See* Solove, *supra* note 7, at 1419.

362. HEW 1973 REPORT, *supra* note 172, at 29.

363. *See* Solove, *supra* note 7, at 1440.

without the individual's knowledge or consent, the information is then used for a host of different purposes by both the government and businesses.

Therefore, the privacy problem caused by public records concerns the structure of information flow—the way that information circulates throughout our society. The problem is not necessarily the disclosure of secrets or the injury of reputations, but is one created by increased access and aggregation of data. Privacy is an issue that concerns what type of society we want to construct for the future. Do we want to live in a Kafkaesque world where dossiers about individuals circulate in an elaborate underworld of public and private sector bureaucracies without the individual having notice, knowledge, or the ability to monitor or control the ways the information is used?

C. TRANSPARENCY AND PRIVACY: RECONCILING THE TENSION

How can the tension between transparency and privacy be reconciled? Must access to public records be sacrificed at the altar of privacy? Or must privacy evaporate in order for government to be disinfected by sunlight?

It is my thesis that both transparency and privacy can be balanced through limitations on the access and use of personal information in public records. Of course, we must rethink what information belongs in public records. But we must also regulate the uses of our digital biographies. Government is not doing enough to protect against the uses of the information that it routinely pumps into the public domain. If we abandon the notion that privacy is an exclusive status, and recognize that information in public records can still remain private even if there is limited access to it, then a workable compromise for the tension between transparency and privacy emerges. We can make information accessible for certain purposes only. When government discloses information, it can limit how it discloses that information by preventing it from being amassed by companies for commercial purposes, to be sold to others, or to be combined with other information and sold back to the government.

Much of the personal information in public records is not necessary to shed light on the way government carries out its functions. Rather, this information reveals more about the people who are the subjects of the government's regulatory machinery. In the FOIA context, the Court has recognized that FOIA should not be interpreted beyond its purpose—requiring disclosure for information that "would not shed any light on the conduct of any Government agency or official."[364] Nevertheless, al-

364. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773 (1989); *see also* Schwartz, *supra* note 152, at 594.

though the federal FOIA has served to shed light on government activities and has supplied critical information for hundreds of books and articles,[365] it has also been used as a tool for commercial interests. The vast majority of FOIA requests are made by businesses for commercial purposes.[366] According to Judge Patricia Wald, FOIA turns agencies into "information brokers" rather than "a window for public assessment of how government works."[367] When weighing interests under the privacy exceptions to the federal FOIA, although courts cannot consider the identity and purpose of the requester, they can take into account the relationship of the requested document to the purposes of FOIA.[368] Unlike the federal FOIA, many states routinely permit access by information brokers without looking to the purposes of their sunshine laws or the public interest.

State FOIAs generally do not permit any discrimination among requesters. In a number of cases, states wanting to restrict access to people requesting records for commercial use had no statutory authority to do so. In *Dunhill v. Director, District of Columbia Department of Transportation*,[369] a marketer of personal information about individuals sought a listing on computer tape of the names, addresses, birth dates, gender, and expiration date of drivers permits of all people holding valid District of Columbia drivers permits.[370] The court held that the government had to release the information because the statute did not authorize the government to look to the motives of the request.[371] In *In re Crawford*,[372] a preparer of bankruptcy petitions for debtors challenged the requirement that he divulge his Social Security number on the petition, which would then be made public. The court recognized that although the person had a privacy right in his Social Security number and that disclosure exposed him to dangers of fraud and identity theft, the interest in public access "is of special importance in the bankruptcy arena, as unrestricted access to

365. Cate et al., *supra* note 139, at 65.

366. *See id.* at 50-51 (citing studies by the General Accounting Office, Department of Health and Human Services, and the Department of Defense).

367. Patricia M. Wald, *The Freedom of Information Act: A Short Case Study in the Perils and Paybacks of Legislating Democratic Values*, 33 EMORY L.J. 649, 667 (1984).

368. *See, e.g.*, United States Dep't of State v. Ray, 502 U.S. 164, 178 (1991) ("The addition of the redacted identifying information would not shed any additional light on the Government's conduct of its obligation."); *Reporters Comm.*, 489 U.S. at 772 (1989); *see also* Halloran v. Veterans Admin., 874 F.2d 315, 323 (5th Cir. 1989) ("[I]f disclosure of the requested information does not serve the purpose of informing the citizenry about the activities of their government, disclosure will not be warranted even though the public may nonetheless prefer, albeit for other reasons, that the information be released.").

369. 416 A.2d 244 (D.C. 1980).

370. *Id*. at 246.

371. *Id*. at 247-48.

372. 194 F.3d 954 (9th Cir. 1999).

judicial records fosters confidence among creditors regarding the fairness of the bankruptcy system."[373] Thus, the court formalistically invoked the principle of transparency, relying on the vague argument that total transparency fosters "confidence."

The danger with any principle is that it can drift to different uses over time. J.M. Balkin explains this problem as "ideological drift." "Ideological drift in law means that legal ideas and symbols will change their political valence as they are used over and over again in new contexts."[374] Laws fostering transparency are justified as shedding light into the dark labyrinths of government bureaucracy to expose its inner workings to public scrutiny, and preventing the harrowing situation in Kafka's *The Trial*—a bureaucracy that worked in clandestine and mysterious ways, completely unaccountable and unchecked. These are certainly laudable goals, for they are essential to democracy and to the people's ability to keep government under control. However, sunshine laws are increasingly becoming a tool for powerful corporations to collect information about individuals to further their own commercial interests, not to shed light on the government. A window to look in on the government is transforming into a window for the government and allied private sector entities to peer in on individuals. The data collected about individuals is then subject to a bureaucratic process that is often careless, uncontrolled, and clandestine. Because private sector bureaucracies lack the transparency of those of government, there is a greater potential for personal information to be abused. Paradoxically, a right of access designed to empower individuals and protect them from the ills of bureaucracy can lead to exactly the opposite result.

There are certainly instances where information about individuals can provide illumination on the way that the government is functioning. The examination of accident reports may reveal useful information about widespread problems with particular vehicles. Scrutiny of police records may indicate problems in police investigation and enforcement. Information about the salaries of public school teachers and other public officials and employees may enable the public to assess whether such officials and employees are being over- or under-compensated. Disciplinary information about such employees can allow taxpayers to assess the performance of those who are earning their tax dollars. However, many of these purposes can be achieved through evaluating aggregate statistical data or by examining records with redacted personal identifying information.

The solution is not to eliminate all access to public records, but to

373. *Id*. at 960.

374. J.M. Balkin, *Ideological Drift and the Struggle Over Meaning*, 25 CONN. L. REV. 869, 871 (1993).

redact personal information where possible and to regulate specific uses of information. Real property information must be made available for certain purposes, but it should not be available for all purposes. It is necessary for a litigant to obtain the address of a celebrity the litigant desires to sue in order to serve process; however, to disclose the address to fans or to publish it on the Internet is different.

Use restriction laws, such as those discussed above in Part I.B, are a step in the right direction. These laws attempt to navigate the tension between transparency and privacy by permitting the use of public record information for certain purposes but not all purposes. One of the longstanding Fair Information Practices is purpose specification—that personal information obtained for one purpose cannot be used for another purpose without an individual's consent.[375] Often the purposes for the government collection of personal information vary widely from the purposes for which they are used after they are disclosed in public records. Governments collecting personal information should limit such uncontrolled drift in use. Access should be granted for uses furthering traditional functions of transparency such as the watchdog function; access should be denied for commercial solicitation uses because such uses do not adequately serve the functions of transparency. Rather, such uses make public records a cheap marketing tool, resulting in the further spread of personal information, which is often resold among marketers.

Use restriction laws must go beyond basic restrictions on access for commercial solicitation. The use of public records by information brokers or other entities that aggregate personal information and sell it to others is deeply problematic for the reasons discussed earlier in this Part. Although information brokers have brought a new level of accessibility to public records by combining them together in gigantic databases available online, they have also contributed greatly to the creation of the digital biography. This type of aggregated public record information is often not used for the purposes of checking governmental abuse or monitoring governmental activities. Rather, it is used to investigate individuals. This investigation is at the behest of other individuals, private detectives, employers, and law enforcement officials. Information brokers such as ChoicePoint collect public record information and supplement it with a host of other personal information, creating a convenient investigation

375. *See* HEW 1973 REPORT, *supra* note 172, at viii. The Fair Information Practices were developed by the United Stated Department of Health, Education and Welfare (HEW) in 1973, and they consist of a number of principles for the use and processing of personal information. The Fair Information Practices have proven to be highly influential in United States law as well as throughout the world. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 44, *at* http://stlr.stanford.edu/STLR/Articles/01_STLE_index.htm.

tool for government entities. The use of information brokers by the government to investigate citizens runs directly counter to the spirit of freedom of information laws, which were designed to empower individuals to monitor their government, not vice versa.

Certain information should be restricted from public records completely. The Administrative Office proposal to separate both paper and electronic documents into a public and private file for civil cases and to restrict access to certain documents in criminal proceedings such as presentence reports is a step in the right direction.[376] One example of information that should be excluded from public records is a person's Social Security number. Social Security numbers serve as a gateway to highly sensitive information such as financial accounts, school records, and a host of other data. Social Security numbers are very difficult to replace if they fall into the hands of an identity thief. As a routine practice, Social Security numbers should automatically be redacted from every document before being disclosed publicly.

Jurors, parties to litigation, and witnesses should all be informed of the extent to which their personal information could become a public record and must be given an opportunity to voice their privacy concerns and have information redacted.

The federal Privacy Act must be amended to provide more meaningful protection. Its restrictions on the use of Social Security numbers must be strengthened to regulate and restrict the use of Social Security numbers by the private sector. Further, the Privacy Act should contain meaningful remedies for violations and the "routine use" exception must be significantly tightened.

Finally, more laws like the Driver's Privacy Protection Act are necessary to nationalize public records law. We are becoming an information society where information is no longer localized. People frequently move from state to state and often do not live where they were born or grew up. We need a strong national information policy rather than the widely differing state public record regimes. This is the most efficient and effective means to govern information flow in the United States. A uniform baseline provides a good way to ensure privacy, for all citizens to know about their privacy rights in public record information, and for all users of information to know their responsibilities.

Therefore, a federal baseline should be established to govern public records in all states. This law should not preempt states from adopting stricter protections of privacy, but it must provide a meaningful floor of

376. Judicial Conference, *Request for Comment on Privacy and Public Access to Electronic Case Files* (Sept. 26, 2001), *available at* http:// www.privacy.uscourts.gov/ RFC.htm.

protection. Although each state should adopt its own statute akin to the federal Privacy Act, one option would be to extend the federal Privacy Act to the states.

We may never be able to achieve complete secrecy of information in many situations and, in some situations, complete secrecy would be undesirable. We can, however, limit accessibility and use. The next Part examines to what extent the Constitution might limit this approach.

III. PUBLIC RECORDS AND THE CONSTITUTION

In this Part, I examine whether the access and use restrictions I advocated in Part II can pass muster under the First Amendment to the United States Constitution. Understood broadly, the First Amendment protects openness in information flow. First, the Court and lower courts have held that the First Amendment provides certain rights of access to at least some government proceedings and records. Restrictions on the information available in public records might infringe upon this right. Second, freedom of speech and the press prevent the government from restricting the disclosure and dissemination of information. A close analysis of the Court's decisions, however, reveals that access and use restrictions are constitutional.

A. THE FIRST AMENDMENT RIGHT TO ACCESS

In a series of cases, the Supreme Court has held that the First Amendment mandates that certain government proceedings be open to the public. In *Richmond Newspapers, Inc. v. Virginia*,[377] a plurality of the Court concluded that the First Amendment provided the public with a right of access to criminal trials.[378] Although seven Justices agreed that the First Amendment provides a right of access to trials, no rationale achieved a majority.

Two years later, the Court coalesced around an approach in *Globe Newspaper Co. v. Superior Court*.[379] There, a Massachusetts law mandated that criminal trials be closed in all cases where juvenile victims of sexual assault testified to protect their privacy.[380] The Court struck down the law, reasoning that a "major purpose" of the First Amendment is "to protect the free discussion of governmental affairs."[381] The Court articulated a two-prong test to determine whether the right to access applies, first looking to whether the proceeding "historically has been open to the

377. 448 U.S. 555 (1980).
378. *Id*. at 575-78.
379. 457 U.S. 596 (1982).
380. *Id.* at 623.
381. *Id.* at 604 (citation omitted).

press and general public" and then examining whether access "plays a particularly significant role in the functioning of the judicial process and the government as a whole."[382] According to the Court, "public access to criminal trials permits the public to participate in and serve as a check upon the judicial process—an essential component in our structure of self-government."[383] The Court recognized that the right to access criminal trials is not absolute. A state can deny access to criminal proceedings if "the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest."[384] Although the state interest to protect juvenile sexual assault victims was compelling, the Court concluded that the mandatory rule requiring closure in all cases was too broad.[385]

Shortly after *Globe*, the Court resolved that the right to access extends beyond the immediate criminal trial to jury selection. In *Press-Enterprise Co. v. Superior Court* (*Press-Enterprise I*),[386] a trial for capital murder, the trial court severely restricted public access to the questioning of prospective jurors. Press-Enterprise moved for a release of the complete transcript of the voir dire proceedings, but the trial court refused because of concern for juror privacy since certain sensitive matters were discussed.[387] The Court held that there is a public interest in ensuring that jurors are "fairly and openly selected,"[388] and concluded that the trial court too broadly closed off access and failed to consider alternatives that were available to protect the jurors' privacy.[389]

The Court extended the right to access to pretrial proceedings in *Press-Enterprise Co. v. Superior Court* (*Press-Enterprise II*).[390] The Court reasoned that historical practice in the United States had been "to conduct preliminary hearings in open court"[391] and that public access to preliminary hearings served as an important "safeguard against the corrupt or overzealous prosecutor and against the compliant, biased, or eccentric judge."[392]

Lower courts determining the applicability of the First Amendment right to access apply the two-prong test of *Globe Newspaper* and the

382. *Id*. at 605-06.
383. *Id*. at 606.
384. *Id.* at 607.
385. *See id.* at 607-08.
386. 464 U.S. 501 (1984).
387. *Id*. at 504.
388. *Id*. at 509.
389. *Id*. at 512.
390. 478 U.S. 1 (1986).
391. *Id*. at 10.
392. *Id*. at 12-13 (internal quotations and citation omitted).

Press-Enterprise cases. Following the lead of the Supreme Court, lower courts have proclaimed that the right to access to criminal proceedings applies not only to trials, pretrial proceedings, and jury selection, but also to pretrial suppression, due process, and entrapment hearings,[393] as well as bail hearings.[394]

Although the Court has never squarely addressed whether the right of access applies beyond criminal proceedings, several lower courts have extended it to civil cases. For example, in *Publicker Industries, Inc. v. Cohen*,[395] the court reasoned that there was a long tradition for open civil trials and that "the civil trial, like the criminal trial, plays a particularly significant role in the functioning of the judicial process and the government as a whole."[396] Further, although no Supreme Court case directly addresses whether the First Amendment requires access to court documents, several courts "have concluded that the logic of *Press-Enterprise II* extends to at least some categories of court documents and records."[397] Not all courts agree, however.[398]

Courts have rarely applied the First Amendment right to access beyond court records to other public records. The rationale for the right to access turns on the need for knowledge about the government as an essential component of discourse about the government. Although the Court's cases involve judicial proceedings, the rationale can be logically extended beyond such proceedings. Therefore, even if a state did not have a sunshine law or a common law right of access, the Constitution might be interpreted to require a degree of openness.

Nevertheless, even under an expansive view, the right to access does not apply to efforts to restrict the access to personal information for particular uses. When public records illuminate government functioning, access to government records is generally consistent with the rationale for the First Amendment right to access. However, the grand purposes behind the right to access are simply not present in the context of much information gathering from public records today. As discussed in Part II,

393. *See* United States v. Criden, 675 F.2d 550, 557 (3d Cir. 1982).

394. *See* United States v. Chagra, 701 F.2d 354, 363 (5th Cir. 1983).

395. 733 F.2d 1059 (3d Cir. 1984).

396. *Id*. at 1070 (internal quotations and citation omitted).

397. United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997); *see also* Littlejohn v. BIC Corp., 851 F.2d 673, 678 (3d Cir. 1988) ("Access means more than the ability to attend open court proceedings; it encompasses the right of the public to inspect and to copy judicial records."); Associated Press v. United States Dist. Court, 705 F.2d 1143, 1145 (4th Cir. 1984) ("There is no reason to distinguish between pretrial proceedings and the documents filed in regard to them.").

398. Lanphere & Urbaniak v. Colorado, 21 F.3d 1508, 1512 (10th Cir. 1994) ("[T]here is no general First Amendment right in the public to access criminal justice records.").

public records are becoming a tool for powerful private sector interests to use in furtherance of commercial gain. These uses engender significant threats to individuals and to the structure of our society, and they do not shed light on the government.

In fact, the Constitution does not simply require open information flow; it also establishes certain responsibilities for the way that the government uses the information it collects. The Court has held that there are circumstances where the government cannot force individuals to disclose personal information absent a compelling government interest. In *NAACP v. Alabama*,[399] the Court struck down a state statute requiring the NAACP to disclose a list of the names and addresses of its members. The Court observed that there is a "vital relationship between freedom to associate and privacy in one's associations."[400] Noting that revelation of membership in the NAACP exposed members to potential economic reprisal and physical violence, the Court declared that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association."[401] *NAACP v. Alabama* suggests that the government cannot expose citizens to the potential perils that public disclosure may bring. Reasoning in a similar fashion, in *Greidinger v. Davis*,[402] the Fourth Circuit held that Virginia's voter registration system, which required voters to provide their Social Security numbers (which were then made publicly available), was unconstitutional because it forced people to risk public disclosure of their Social Security numbers in order to vote.[403] These cases can be read to establish the important principle that the fear of disclosure of personal information collected by the government is a recognized injury, one that can interfere with the exercise of fundamental rights.

Further, under the constitutional right to privacy, the Court has held that government has a duty to protect privacy when it collects personal data. In 1977, the Court addressed whether the right to privacy established in *Griswold v. Connecticut*,[404] *Eisenstadt v. Baird*,[405] and *Roe v. Wade*[406] extended to issues involving information as opposed to decisions about one's body, sexual conduct, or health. In the landmark case *Whalen v. Roe,*[407] the Court held that the right to privacy encompassed

399. 357 U.S. 449 (1958).
400. *Id*. at 462.
401. *Id*.
402. 988 F.2d 1344 (4th Cir. 1993).
403. *Id*. at 1354.
404. 381 U.S. 479 (1965).
405. 405 U.S. 438 (1972).
406. 410 U.S. 113 (1973).
407. 429 U.S. 589 (1977).

the protection of personal information. At issue in *Whalen* was a record-keeping system of people who obtained prescriptions for certain addictive medications.[408] The plaintiffs argued that the statute infringed upon their right to privacy.[409] The Court proclaimed that the constitutionally protected "zone of privacy" extends to two distinct types of interests: (1) *decisional privacy*, which the Court defined as "independence in making certain kinds of important decisions"; and (2) *information privacy*, which the Court defined as the "individual interest in avoiding disclosure of personal matters."[410] The Court concluded,

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . [I]n some circumstances that duty arguably has its roots in the Constitution . . . .[411]

Whalen recognized that when the government collected personal information, it took on a responsibility to keep it secure and avoid disclosing it to others.[412]

Since its creation in *Whalen*, the constitutional right to information privacy has begun to evolve in the courts.[413] The full extent of the gov-

408. Such medications included opium, cocaine, methadone, and amphetamines which were used in treating epilepsy, narcolepsy, migraine headaches, and certain psychological disorders. *See id.* at 593 n.8.

409. *Id.* at 598.

410. *Id.* at 599-600.

411. *Id*. at 605.

412. The Court reiterated this notion of constitutional protection for information privacy in *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977), concluding that President Nixon had a constitutional privacy interest in records of his private communications with his family. *Id.*

413. After *Whalen* and *Nixon*, the Court has done little to develop the right of information privacy. As one court observed, the right "has been infrequently examined; as a result its contours remain less than clear." Davis v. Bucher, 853 F.2d 718, 719 (9th Cir. 1988). The scope and existence of the constitutional right to information privacy remains in dispute among lower courts. A majority of the circuit courts has accepted the constitutional right to information privacy. *See, e.g.*, *In re* Crawford, 194 F.3d 954, 958 (9th Cir. 1999); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978). One circuit court has expressed "grave doubts" as to the existence of the right, stopping short of confronting the issue of whether the right existed. Am. Fed'n of Gov't Employees v. Dep't of Housing & Urban Dev., 118 F.3d 786, 788, 791-92 (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 (6th Cir. 1981). To date, only a handful of law review articles and notes have discussed the constitutional right to information privacy in great depth. *See, e.g.*, Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerg-*

ernment's information handling obligations awaits further development. It remains undetermined whether these obligations extend to measures beyond non-disclosure, such as the security of information, limited use, purpose specification, and other Fair Information Practices.

Nevertheless, taken together, the Court's jurisprudence in the contexts of free association and the constitutional right to information privacy suggests that the Constitution does not merely mandate public access to information but also obligates the government to refrain from disclosing personal information.

B. THE FIRST AMENDMENT RIGHT TO FREEDOM OF SPEECH AND PRESS

The First Amendment more directly fosters information flow about government activities by forbidding restrictions on freedom of speech and the press. These freedoms extend beyond disclosure about government to almost all forms of discourse, including speech about private citizens.

Understanding how use and access restrictions on public record information interact with the First Amendment requires a difficult navigation between two lines of Supreme Court jurisprudence. Under one line of cases—*Cox Broadcasting Corp. v. Cohn Publishing Co.*,[414] *Oklahoma Publishing Co. v. District Court In and For Oklahoma County*,[415] *Smith v. Daily Mail*,[416] and *Florida Star v. B.J.F.*[417] —the Court has held that when the government makes information publicly available in a public record, the press cannot be sanctioned for publishing it.[418] In *Los Angeles Police Department v. United Reporting Publishing Co.,*[419] however, the Court concluded that the government may selectively grant access to public record information.[420] In *Seattle Times Co. v. Rhinehart*,[421] the Court stated that the government may condition the receipt of discovery information on nondisclosure,[422] a conclusion that is supported by the Court's extensive unconstitutional condition jurisprudence. I will attempt to navigate these choppy waters of Supreme Court free speech jurispru-

ing Unencumbered Constitutional Right to Informational Privacy, 10 N. ILL. U. L. REV. 479 (1990); Bruce W. Clark, Note, *The Constitutional Right to Confidentiality*, 51 GEO. WASH. L. REV. 133 (1982); Gary R. Clouse, Comment, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536 (1982).

414. 420 U.S. 469 (1975).
415. 430 U.S. 308 (1977) (per curiam).
416. 443 U.S. 97 (1979).
417. 491 U.S. 524 (1989).
418. *See, e.g.*, *Cox Broad. Corp.*, 420 U.S. at 495; *Fla. Star*, 491 U.S. at 538.
419. 528 U.S. 32 (1999).
420. *Id.* at 40-41.
421. 467 U.S. 20 (1984).
422. *Id.* at 33-34.

dence to assess how the Court would (and should) analyze the types of use and access restrictions I suggested in Part II.

In a series of cases, the Court has struck down a number of statutes prohibiting the disclosure of information gleaned from public records. In *Cox Broadcasting Corp.*,[423] the Court held that a state could not impose civil liability based upon publication of a rape victim's name obtained from a court record.[424] The Court pronounced that "[o]nce true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it."[425] In justifying the rule, the Court concluded that not only does the ability to report on the criminal justice system provide greater transparency in government, but that the fact that the information was in a public record reduced the plaintiff's privacy interest.[426] "[T]he interests in privacy fade when the information involved already appears on the public record."[427] Punishing the press for publishing public record information would "invite timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public."[428] If states wish to protect privacy, they "must respond by means which avoid public documentation or other exposure of private information."[429]

After *Cox Broadcasting Corp.*, in *Oklahoma Publishing Co.*,[430] the Supreme Court held that a state court could not prohibit the media from disclosing the name and photograph of an eleven-year-old boy when the media had gleaned that information by attending a juvenile proceeding.[431] In *Smith*[432] the Court struck down a statute prohibiting the publication of the names of juvenile offenders: "[I]f 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."[433]

This line of cases culminated in *Florida Star*,[434] in which a newspaper published the name of a rape victim, which it obtained in a publicly

423. 420 U.S. 469 (1975).
424. *Id.* at 496-97.
425. *Id.* at 496.
426. *Id.* at 494-95.
427. *Id.*
428. *Id.* at 496.
429. *Id.*
430. 430 U.S. 308 (1977) (per curiam).
431. *Id.* at 311-12.
432. 443 U.S. 97 (1979).
433. *Id.* at 103.
434. 491 U.S. 524 (1989).

released police report. The report was in a room with signs indicating that the names of rape victims were not part of the public record and were not to be published.[435] The reporter even admitted that she knew she was not allowed to report on the information.[436] The victim's fellow workers and friends read the article; her mother received threatening phone calls from a man who stated he would rape the woman again; and these events caused her to change her phone number and residence, seek police protection, and obtain mental health counseling.[437] Under a Florida law prohibiting the mass communication of the names of rape victims, the paper was found civilly liable.[438] The Court, however, held that the Florida law ran afoul of the First Amendment. "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 . . . ."[439]

Taken together, these cases support the premise that once the government makes information public, the government cannot subsequently sanction its further disclosure. In *Cox*, however, 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."[440]

The Court addressed this issue in *United Reporting Publishing Corp.*[441] when it examined the constitutionality of California's access restriction law for arrestee information.[442] The law required those seeking access to the information to execute a declaration under penalty of perjury that address information "shall not be used directly or indirectly to sell a product or service to any individual or group of individuals."[443] Rejecting a facial challenge that the law infringed upon commercial speech, the Court reasoned that the statute was not "prohibiting a speaker from conveying information that the speaker already possesses" but was merely "a governmental denial of access to information in its possession" under which it had no duty to disclose.[444] As long as the government is not under a duty to provide access to information, it can selectively de-

435. *Id.* at 546 (White, J., dissenting).
436. *Id.*
437. *Id.* at 528.
438. *Id.* at 526.
439. *Id.* at 541.
440. *Cox Broad.*, 420 U.S. at 496 n.26 (1975).
441. 528 U.S. 32, 34 (1999).
442. *Id.* at 34.
443. CAL. GOV'T CODE § 6254(f)(3) (West Supp. 1999).
444. *United Reporting Publ'g Corp.*, 528 U.S. at 40.

termine who shall have access to it.[445] The Court also held in *Houchins v. KQED Inc.*[446] that "[n]either the First Amendment nor the Fourteenth Amendment mandates a right of access to government information or sources of information within the government's control."[447]

In addition to the cases discussed above, the Supreme Court's "unconstitutional condition" jurisprudence lends further support for the government's ability to condition access to public records.[448] A series of cases establishes the limits of what access conditions are permissible. According to the doctrine, originating during the *Lochner* era, "government may not grant a benefit on the condition that the beneficiary surrender a constitutional right, even if the government may withhold that benefit altogether."[449] Kathleen Sullivan aptly characterizes the doctrine as "riven with inconsistencies."[450]

In several cases decided during the 1950s and 1960s, the Court invalidated several conditions requiring that recipients of the government's largesse surrender constitutional rights. In *Speiser v. Randall*,[451] the Court held that war vetarans could not be required to take a loyalty oath in order to receive a property tax exemption because it "will have the ef-

445. In *Seattle Times Co. v. Rhinehart*, the Court held that a party obtaining access to information via discovery could be restricted from disclosing that information through a protective order. 467 U.S. 20, 37 (1984). A newspaper challenged a protective order on First Amendment grounds, but the Court upheld the order, noting that the broad discovery rules permit parties to obtain information "that not only is irrelevant but if publicly released could be damaging to reputation and privacy." *Id.* at 35. Therefore, the Court held that when a "protective order is entered on a showing of good cause as required by Rule 26(c), is limited to the context of pretrial civil discovery, and does not restrict the dissemination of the information if gained from other sources, it does not offend the First Amendment." *Id*. at 37 (citation omitted).

446. 438 U.S. 1 (1978).

447. *Id*. at 15. In a series of cases, the Court has held that outside of the First Amendment right of access, freedom of the press does not require that the press be given any special rights to acquire information from the government. *See, e.g.,* Nixon v. Warner Communications, Inc., 435 U.S. 589, 609 (1978) ("The First Amendment generally grants the press no right to information about a trial superior to that of the general public.); Pell v. Procunier, 417 U.S. 817, 834 (1974) (The Constitution does not . . . require government to accord the press special access to information not shared by members of the public generall) (citation omitted); Zemel v. Rusk, 381 U.S. 1, 17 (1965) ("The right to speak and publish does not carry with it the unrestrained right to gather information."). Additionally, the Court held that the First Amendment cannot foreclose a lawsuit by a confidential source to enforce a newspaper's promise of confidentiality because the press "has no special immunity from the application of general laws. . . . [and] no special privilege to invade the rights and liberties of others." Cohen v. Cowles Media Co., 501 U.S. 663, 670 (1991) (quoting Associated Press v. NLRB, 301 U.S. 103, 132-22 (1937)).

448. Kathleen Sullivan, *Unconstitutional Conditions*, 102 HARV. L. REV. 1413, 1418 (1989).

449. *Id.* at 1415.

450. *Id*. at 1416.

451. 357 U.S. 513 (1958).

fect of coercing the claimants to refrain from the proscribed speech."[452] *Sherbert v. Verner*[453] struck down the denial of state unemployment benefits to a person who refused to work on Saturday for religious reasons because it "forces her to choose between following the precepts of her religion and forfeiting benefits."[454] Furthermore, in *Shapiro v. Thompson*,[455] the Court held unconstitutional the denial of welfare benefits to people who had recently moved into a state because it chilled the right to interstate travel.[456]

Cases decided after the mid-1970s, however, are very inconsistent. In *Regan v. Taxation With Representation of Washington*,[457] the Internal Revenue Code provided a tax benefit to veterans' lobbying groups but not other charities.[458] The Court applied minimal scrutiny because Congress was not required to provide any tax advantage for lobbying.[459] The government was simply selecting "particular entities or persons for entitlement."[460]

A year later in *FCC v. League of Women Voters of California*,[461] the Court applied heightened scrutiny to strike down a condition that federally-funded broadcasting stations refrain from editorializing in order to receive funding from the government.[462] Similarly, in *Arkansas Writers' Project, Inc. v. Ragland*,[463] the Court struck down a state sales tax that excluded certain types of magazines (religious, professional, trade, and sports) but not others.[464]

Returning to its permissive view of conditional funding, the Court in *Lyng v. International Union*[465] upheld a statute making households ineligible for food stamps if any member of that household was on strike: "[E]ven where the Constitution prohibits coercive governmental interference with specific individual rights, it does not confer an entitlement to such funds as may be necessary to realize all the advantages of that freedom."[466] Likewise, the Court reasoned in *Maher v. Roe*[467] that the gov-

452. *Id.* at 519.
453. 374 U.S. 398 (1963).
454. *Id*. at 404.
455. 394 U.S. 618 (1969).
456. *See id*. at 634.
457. 461 U.S. 540 (1983).
458. *Id.* at 542.
459. *See id.* at 549-50.
460. *Id.* at 549.
461. 468 U.S. 364 (1984).
462. *Id.* at 402.
463. 481 U.S. 221 (1987).
464. *Id.* at 233.
465. 485 U.S. 360 (1988).
466. *Id.* at 369 (internal quotations omitted).

ernment can selectively provide funds for normal childbirth without having also to fund abortions.[468]

Today, the leading case on the subject is *Rust v. Sullivan*,[469] in which Congress prohibited workers in federally funded family planning services from engaging in counseling advocating abortion as a method of family planning.[470] Rejecting a First Amendment challenge, the Court concluded that

> [t]he Government can, without violating the Constitution, selectively fund a program to encourage certain activities it believes to be in the public interest, without at the same time funding an alternative program which seeks to deal with the problem in another way. In so doing, the Government has not discriminated on the basis of viewpoint; it has merely chosen to fund one activity to the exclusion of the other . . . .[471]

As these cases indicate, the government retains significant discretion in how it chooses to distribute its largesse. Public record information is part of this largesse, and the most recently decided unconstitutional condition cases suggest that the government can impose certain conditions on how this information is used before it grants access.

The Court's jurisprudence thus creates a distinction between pre-access conditions on obtaining information and post-access restrictions on the use or disclosure of the information. If the government is not obligated to provide access to certain information by the First Amendment, it can amend its sunshine laws to establish pre-access conditions, restricting access for certain kinds of uses. Governments can make a public record available *on the condition that* certain information is not disclosed or used in a certain manner. However, governments cannot establish post-access restrictions on the disclosure or use of information that is publicly available.[472] Once the information is made available to the public, the *Florida Star* case prohibits a state from restricting use.[473]

One could certainly argue that the Court's distinction between pre-access and post-access restrictions seems rather tenuous. States can accomplish the same restrictions on disclosure of public information that the Court struck down in *Florida Star* with a simple redrafting of their statutes. In *Florida Star*, Florida could have easily rewritten its law to make rape victims' names available on the condition that the press promise they not

467. 432 U.S. 464 (1977).

468. *Id.* at 479.

469. 500 U.S. 173 (1991).

470. *Id.* at 202-03.

471. *Id*. at 193.

472. *See* Bartnicki v. Vopper, 523 U.S. 514 (2001).

473. 491 U.S. at 524 (1989); *see also* Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 838 (1978) (holding that a state could not criminalize a newspaper's disclosure of leaked information about a judicial disciplinary proceeding).

be disclosed. Those seeking access could be required to sign a declaration that the information would not be disclosed or used for certain purposes. Conditional access and use restrictions thus appear to be an end-run around *Florida Star*. Can the Court's distinction between pre- and post-access restrictions be defended?

Certain language in *Florida Star* suggests that the case turns on the government's unclean hands, as the Court emphasizes the government's failure "to police itself in disseminating information."[474] "[W]here the government has made certain information publicly available," the Court observed, "it is highly anomalous to sanction persons other than the source of its release."[475] Acting hypocritically by disclosing information and then punishing the press for the same offense, the state cannot give the press the forbidden fruit and ask the press not to eat it. Moreover, the Florida statute had no scienter requirement; it imposed liability regardless of whether the rape victim's name was already known throughout the community.[476]

This distinction between post- versus pre-access conditions can be defended as a protection against the chilling effects caused by uncertainty over the public record information that can be disclosed. According to *Cox Broadcasting Corp.* and *Florida Star*, one should not have to act at her peril whenever she discloses information obtained from a public record. By making access conditional on a promise not to disclose or restricting access in certain cases, however, there is a clear notice to the recipient as to her obligations and responsibilities in handling that information.

Without a distinction between post- and pre-access conditions, the government would be forced into an all-or-nothing tradeoff between transparency and privacy. The government could make records public, allowing all uses of the personal information contained therein, or the government could simply make records unavailable to the public for any purpose. However, by making access conditional on accepting certain responsibilities when using data—such as using it for specific purposes, not disclosing it to others, and so on, certain functions of transparency can be preserved at the same time privacy is protected.

Has the Court too quickly dispatched with the free speech implications of conditional or limited access regulation? Do restrictions on commercial access, for example, constitute unconstitutional content-based restrictions on free speech because they single out specific messages and viewpoints—namely, commercial ones? Prior to *United Re-*

474. 491 U.S. at 538.
475. *Id.* at 535.
476. *Id.* at 539.

porting Publishing, courts were divided on the issue.[477] Although commercial speech was originally not considered to fall within the domain of the First Amendment,[478] in 1976, the Court recognized a limited First Amendment protection for commercial speech.[479] Typically, a content-based restriction on regular speech is reviewed under strict scrutiny, the most stringent form of constitutional scrutiny.[480] Content-based restrictions on commercial speech, however, are reviewed under a form of intermediate scrutiny. *Central Hudson Gas & Electric Corp. v. Public Service Commission of N.Y.*[481] sets forth the current test for analyzing restrictions on commercial speech.[482] Courts are to first examine whether commercial speech is misleading or involves illegal activity; if so, it is not protected.[483] If, however, the speech is not illegal or deceptive, then it is protected by intermediate scrutiny.[484] The government interest must be substantial; the regulation must directly advance the government interest; finally, the regulation must be appropriately tailored to advance the government interest (i.e., be no more extensive than necessary).[485]

The issue, then, is whether access restrictions are subject to no First Amendment protection (except where barred by the First Amendment right to access) or whether they implicate speech and are subject to intermediate scrutiny under *Central Hudson*. Dissenting in *United Reporting Publishing Corp.*, Justice Stevens argued that the California access and use restriction improperly singled out "a narrow category of persons

477. *Compare* Amelkin v. McClure, 168 F.3d 893, 902 (6th Cir. 1999), *vacated and remanded by* McClure v. Amelkin, 528 U.S. 1059 (striking down an access restriction statute), *and* Speer v. Miller, 15 F.3d 1007 (11th Cir. 1994) (holding that an access restriction statute implicated First Amendment), *and* Babkes v. Satz, 944 F. Supp. 909, 912-13 (S.D. Fla. 1996) (striking down an access restriction statute), *with* Lanphere & Urbaniak v. Colorado, 21 F.3d 1508, 1516 (10th Cir. 1994) (upholding Colorado access restriction to arrestee records), Fed. Election Comm'n v. Int'l Funding Inst., Inc., 969 F.2d 1110, 1117-18 (D.C. Cir. 1992) (upholding the Federal Election Campaign Act's making political committee contributor lists available for public inspection with the limitation that any information copied may not be sold or used for the purpose of soliciting contributions or for commercial purposes because there was no pre-existing right to have access to such lists), *and* DeSalvo v. State, 624 So. 2d 897, 901 (La. 1993) (upholding access restriction statute), *and* Walker v. S. C. Dep't of Highways & Pub. Transp., 466 S.E.2d 346, 348 (S.C. 1995) (holding that vehicle report access restriction "regulates only access to information").

478. *See* Valentine v. Chrestensen, 316 U.S. 52, 54 (1942).

479. *See* Va. Pharmacy Bd. v. Va. Citizen's Consumer Council, Inc., 425 U.S. 748, 770 (1976).

480. *See* Daniel J. Solove, Note, *Faith Profaned: The Religious Freedom Restoration Act and Religion in the Prisons*, 106 YALE L.J. 459, 461 (1996).

481. 447 U.S. 557 (1980).

482. *Id.* at 574.

483. *Id.* at 563-64.

484. *Id.* at 564.

485. *Id.* at 565.

solely because they intend to use the information for a constitutionally protected purpose."[486]

Stevens's argument is rejected by the unconstitutional condition cases (especially *Rust*), which suggest that many access restrictions will not implicate speech. *Rust* and some of its predecessors have engendered significant criticism, and in my opinion, rightly so. Although I believe that a number of the unconstitutional conditions cases, including *Rust*, were wrongly decided, many use and access restrictions on personal information in public records will still pass constitutional muster without the aid of these cases.

Kathleen Sullivan has made one of the most persuasive attacks against the unconstitutional condition cases. As she explains, the Court's approach is to look for when conditions coerce individuals to surrender rights or whether such conditions are enacted out of subterfuge and manipulation.[487] This approach, Sullivan argues, is too narrow and crabbed, for unconstitutional conditions "can alter the balance of power between government and rightholders" and can "skew the distribution of constitutional rights among rightholders because [the government] necessarily discriminates facially between those who do and those who do not comply with the condition."[488] Accordingly, Sullivan suggests a broader form of analysis for unconstitutional conditions, one that "would subject to strict review any government benefit condition whose primary purpose or effect is to pressure recipients to alter a choice about exercise of a preferred constitutional liberty in a direction favored by government."[489]

Rust certainly lends support for the theory that government can make access to personal information in public records conditional on non-disclosure or on particular uses. Additionally, *Rust* supports selective access restrictions. *Rust* is a troubling case in my opinion, but I contend that the free speech argument against public record access restrictions fails without having to enlist the aid of cases like *Rust.* In *Rust*, the government made funding conditional on the expression of a particular viewpoint. This is troublesome, for it is a use of government power (albeit in the guise of a carrot rather than a stick) to restrict certain views. In contrast, commercial access restrictions are not being applied because of disagreement with the message that commercial users wish to send. Nor do they favor a particular speaker or specific ideas. Although particular categories of use (i.e., commercial) are being singled out, avoiding viewpoint discrimination does not entail avoiding all attempts to catego-

486. L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32, 45 (1999) (Stevens, J., dissenting).

487. *See* Sullivan, *supra* note 448, at 1413-21.

488. *Id*. at 1490.

489. *Id*. at 1499-1500.

rize or limit uses of information. Indeed, the First Amendment constitutional regime depends upon categorizing speech. Obscene speech and fighting words are not protected,[490] false speech about public figures is protected in a limited way,[491] and commercial speech is protected by intermediate scrutiny. Although there is no bright line that distinguishes when certain categories map onto particular viewpoints to such a degree as to constitute discrimination based on viewpoint, the category of commercial speech is broad enough to encompass a multitude of viewpoints and is a category that forms part of the architecture of the current constitutional regime.

Therefore, governments should be able to restrict access for certain purposes or condition access on an enforceable promise not to engage in certain uses of information. Although the Court has opened a wide door to viewpoint discrimination in *Rust*, a more appropriate approach is to curtail broad categories of uses (i.e., commercial, information brokering, further disclosure, and so on) rather than narrow categories, which often single out particular viewpoints. Thus, for example, governments should not restrict access to public records to those who wish to use the information to advocate for certain causes rather than others. Nor could the government restrict access based on the particular beliefs or ideas of the person or entities seeking access to the information.

Even if *Rust* were wrongly decided, we are still not bound to a rigid version of neutrality that forces the government into a total access versus no access regime. The issue is whether the government is singling out certain uses because of an intent to curtail particular ideas it dislikes. A limitation on commercial use is broad enough to encompass a diverse enough range of viewpoints, and the government is merely limiting uses of information rather than the expression of particular ideas.[492]

490. Chaplinsky v. New Hampshire, 315 U.S. 568, 573 (1942).

491. *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 352 (1974); Curtis Publ'g Co. v. Butts, 388 U.S. 130, 160-61 (1967); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 296 (1964).

492. Even if the *Central Hudson* test were to apply, there is a good argument that commercial use restrictions would satisfy the test. It is true that before *United Reporting,* a number of courts struck down access and use restrictions. However, they did so based on their adherence to the secrecy paradigm. These courts often rejected the state's asserted privacy interest because other uses of information were permitted. *See, e.g.*, United Reporting Publ'g Co. v. Cal. Highway Patrol, 146 F.3d 1133, 1139 (9th Cir. 1998), *rev'd* L. A. Police Dep't v. United Reporting Publ'g Co., 528 U.S. 32 (1999) ("The fact that journalists, academicians, curiosity seekers, and other noncommercial users may peruse and report on arrestee records . . . belies the LAPD's claim that the statute is actually intended to protect the privacy interests of arrestees."); Speer v. Miller, 15 F.3d 1007, 1011 (11th Cir. 1994) ("We note that any privacy arguments the state asserts are disingenuous in light of the fact that the statute carves out an exception for the media to place any information they obtain on the front page of any newspaper in Georgia.") (citation omitted); Babkes v. Satz, 944 F. Supp. 909, 912 (S.D. Fla. 1996). According to this argument, if states really

CONCLUSION: REGULATING PUBLIC RECORDS

Public records are increasingly posing a serious threat to privacy in the Information Age. To understand this threat, our conceptions of privacy must be adapted to today's technological realities. We must abandon the secrecy paradigm and recognize that what is public can be private—not in the sense that it is secret, but in that uses and disclosures of information can be limited. Privacy is about degrees of accessibility. The threat to privacy is not in isolated pieces of information, but in increased access and aggregation, the construction of digital biographies and the uses to which they are put.

I advocate access and use restrictions on information as well as a federal baseline of protection for all public records beyond the limited scope of DPPA. The key issue is whether such a solution would be constitutional. As long as access and use restrictions are based on a conditional grant of access, they will pass constitutional muster. Further, the Constitution establishes an obligation to protect against disclosure and uses of information by the government. Today, government public record systems are not meeting this constitutional obligation. States must begin to rethink their public record regimes, and the federal government should step in to serve as the most efficient mechanism to achieve this goal. It is time for the public records laws of this country to mature to meet the problems of the Information Age.

want to protect privacy, they should also restrict the noncommercial uses of information, such as publication of personal information by the media. This argument is also raised by Justice Stevens in dissent in *United Reporting*: "By allowing such widespread access to the information, the State has eviscerated any rational basis for believing that the [statute] will truly protect the privacy of these persons." *United Reporting*, 528 U.S. at 46 (Stevens, J., dissenting). As I argued earlier, however, the fact that personal information is disclosed selectively does not extinguish one's privacy interest. It is the particular uses of information that pose some of the greatest problems for privacy. Even if the information is available for other purposes, there is an interest in limiting access and uses, especially commercial access given the escalating affront to privacy caused by private sector public record aggregation and considering the fact that commercial users do not advance the purpose of making such records public in the first place.