2001

Privacy and Power: Computer Databases and Metaphors for Information Privacy

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

ARTICLES

Privacy and Power: Computer Databases and Metaphors for Information Privacy

Daniel J. Solove*

Journalists, politicians, jurists, and legal academics often describe the privacy problem created by the collection and use of personal information through computer databases and the Internet with the metaphor of Big Brother—the totalitarian government portrayed in George Orwell's Nineteen Eighty-Four. Professor Solove argues that this is the wrong metaphor. The Big Brother metaphor as well as much of the law that protects privacy emerges from a longstanding paradigm for conceptualizing privacy problems. Under this paradigm, privacy is invaded by uncovering one's hidden world, by surveillance, and by the disclosure of concealed information. The harm caused by such invasions consists of inhibition, self-censorship, embarrassment, and damage to one's reputation. Privacy law has developed with this paradigm in mind, and consequently, it has failed to grapple effectively with the database problem. Professor Solove argues that the Big Brother metaphor merely reinforces this paradigm and that the problem is better captured by Franz Kafka's The Trial. Understood with the Kafka metaphor, the problem is the powerlessness, vulnerability, and dehumanization created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information. Professor Solove illustrates that conceptualizing the problem with the Kafka metaphor has profound implications both for the law of information privacy and for choosing legal approaches to solve the problem.

* Assistant Professor, Seton Hall Law School; J.D., Yale University. I would like to thank Jack Balkin, Howard Erichson, Alan Hobbs, Jerry Kang, Raymond Ku, Michael Risinger, Marc Rotenberg, Richard St. John, Don Stepka, Charles Sullivan, Michael Sullivan, Richard Weisberg, and the participants of the Emory University Legal Theory Workshop for their exceedingly helpful comments and insights. I would also like to thank my research assistant, Peter Choy, for his capable assistance, and the Seton Hall Law School faculty scholarship fund for its financial support for this project.

I. INTRODUCTION

We are in the midst of an information revolution, and we are only beginning to understand its implications. In the past decade, we have undergone a dramatic transformation in the way we shop, bank, and go about our daily business—changes that have resulted in an unprecedented proliferation of records and data.[1] The small details that were once captured in dim memories or fading scraps of paper are now preserved forever in the digital minds of computers, vast databases with fertile fields of personal data. Our wallets are stuffed with ATM cards, calling cards, frequent shopper cards, and credit cards—all of which can be used to record where we are and what we do. Every day, rivulets of information stream into electric brains to be sifted, sorted, rearranged, and combined in hundreds of different ways. Technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. Companies are constructing gigantic databases of psychological profiles, amassing data about an individual's race, gender, income, hobbies, and purchases. It is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital biography composed in the collective computer networks of the world.

Since their creation, computer databases have been viewed as problematic—a fear typically raised under the mantra of "privacy."[2] Databases certainly

1. Although the transformation started in the mid-twentieth century, it began to reach a new level of maturity since the rise of the Internet in the 1990s.

2. *See, e.g.*, ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY 3-5 (1972) (discussing debates over computer databases and privacy in the 1960s). Indeed, long before the advent of the computer database, Justice Brandeis prophesized: "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

present a privacy problem, but what exactly is the nature of that problem? Although the problem of databases is understood as one of concern over privacy, beyond this, the problem is often not well defined. How much weight should our vague apprehensions be given, especially considering the tremendous utility, profit, and efficiency of using databases? The answer to this question depends upon how the privacy problem of databases is conceptualized. Unfortunately, so far, the problem has not been adequately articulated.

Journalists,[3] politicians,[4] and jurists[5] often describe the problem created by databases with the metaphor of Big Brother—the harrowing totalitarian government portrayed in George Orwell's *Nineteen Eighty-Four*.[6] For example, in 1974, when the use of computer databases was in its infancy, Justice Douglas observed:

> With dossiers being compiled by commercial credit bureaus, state and local law enforcement agencies, the CIA, the FBI, the IRS, the Armed Services, and the Census Bureau, we live in an Orwellian age in which the computer has become "the heart of a surveillance system that will turn society into a transparent world."[7]

Legal academics similarly characterize the problem.[8] In *The Culture of*

---

3. *See, e.g.*, William Branigin, *Employment Database Proposal Raises Cries of '"Big Brother,'"* WASH. POST, Oct. 3, 1995, at A17; James Gleick, *Big Brother Is Us: Our Privacy is Disappearing, But Not by Force. We're Selling it, Even Giving it Away*, N.Y. TIMES , Sept. 29, 1996, (magazine), at 130; Carey Goldberg, *DNA Databanks Giving Police a Powerful Weapon, and Critics*, N.Y. TIMES, Feb. 19, 1998, at A1 ("The very existence of a DNA database smacks more of a Big Brother-ish assault on privacy than the existence of the national computerized network of fingerprints, civil libertarians say.").

4. To respond to the computerization of records, in 1984 a House committee held hearings called "1984 and the National Security State." PRISCILLA M. REGAN, LEGISLATING PRIVACY 93 (1995); *see also* 140 CONG. REC. H9797, H9810 (statement of Rep. Kennedy) (concerning the Consumer Reporting Reform Act of 1994, Senate Bill 783) ("For tens—if not hundreds—of thousands of consumers, the promise of the information highway has given way to an Orwellian nightmare erroneous and unknowingly disseminated credit reports."); Tod Robberson, *Plan for Student Database Stirs Opposition in Fairfax*, WASH. POST, Jan. 9, 1997, at A1 ("'This thing is Orwellian,' said board member Carter S. Thomas (Springfield). 'It triples the amount of data that can be collected on individual students, teachers and even janitors.'").

5. *See* J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 608 (D.C. Cir. 1996) (Tatel, J., dissenting) ("Congress passed the Privacy Act to give individuals some defenses against governmental tendencies towards secrecy and 'Big Brother' surveillance.'"); McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998) ("In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.").

6. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

7. Sampson v. Murray, 415 U.S. 61, 96 n.2 (1974) (Douglas, J., dissenting) (quoting Arthur Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 2 (1972).

8. *See infra*, notes 133-144, and accompanying text; *see also* Charles N. Faerber, *Book Versus Byte: The Prospects and Desirability of a Paperless Society*, 17 J. MARSHALL J.

Surveillance, William Staples observes that we have internalized Big Brother —we have created a Big Brother culture, where we all act as agents of surveillance and voyeurism.[9] "The specter of Big Brother has haunted computerization from the beginning," Abbe Mowshowitz observes. "Computerized personal record-keeping systems, in the hands of police and intelligence agencies, clearly extend the surveillance capabilities of the state."[10]

Even when not directly discussing Big Brother, commentators describe the problem in similar conceptual terms. Paul Schwartz and Joel Reidenberg write:

> [Computer] data processing creates a potential for suppressing a capacity for free choice. The more that is known about an individual, the easier it is to force his obedience. Through the use of databanks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children.[11]

Commentators have adapted the Big Brother metaphor to describe the threat to privacy caused by private sector databases, often referring to private sector entities as "Little Brothers."[12] As David Lyon puts it: "Orwell's

---

COMPUTER & INFO. L. 797, 798 (1999) ("Many are terrified of an Orwellian linkage of databases allowing any individual to leave home without a wallet or purse but with a retinal pattern or other biometric identifier and then to perform any conceivable financial or documentary transaction."); Bryan S. Schultz, *Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 U. CIN. L. REV. 779, 797 (1999) ("As technology propels America toward a cashless marketplace where financial transactions are conducted with the aid of computer record-keeping, society inches closer to fulfilling George Orwell's startling vision of a nation where 'Big Brother' monitors the who, what, where, when, and how of every individual's life."); Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values*, 72 CHI.-KENT L. REV. 271, 273 (1996) (stating that Americans would view the idea of government data protection boards to regulate private sector databases as "calling on 'Big Brother' to protect citizens from 'Big Brother.'"); Wendy Wuchek, *Conspiracy Theory: Big Brother Enters the Brave New World of Health Care Reform*, 3 DEPAUL J. HEALTH CARE L. 293, 303 (2000). In 1999, the University of Chicago Law School hosted a conference entitled *1984: Orwell and Our Future*.

9. WILLIAM G. STAPLES, THE CULTURE OF SURVEILLANCE: DISCIPLINE AND SOCIAL CONTROL IN THE UNITED STATES 129-134 (1997).

10. Abbe Mowshowitz, *Social Control and the Network Marketplace*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 79, 95-96 (David Lyon & Elia Zureik eds., 1996).

11. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 39 (1996); *see also* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) [hereinafter Schwartz, *Privacy and Participation*].

12. *See, e.g.*, Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. LJ. 357, 377 (2000) (describing privacy problem created by the private-sector as the "little brother" problem); Marsha Morrow McLaughlin & Suzanne Vaupel, *Constitutional Right of Privacy and Investigative Consumer Reports: Little Brother Is Watching You*, 2 HASTINGS CONST. L.Q. 773 (1975); Hon. Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 FLA. ST. U. L. REV. 25, 27 (1997) ("In his book, *1984*, we were warned by George Orwell to watch out for 'Big Brother.' Today, we are cautioned to look out for 'little brother' and 'little sister.'"); Thomas L.

dystopic vision was dominated by the central state. He never guessed just how significant a decentralized consumerism might become for social control."[13] "Today," Paul Schwartz observes, "myriad Big and Little Brothers are involved in the collection and processing of personal data in the United States."[14] Katrin Byford writes: "Life in cyberspace, if left unregulated, thus promises to have distinct Orwellian overtones—with the notable difference that the primary threat to privacy comes not from government, but rather from the corporate world."[15] In his book, *The End of Privacy*, Reg Whitaker also revises the Big Brother narrative into one of a multitude of Little Brothers.[16]

The use of the Big Brother metaphor to understand the database privacy problem is hardly surprising. Big Brother has long been the metaphor of choice to characterize privacy problems, and it has frequently been invoked when discussing police search tactics,[17] wiretapping and video surveillance,[18] and drug testing.[19] With regard to computer databases, however, Big Brother

---

Friedman, *Foreign Affairs: Little Brother*, N.Y. TIMES, Sept. 26, 1999, Sec. 4 at 17; Wendy R. Leibowitz, *Personal Privacy and High Tech: Little Brothers Are Watching You*, NAT'L L.J., Apr. 7, 1997, at B16.

13. DAVID LYON, THE ELECTRIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 78 (1994).

14. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1657 n.294 (1999).

15. Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment,* 24 RUTGERS COMPUTER & TECH. L.J. 1, 50 (1998).

16. REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 160-75 (1999).

17. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 466 (1989) (Brennan, J., dissenting) (quoting passage from *Nineteen Eighty-Four* to criticize the majority's holding that viewing the defendant's greenhouse from a low-flying helicopter was not a search); United States v. Kyllo, 190 F.3d 1041, 1050 (9th Cir. 1999) *rev'd* 121 S. Ct. 2038 (Noonan, J., dissenting) ("The first reaction when one hears of the Agema 210 [thermal imaging device used to detect heat emissions from the home] is to think of George Orwell's *1984*. Although the dread date has passed, no one wants to live in a world of Orwellian surveillance."); Lorenzana v. Superior Court, 511 P.2d 33, 41 (Cal. 1973) (en banc) ("Surely our state and federal Constitutions and the cases interpreting them foreclose a regression into an Orwellian society. . . .").

18. *See, e.g.*, United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994) ("It is clear that silent video surveillance, like the interception of wire, oral, or electronic communications under Title I, results in a very serious, some say Orwellian, invasion of privacy."); United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (stating that "indiscriminate video surveillance raises the spectre of the Orwellian state."); United States v. Marion, 535 F.2d 697, 698 (2d Cir. 1976) (Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to "guard against the realization of Orwellian fears. . . ."); People v. Teicher, 422 N.E.2d 506, 513 (N.Y. 1981) ("Certainly the Orwellian overtones involved in this activity demand that close scrutiny be given to any application for a warrant permitting video electronic surveillance.").

19. *See, e.g.*, Capua v. City of Plainfield, 643 F. Supp. 1507, 1511 (D.N.J. 1986) (stating that drug testing is "George Orwell's 'Big Brother' Society come to life"); Edward M. Chen, Pauline T. Kim, & John M. True, *Common Law Privacy: A Limit on an Employer's Power to Test for Drugs*, 12 GEO. MASON L. REV. 651, 674 (1990)

is the wrong metaphor.

In this article, I argue that the database problem cannot adequately be understood by way of the Big Brother metaphor—even when adapted to account for private sector databases. Although the Big Brother metaphor certainly describes particular facets of the problem, it neglects many crucial dimensions. This oversight is far from inconsequential, for the way we conceptualize a problem has important ramifications for law and policy. I argue that the Big Brother metaphor as well as much of the law that protects privacy[20] emerges from an older paradigm for conceptualizing privacy problems. Under this paradigm, privacy is invaded by uncovering one's hidden world, by surveillance, and by the disclosure of concealed information. The harm caused by such invasions consists of inhibition, self-censorship, embarrassment, and damage to one's reputation. Privacy law has developed with this paradigm in mind, and consequently, it has failed to adapt to grapple effectively with the database problem. The Big Brother metaphor merely reinforces this old paradigm, and impedes our understanding of the problem.

I argue that the problem is best captured by Franz Kafka's depiction of bureaucracy in *The Trial*[21]—a more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information.

Generally, a metaphor is the use of one thing to represent or symbolize another.[22] As George Lakoff and Mark Johnson observe in their groundbreaking analysis, metaphors are not mere linguistic embellishments or decorative overlays on experience; they are part of our conceptual systems and affect the way we interpret our experiences.[23] Metaphor is not simply an act of description; it is a way of conceptualization. "The essence of metaphor," write Lakoff and Johnson, "is understanding and experiencing one kind of thing in terms of another."[24] Much of our thinking about a problem involves the metaphors we use. According to J. M. Balkin, "metaphoric models selectively describe a situation, and in so doing help to suppress alternative conceptions."[25] Metaphors do not just distort reality but compose it; the "power [of metaphors] stems precisely from their ability to empower

---

(characterizing drug testing as "George Orwell's 'Big Brother' Society come to life").

20. I will refer to this diverse body of law generally as "privacy law." Privacy law consists of an interrelated web of tort law, constitutional law, evidentiary privileges, contract law, property law, state and federal statutory law, and criminal law.

21. FRANZ KAFKA, THE TRIAL (Willa & Edwin Muir trans., 1937).

22. According to the American Heritage Dictionary, a "metaphor" is "[o]ne thing conceived as representing another; a symbol." THE AMERICAN HERITAGE DICTIONARY 1104 (4th ed. 2000). An "analogy" is a more direct similarity between things: "Similarity in some respects between things that are otherwise dissimilar." *Id.* at 64.

23. GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY 145-46 (1980).

24. *Id.* at 5.

25. J.M. BALKIN, CULTURAL SOFTWARE: A THEORY OF IDEOLOGY 247 (1998).

understanding by shaping and hence limiting it."[26]

The Big Brother metaphor is definitely effective at capturing certain privacy problems, but not all privacy problems are the same. I argue that the metaphor fails to capture the most important dimension of the database problem: the nature of our relationships with public and private bureaucracy and the effects of these relationships on human dignity and freedom. We live today in a world largely controlled by public and private bureaucracies, affecting our communication, entertainment, health care, employment, education, transportation, and culture. These institutions structure our lives in the modern state, and our freedom is implicated in our relationships to them. Databases alter the way the bureaucratic process makes decisions and judgments affecting our lives; and they exacerbate and transform existing imbalances in power within our relationships with bureaucratic institutions. This is the central dimension of the database privacy problem, and it is best understood with the Kafka metaphor.

As John Dewey aptly said, "a problem well put is half-solved."[27] "The way in which the problem is conceived," Dewey elaborated, "decides what specific suggestions are entertained and which are dismissed; what data are selected and which rejected; it is the criterion for relevancy and irrelevancy of hypotheses and conceptual structures."[28] Understanding the problem in light of the Kafka metaphor reveals systematic deficiencies across the spectrum of privacy law in addressing the special nature of the problem of databases. Further, understanding the problem with the Kafka metaphor reveals significant difficulties in the solutions proposed by the existing discourse on information privacy.

Part II provides a background into the problem of databases. Part III discusses and critiques how the Big Brother metaphor structures how the database problem is currently conceptualized within the emerging discourse of information privacy. Part IV looks more broadly at the implications for privacy law of understanding the problem in terms of the Kafka metaphor.

---

26. *Id.* at 248.

27. JOHN DEWEY, LOGIC: THE THEORY OF INQUIRY 108 (1938).

28. *Id.*

II. THE INFORMATION REVOLUTION

What is the nature and extent of the database privacy problem? Almost all of us are aware that our personal information is being collected and stored by many different entities. Many view this with great concern, although they find it difficult to articulate what the concern entails. This article aims to articulate that concern in a useful way. Before discussing the database problem conceptually, I will provide some background into the current methods of information collection and the existing and potential uses of databases. This Part will chronicle the history of record-keeping and databases in the United States in order to understand the motivating forces behind these practices and shed light on their future development.

The history of record-keeping and databases in the United States reveals some important points that I will highlight at the outset. First, the developments in record-keeping were not orchestrated according to a grand scheme but were largely ad hoc, arising as technology interacted with the demands of the growing public and private bureaucracies. Second, the goals of data collection have often been rather benign—or at least far less malignant than the aims of Big Brother. In fact, personal information has been collected and recorded for a panoply of purposes. The story of record keeping and database production is, in the end, not a story about the progression toward a world ruled by Big Brother or a multitude of Little Brothers. Instead, it is a story about a group of different actors with different purposes attempting to thrive in an increasingly information-based society.

A. *Public Sector Databases*

Although personal records have been kept for centuries,[29] only in contemporary times has the practice become a serious concern. In earlier times, communities were much smaller and people knew each other's business. Personal information was preserved in the memories of friends, family, and neighbors, and spread by gossip and storytelling. Few public records were collected, and most of them were kept at a very local level, often by institutions associated with churches.[30] During the late 19th century, record-keeping by state and local governments became increasingly prevalent.[31]

The federal government's early endeavors at collecting data consisted mainly in its responsibility of conducting the census. The first census in 1790

---

29. For example, in the 11th century, William the Conquerer collected information about his subjects for taxation in the Doomsday Book. REGAN, *supra* note 4, at 69.

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

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

was basically just a head-count, asking only four questions.[32] With each proceeding census, more personal information was collected. In 1830, two personal questions were asked—whether the individual was deaf or blind.[33] By 1860, 142 questions were asked.[34] When the 1890 census included questions about diseases, disabilities, and finances, it sparked a public outcry by the press, leading to the passage in the early twentieth century of stricter laws protecting the confidentiality of census data.[35]

One of the next significant steps in federal personal information record-keeping was the creation of a federal tax system. Tax records, containing financial information, began to be kept during the early twentieth century, and in the 1920s and 1930s, Congress occasionally flirted with requiring the public disclosure of information in these records.[36]

It was not until the middle of the twentieth century that information collection began to flourish. The creation and growth of government bureaucracy—spawning well over 100 federal agencies within the past century—has led to an overwhelming increase in the collection and use of data. The expansion of the bureaucratic network of regulation, licensing, and entitlements in the 1930s, 40s and 50s resulted in an insatiable thirst for information about individuals.[37] One example was the Social Security System, created in 1935, which assigned nine-digit numbers to each citizen and required extensive record-keeping of each employed individual's earnings.[38]

Technology was one of the primary factors in the rise of information collection. The 1880 census required almost 1500 clerks to tally information tediously, by hand—and it took seven years to complete.[39] At the rapid rate of population growth, if a faster way could not be found to tabulate the information, the 1890 census would not be completed before the 1900 census began. Fortunately, just in time for the 1890 census, a census official named

---

32. *See* REGAN, *supra* note 4, at 46.

33. *See* SMITH, *supra* note 30, at 58.

34. *See* REGAN, *supra* note 4, at 46.

35. *See id.* at 47.

36. Congress provided varying protection for the confidentiality of tax records. In 1924, Congress required the public disclosure of taxpayer income, but then repealed the requirement two years later. In 1934, Congress once again required this disclosure—by making taxpayers submit a form called a "pink slip" which contained name, address, gross income, deductions, net income, credit against net income, and tax payable. The law was repealed a year later. ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 10 (1992).

37. *See* WESTIN & BAKER, *supra* note 2, at 220-23. 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).

38. For a general introduction to Social Security numbers, see SOCIAL SECURITY ADMINISTRATION, YOUR NUMBER AND CARD (1999), *available at* http://www.ssa.gov/pubs/10002.html.

39. MARTIN CAMPBELL-KELLY & WILLIAM ASPRAY, COMPUTER: A HISTORY OF THE INFORMATION MACHINE 21 (1996).

Herman Hollerith developed an innovative tabulating device—a machine that read holes punched in cards.[40] With Hollerith's new machine, the 1890 census was tabulated in under three years.[41] Hollerith left the Census Bureau and founded a small firm that developed his punched-card machines—a firm that through a series of mergers eventually formed the company that became IBM.[42]

IBM's subsequent rise to prosperity was due, in significant part, to the government's increasing need for data. The Social Security System and the New Deal programs required a vast increase in records that had to be kept by both the public and private sectors. As a result, the government became one of the largest purchasers of IBM's punching machines.[43] The Social Security Board kept most of its records on punch cards, and by 1943 it had more than 100 million cards in storage.[44]

The advent of the mainframe computer in 1946 revolutionized information collection. The computer and magnetic tape enabled the systematic storage of data. As computer processing speeds accelerated, and as computer memory ballooned, computers provided a vastly increased ability to collect, search, analyze, copy, and transfer records.

Federal and state agencies were among the first to computerize their records. The Census Bureau was one of the earliest purchasers of commercially available computers.[45] Social Security numbers—which originally were not designed to be used as identifiers beyond the social security system[46]—became immensely useful for computer databases. In the 1970s, federal, state, and local governments—as well as the private sector—increasingly began to use them as identifiers.[47]

---

40. SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 17-18 (2000).

41. CAMPBELL-KELLY & ASPRAY, *supra* note 39, at 26.

42. *Id.* at 44-52; GARFINKEL, *supra* note 40, at 18.

43. *See* CAMPBELL-KELLY & ASPRAY, *supra* note 39, at 52.

44. GARFINKEL, *supra* note 40, at 19.

45. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 55 (1971).

46. PHILIPPA STRUM, PRIVACY: THE DEBATE IN THE UNITED STATES SINCE 1945, at 46 (1998).

47. *Id.* at 47. In the 1960s and 1970s, Social Security numbers began to be used for taxpayer identification numbers, motor vehicle registration, drivers' licenses, and identifiers for other programs. CHARLES J. SYKES, THE END OF PRIVACY 52 (1999). In 1984, Congress required all holders of bank accounts to provide their Social Security numbers to their banks so the IRS could better monitor finances. *Id.* A recent study by the United States General Accounting Office documents the current widespread use of Social Security numbers. *See* UNITED STATES GENERAL ACCOUNTING OFFICE, TESTIMONY BEFORE THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY, COMMITTEE ON GOVERNMENT REFORM, HOUSE OF REPRESENTATIVES, GAO/T-HEHS-00-120, SOCIAL SECURITY: GOVERNMENT AND OTHER USES OF THE SOCIAL SECURITY NUMBER ARE WIDESPREAD (May, 2000). For a listing of the increasing authorized uses of Social Security numbers, see GARFINKEL, *supra* note 40, at 33-34.

Today, federal agencies and departments maintain almost 2000 databases,[48] including records pertaining to immigration, bankruptcy, Social Security, military personnel, as well as countless other matters. In a recent effort to track down parents who fail to pay child support, the federal government has created a vast database consisting of information about all people who obtain a new job anywhere in the nation. The database contains their Social Security numbers, addresses, and wages.[49]

States maintain public records of arrests, births, criminal proceedings, marriages, divorces, property ownership, voter registration, workers compensation, and scores of other types of records. State licensing regimes mandate that records be kept on numerous professionals such as doctors, lawyers, engineers, insurance agents, nurses, police, accountants, and teachers.

States are also creating DNA databases about individuals. States have been constructing databases of their felons and placing them on the Internet.[50] Many states maintain sexual offender DNA databases.[51] Some states are in the process of expanding their databases to include the genetic information of a greater range of felons.[52] DNA databases are not merely limited to criminals. The military maintains a DNA database to identify remains of missing soldiers.[53] Recently, Iceland sold a database containing the genetic information of its entire population to a biotechnology company.[54]

B. *Private Sector Databases*

The rise of databases was driven not only by the public sector's expanding regulatory system, but also by the private sector's increasing competition in marketing and advertising.

---

48. *See* BETH GIVENS & THE PRIVACY RIGHTS CLEARINGHOUSE, THE PRIVACY RIGHTS HANDBOOK: HOW TO TAKE CONTROL OF YOUR PERSONAL INFORMATION 116 (1997)

49. *See* Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996). *See generally* Robert O' Harrow, Jr., *Uncle Sam Has All Your Numbers: Huge Net for Deadbeat Dads Catches Privacy Criticism*, WASH. POST, June 27, 1999, at A1 (describing the "vast computerized data-monitoring system" used for child support enforcement).

50. Currently, these databases are used only for identification purposes, and only a very small portion of an individual's DNA is used.

51. Craig Timberg, *Virginia Lists Sex Offenders on Internet*, WASH. POST, Dec. 30, 1998, at A1.

52. *See, e.g.*, Amy Argetsinger & Craig Whitlock, *Md. Seeks the DNA of Violent Criminals: Critics Cite Threat to Privacy Rights*, WASH. POST, Mar. 24, 1999, at B1 (discussing Maryland plan to "collect the genetic fingerprints of almost every violent felon").

53. SYKES, *supra* note 47, at 128.

54. John Schwartz, *For Sale in Iceland: A Nation's Genetic Code: Deal with Research Firm Highlights Conflicting Views of Progress, Privacy and Ethics*, WASH. POST, Jan. 12, 1999, at A1.

Long before the rise of nationwide advertising campaigns there was a personal relationship between merchant and customer. Local merchants lived next door to their customers and learned about their lives from their existence together in the community. To a large extent, marketing was done locally—by the peddler on the street or the shopkeeper on the corner. Mass marketing, which began in the nineteenth century and flourished in the twentieth century, transformed the nature of selling from personal one-to-one persuasion to large-scale advertising campaigns designed for the nameless, faceless American consumer.

Mass marketing consumed vast fortunes, and advertisements captured only a limited percentage of those exposed to them. Soon marketers discovered the power of a new form of marketing—targeted marketing, directed to discrete individuals or groups.

The sales department of General Motors Corporation began one of the early experiments with targeted marketing in the 1920s. Through research, it discovered that owners of Ford vehicles frequently did not purchase a Ford as their next vehicle—so it targeted owners of two-year-old Fords and sent them a brochure on GM vehicles.[55] GM then began to send out questionnaires asking for consumer input into their products. GM believed that this would be a good marketing device, presenting the image of a big corporation that cared enough to listen to the opinions of everyday people.[56] GM cast itself as a democratic institution, its surveys demonstrating that it was "*OF* THE PEOPLE, *FOR* THE PEOPLE, *BY* THE PEOPLE."[57] One GM print advertisement depicted a delighted child holding up the survey letter exclaiming: "Look dad, a letter from General Motors!"[58] The campaign was quite successful—ironically not because of the data collected but because of the impression of GM as a company that was interested in the consumer's opinions and ideas. Despite GM's rhetoric of listening to the consumer, GM's engineers virtually ignored the surveys, claiming that the consumer views were naïve.[59]

Things have come a long way. Today, corporations are desperate for whatever consumer information they can glean, and their quest for such information is hardly perceived by the general public as democratic. The data collected extends beyond information about consumer's views of the product to information about the consumer herself, often including lifestyle details and even a full-scale psychological profile.

The turn to targeting was spurred by the proliferation and specialization of

---

55. Roland Marchand, *Customer Research as Public Relations: General Motors in the 1930s*, *in* GETTING AND SPENDING: EUROPEAN AND AMERICAN CONSUMER SOCIETIES IN THE TWENTIETH CENTURY 85, 86 (Susan Strasser, Charles McGovern, & Matthias Judt eds., 1998).

56. *Id.* at 92.

57. *Id.* at 99.

58. *Id.* at 109.

59. *See id.* at 105.

mass media throughout the century,[60] enabling marketers to tap into groups of consumers with similar interests and tastes. Selecting particular television or radio shows or specific magazines to place advertisements was the most basic form of targeting. This technique, however, was only a variation of mass marketing.

The most revolutionary developments in targeted marketing occurred in the direct marketing industry, consisting originally of companies that contacted consumers directly through the mail (often by mail order catalogs). The practice of sending catalogs directly to consumers began in the late nineteenth century when railroads extended the reach of the mail system.[61] The industry also reached out to people by way of door-to-door salespersons. In the 1970s, marketers began calling people directly on the telephone, and "telemarketing" was born.

Direct marketing remained a fledgling practice and fringe form of marketing for most of the century.[62] Direct marketers had long accepted the "two percent" rule—only two percent of those contacted would respond.[63] With such a staggering failure rate, direct marketing achieved its successes at great cost. To increase the low response rate, marketers sought to sharpen their targeting techniques. This required more consumer research and an effective way to collect, store, and analyze information about consumers. The advent of the computer database gave marketers this long sought after ability—and it launched a revolution in targeting technology.

Databases provided an efficient way to store and search for data. Organized into fields of information, the database enabled marketers to sort by various types of information and to rank or select various groups of individuals from its master list of customers—a practice called "modeling."[64] Through this process, fewer mailings or calls needed to be made, resulting in a higher response rate and lower costs.[65] In addition to isolating a company's most profitable customers, marketers studied them, profiled them, and then used that profile to hunt for similar customers.[66] This, of course, demanded not only information about existing customers, but the collection of data about prospective customers as well.

---

60. In 1950, for example, there were 700 radio stations. In 1984, there were 9000. CHESTER A. SWENSON, SELLING TO A SEGMENTED MARKET: THE LIFESTYLE APPROACH xvi (1990). In 1989, there were 2192 consumer magazines and 5000 business publications. *Id.*

61. ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER: SECOND-GENERATION STRATEGIES AND TECHNIQUES FOR TAPPING THE POWER OF YOUR CUSTOMER DATABASE 51 (2d ed. 1996).

62. *Id.* ("But for most of the twentieth century, catalog marketing was always considered a backwater, an aberration, an obscure method for unloading second-class goods on rural people.").

63. *Id.* at 57.

64. *See id.* at 278-88.

65. *See id.* at 285.

66. *See id.* at 267-68.

Originally, marketers sought to locate the best customers by identifying those customers who purchased items most recently, who had the most frequent number of purchases, and who spent the most money.[67] In 1967 when the postal system began using the five-digit zip code, direct marketers began to isolate responses by zip code to determine the best areas to market to.[68] Direct marketers could then send mailings to those zip codes with the greatest response rates. This information, however, was based merely on a company's own sales data.

The turn to demographic information in the 1970s[69] enabled marketers to profile potential consumers. Demographics included basic information such as age level, income level, race, ethnicity, gender, and geographical location. Marketers could target certain demographic segments of the nation, a practice called "cluster marketing." It worked because people with similar incomes and races generally lived together in clusters.

The private sector obtained this demographic information from the federal government. By the 1970s, the United States had begun selling its census data on magnetic tapes.[70] To protect privacy, the Census Bureau sold the information on computer tapes in clusters of 1500 households, supplying only addresses—not names.[71] This privacy protection measure was thwarted when companies such as Donnelley, MetroMail, and R.L. Polk reattached the names by matching the addresses with information in telephone books and voter registration lists.[72] Within five years of purchasing the census data, these companies had constructed demographically segmented databases of over half of the households in the nation.[73]

In the 1980s, marketers looked to supplement their data about consumers by compiling "psychographic" information—data about psychological characteristics such as opinions, attitudes, beliefs, and lifestyle.[74] In the vanguard of collecting psychographic data were clustering companies that had previously relied upon more basic demographic data. For example, one company established an elaborate taxonomy of people, with category names such as "Blue Blood Estates," "Bohemian Mix," "Young Literati," "Shotguns and Pickups," and "Hispanic Mix."[75] For each cluster, there is a description of

---

67. *See id*. at 156.

68. DICK SHAVER, THE NEXT STEP IN DATABASE MARKETING: CONSUMER GUIDED MARKETING®: PRIVACY TO YOUR CUSTOMERS, RECORD PROFITS FOR YOU 27 (1996).

69. CLIFF ALLEN, DEBORAH KANIA, & BETH YAECKEL, INTERNET WORLD GUIDE TO ONE-TO-ONE WEB MARKETING: BUILD A RELATIONSHIP MARKETING STRATEGY ONE CUSTOMER AT A TIME 3 (1998).

70. LARSON, *supra* note 36, at 41; SHAVER, *supra* note 68, at 29.

71. SHAVER, *supra* note 68, at 29-32.

72. *Id*. at 32.

73. *Id*.

74. *See* ALLEN, KANIA & YAECKEL, *supra* note 69, at 3; HUGHES, *supra* note 61, at 295.

75. HUGHES, *supra* note 61, at 298-99.

the type of person, their likes, incomes, race and ethnicity, attitudes, and hobbies.[76]

These innovations in targeting technique have made targeted marketing—or "database marketing" as it is often referred to today—the hottest form of marketing, growing at twice the rate of America's gross national product.[77] In 1995, direct marketing resulted in $600 billion in sales. The industry employed over eighteen million people.[78] On average, over 500 pieces of unsolicited advertisements, catalogs, and marketing mailings arrive every year at each household.[79] Due to targeting, direct mail yields $10 in sales for every $1 in cost—a ratio double that for a television advertisement—and forecasters predict catalog sales will grow faster than retail sales.[80] Telemarketing is a $435 billion dollar a year industry.[81] In a 1996 Gallup poll, 77 percent of United States companies used some form of direct mail, targeted email, or telemarketing.[82]

The effectiveness and profitability of targeted marketing depend upon data, and the challenge is to obtain as much of it as possible. Marketers discovered that they did not have to research and collect all the information from scratch, for data is the perspiration of the Information Age. Billions of bytes are released each second as we click, charge, and call. A treasure trove of information already lay untapped within existing databases, retail records, mailing lists, and government records. All that marketers had to do was plunder it as secretly and efficiently as possible.

The increasing thirst for personal information spawned the creation of a new industry: the database industry. The database industry is an information age bazaar where personal data collections are bartered and sold. List rental prices are calculated at a few cents to a dollar per name.[83] Over 550 companies comprise the personal information industry, with annual revenues in the billions of dollars.[84] The sale of mailing lists alone (not including the sales

---

76. *See id*. at 300.

77. *Id*. at 5.

78. William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 Fordham L. Rev. 951, 956 (1996).

79. Susan Headden, *The Junk Mail Deluge*, U.S. NEWS & WORLD REP., Dec. 8, 1997, at 40. Junk mail sent to each home averages about thirty four pounds per year. *Id*. *See also* GIVENS, *supra* note 48, at 16.

80. Headden, *supra* note 79.

81. ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS, 31 (1994).

82. BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD 7 (Mar. 1997).

83. There are no precise figures, but most sources quote between three cents to one dollar per name. *See* HUGHES, *supra* note 61, at 365 (twenty cents to one dollar per name); Headden, *supra* note 79, (three to twenty cents per name).

84. Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1162 (1997).

generated by the use of the lists) generates three billion dollars a year.[85] The average consumer is on around 100 mailing lists and is contained in at least fifty databases.[86]

An increasing number of companies with databases—magazines, credit card companies, stores, mail order catalog firms, and even telephone companies—are realizing that their databases are becoming one of their most valuable assets and are beginning to sell their data.

Along with companies whose databases were an outgrowth of their business, a new breed of firms devotes their primary business to the collection of personal information. Catalina Marketing Corporation, for example, maintains supermarket buying history databases on 30 million households from more than 5000 stores.[87] Aristotle Industries, Inc. markets a database of the names, addresses, and voting records of 118 million of America's 128 million registered voters.[88]

The most powerful database builders construct information empires, sometimes with information on more than half of the American population. For example, Donnelly Marketing Information Services keeps track of 125 million people.[89] Wiland Services has constructed a database containing over 1000 elements, from demographic information to behavioral data, on over 215 million people.[90] There are around five database compilers that have data on almost all households in the United States.[91]

In addition to marketing databases, credit card companies and credit reporting agencies have also developed extensive personal information databases. The use of general purpose credit cards greatly expanded during the 1970s and 1980s,[92] creating a detailed record of one's purchases and lifestyle.

The increasing mobility of people and the fact that creditors no longer knew one's reputation in the community spawned the need for national credit reporting firms.[93] Credit reporting companies evaluate people's credit, rate each person, and sell this information to creditors. For example, Experian, one of the largest credit reporting companies in the world,[94] collects credit information on 205 million Americans.[95] Credit reports contain financial

85. Fenrich, *supra* note 78, at 956.

86. BRANSCOMB, *supra* note 81, at 11.

87. Robert O'Harrow, Jr., *Behind the Instant Coupons, a Data-Crunching Powerhouse*, WASH. POST, Dec. 31, 1998, at A20.

88. LARSON, *supra* note 36, at 218.

89. *Id.* at 60.

90. *Id.*

91. HUGHES, *supra* note 61, at 354.

92. STRUM, *supra* note 46, at 72-73.

93. SMITH, *supra* note 30, at 314.

94. There are three large credit reporting companies in the United States: Equifax, Experian (formerly TRW), and Trans Union.

95. *See* EXPERIAN FACT SHEET, *at* http://www.experian.com/corporate/factsheet.html

information contained in public records such as bankruptcy filings, judgments and liens, as well as information relating to mortgage foreclosures, checking accounts, and a list of all companies that requested the individual's credit file.[96] Some companies also prepare investigative consumer reports, which supplement the credit report with information about an individual's character and lifestyle.[97] Credit reporting companies provide lists of people at certain income levels with good credit,[98] which are then used to send people pre-approved credit card offers.[99]

In addition to credit card records, there are cable television records, video rental records, phone records, travel records, and so on. The Medical Information Bureau (MIB), a nonprofit institution, maintains a database of medical information on fifteen million individuals, which is available to over 700 insurance companies.[100]

C. *Cyberspace and Personal Information*

Cyberspace is the new frontier for marketing, and its power has only begun to be exploited. The Internet is rapidly becoming the hub of the personal information market. First, the Internet provides a much greater ability to aggregate and consolidate information. Government agencies have begun to place records on their websites, and public records, once physically scattered across the country, can now be searched or gathered from anywhere in the country. A group of Internet websites have compiled public records from across the country and sell the information online. Companies such as KnowX.com and Locateme.com sell records pertaining to aircraft ownership, bankruptcy, death, registered pilots, judgments, liens, lawsuits, professional licenses, residences, real property foreclosures, property refinancing, driver registrations, voter registrations, and credit headers.[101]

Second, the Internet has made the peddling and purchasing of data much easier. Acxiom.com is a website that collects and sells data on consumers.[102] In its "InfoBase," it provides "[o]ver 50 demographic variables . . . including age, income, real property data, children's data, and others." It contains data on education levels, occupation, height, weight, political affiliation, ethnicity,

---

(last visited Apr. 12, 2001).

96. See http://www.econsumer.Equifax.com/webapp/ConsumerProducts/pgOnlineSample.jsp for a sample credit report. (last visited Apr. 12, 2001).

97. *See* GIVENS, *supra* note 48, at 83.

98. LARSON, *supra* note 36, at 76.

99. GIVENS, *supra* note 48, at 21.

100. *See, e.g.,* GARFINKEL, *supra* note 40, at 137; GIVENS, *supra* note 48, at 83 (discussing investigative consumer reports).

101. *See* http://www.knowx.com (last visited Mar. 11, 2001); http://www.locateme.com (last visited Mar. 11, 2001).

102. http://www.acxiom.com (last visited Mar. 11, 2001).

race, hobbies, and net worth. Focus USA's website boasts that it has detailed information on 203 million people.[103] Among its over 100 targeted mailing lists are lists of "Affluent Hispanics," "Big-Spending Parents," "First Time Credit Card Holders," "Grown But Still At Home," "Hi-Tech Seniors," "New Homeowners," "Status Spenders," and "Waist Watchers."[104]

In addition to serving as a marketplace for personal information, cyberspace has provided a revolution for the targeted marketing industry, through profound targeting capabilities and effective methods for collecting personal information. Advertisers spend millions of dollars on Internet advertising. Internet ad spending was approximately $301 million in 1996,[105] and it leaped to about $1.9 billion in 1998.[106] That figure rose to around $4 billion in 1999.[107] Over fifty percent of the Fortune 500 companies have paid for advertisements on the Internet.[108]

The Internet provides much greater targeting capabilities for advertisers. As one book for web advertisers boasts: "The targeting that magazines give you over television is nothing compared to the targeting the Web gives you over magazines."[109] This revolution in targeting technology is possible because web pages are not static like magazine pages. They are generated every time the user clicks. Each page contains spaces reserved for advertisements and specific advertisements are download into those spots.[110] The dynamic nature of web pages makes it possible for a page to download different advertisements for different users.

Targeting is very important for web advertising because a web page is cluttered with information and images all vying for the users' attention. Whereas a television commercial is an orderly linear presentation of details, the web page places everything before the user at once. Similar to the response rates of earlier efforts at direct marketing, only a small percentage of viewers (from 2%-3.5%) click the advertisements they view.[111] The Internet's greater targeting potential and the fierce competition for the consumer's attention have given companies an unquenchable thirst for information about web users. This information is useful in developing more targeted advertising as well as in enabling companies to better assess the performance and popularity of various

---

103. http://www.focus-usa-1.com/lists_az.htm

104. *Id*.

105. *See* JIM STERNE, WHAT MAKES PEOPLE CLICK: ADVERTISING ON THE WEB 21 (1997).

106. Greg Farrell, *Advertising on Internet Zooms: Industry Leaders See Web Snaring Target Market at Low Cost*, USA TODAY, May 10, 1999, at B9.

107. John Markoff, *Sizing Up the Web*, N.Y. TIMES, Dec. 11, 2000, at C4 (graphic accompanying article *Coming to Grips with the Web: Fast Changing Genie Alters the World)*.

108. STERNE, *supra* note 105, at 14.

109. *Id*. at 37.

110. *See id*. at 69.

111. *See id*. at 179.

parts of their web sites.

Currently, there are two basic ways personal information is collected in cyberspace: (1) by directly collecting information from users (registration and transactional data); and (2) by surreptitiously tracking the way people navigate through the Internet (clickstream data).

The direct solicitation of information is widespread. Websites collect both registration and transactional data. Registration data is collected by those websites that request users to log in to access parts of the website. Transactional data is gleaned by websites engaging in business with users, such as selling merchandise or services. For example, Amazon.com, one of the largest Internet merchants, keeps track of its customers' purchases in books, CDs, electronics, toys, and other items.

Websites can also secretly track a customer's websurfing. When a person explores a website, the website can record the Internet service provider, the type of computer and software used, the website linked from, the amount of time spent perusing each page, and exactly what parts of the website were explored and for how long. This information is referred to as "clickstream data" because it is a trail of how a user navigates throughout the web by clicking on various links. It enables the website to calculate how many times it has been visited and what parts are most popular. With a way to connect this information to particular web users, marketers can gain a window into people's minds. This is a unique vision, for while marketers can measure the size of audiences for other media such as television, radio, books, and magazines, they have little ability to measure attention span. Due to the interactive nature of the Internet, marketers can learn how we respond to what we hear and see. A website collects information about the way a user interacts with the site and stores the information in its database. This information will enable the website to learn about the interests of a user so it can better target advertisements to the user. For example, Amazon.com could, if it desired, keep track of every book or item that a customer browsed but did not purchase.

To connect this information with particular users, a company can either require a user to log in or it can secretly tag a user so that it recognizes the user when she returns. This latter form of identification occurs through what is called a "cookie."[112] A cookie is a small text file of codes that is deployed into the user's computer when she downloads a web page. Web sites place a unique identification code into the cookie, and the cookie is saved on the user's hard drive. When the user visits the site again, the site looks for its cookie, recognizes the user, and locates the information it collected about the user's previous surfing activity in its database. Basically, a cookie works as a form of high-tech cattle-branding.

---

112. Cookies are not used only for tracking or targeting purposes. Cookies also have beneficial uses, such as storing passwords and identifying returning customers so they do not have to reenter information.

Cookies have certain limits. First, they are not tagged to particular individuals—just to particular computers. Second, websites can only read the cookies that they placed on a user's computer; they cannot obtain cookies stored by a different website.

Although cookies alone do not supply much information, companies have devised strategies of information sharing with other websites. One of the most popular information sharing techniques is performed by a firm called DoubleClick. Companies pay DoubleClick to distribute their advertisements. When a user clicks a company's advertisement banner, a secret message is deployed to DoubleClick before the web page associated with the banner is downloaded. The messages sent to DoubleClick enable it to keep track of which ads are being clicked and by whom.[113] Once DoubleClick develops a profile of a user, it can scan through its subscribing companies' advertisements and match them to the user based on the information it has gathered.[114] As of the end of 1999, DoubleClick had amassed eighty million customer profiles.[115]

"The time will come," predicts one marketer, "when we are well known for our inclinations, our predilections, our proclivities, and our wants. We will be classified, profiled, categorized, and our every click will be watched."[116] As we stand at the threshold of an age structured around information, we are only beginning to realize the extent to which our lives can be encompassed within its architecture. As we live more of our lives on the Internet, we are also creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived. One company has even been systematically sweeping up all the data from the Internet and storing it in a vast electronic warehouse.[117] Our online personas—captured, for instance, in our web pages and usenet postings—are swept up as well. We are accustomed to information on the web quickly flickering in and out of existence, presenting the illusion that it is ephemeral. But little on the Internet disappears or is forgotten, even when we delete or change the information. The amount of personal information archived will only escalate as our lives are increasingly

---

113. STERNE, *supra* note 1085, at 238.

114. *Id.* at 241.

115. Heather Green, *Privacy Online: The FTC Must Act Now*, BUS. WK.,, Nov. 29, 1999, at 48. DoubleClick's activities have come under increasing scrutiny. In 1999, DoubleClick purchased Abacus Direct Corp., a direct marketing company maintaining a database on about ninety percent of United States households. In re DoubleClick, Inc. Privacy Litigation, No. 00 CIV 0641 NRB, 2001 WL 303744, at *5 (S.D.N.Y. Mar. 29, 2001). To address the possibility that DoubleClick might merge its profiles with Abacus's database, the Federal Trade Commission (FTC) initiated an investigation. *Id.* at *5-6. In 2000, DoubleClick announced that it was temporarily backing away from its plan to merge the data, and in January, 2001, the FTC ended its investigation. *Id.* at *6. Recently, a federal district court dismissed a class action against DoubleClick alleging, among other things, that DoubleClick's use of cookies violated the Federal Wiretap Act. *Id.* at *1.

116. STERNE, *supra* note 105, at 255.

117. J.D. Lasica, *The Net NEVER Forgets*, SALON, Nov. 25, 1998, *at* http://www.salon.com /21st/feature /1998/11/25feature.html.

digitized into the electric world of cyberspace.

These developments certainly suggest a threat to privacy, but what specifically is the problem? As the remainder of this Article will show, the way this question is answered has profound implications for the way the law will grapple with the problem in the future.

III. RETHINKING INFORMATION PRIVACY

The most widely discussed metaphor in the discourse of information privacy[118] is George Orwell's depiction of Big Brother in *Nineteen Eighty-Four*. Courts and commentators have consistently turned to this metaphor when discussing a host of other privacy problems, and it has proven quite useful for understanding the threat to privacy caused by government searches and seizures and other law enforcement actions.[119] It is no surprise, then, that the burgeoning discourse on information privacy has seized upon this metaphor.

However, not all privacy problems are the same, and not all problems can be understood in their full depth and complexity with the same metaphor. The problem of databases is relatively new. Although it has slowly brewed during the twentieth century, the problem has only begun to boil in the past thirty to forty years. Discussion of the problem by legal academics began only in the mid 1960s and early 1970s as the public and private sectors began to computerize their records.[120]

In this Part, I explain why the Big Brother metaphor does not adequately conceptualize the database problem and propose an alternative metaphor (Kafka's *The Trial*) to understand the problem more completely.

A. *The Big Brother Metaphor*

George Orwell's depiction of Big Brother in *Nineteen Eighty-Four* is so commonly known that a short description will suffice. Big Brother is an all-knowing, constantly vigilant government that regulates every aspect of one's existence—even one's private thoughts. In every corner are posters of an enormous face, with "eyes [that] follow you about when you move" and the

---

118. "Information privacy" is the term theorists use to discuss the privacy implications of the collection, use, and disclosure of personal information. Information privacy is often contrasted with "decisional privacy" which involves the extent to which the state can interfere with the decisions one makes with regard to one's body and family. Decisional privacy involves matters such as contraception, procreation, abortion, and child rearing.

119. *See* notes 3-16 *supra* and accompanying text.

120. *See* MILLER, *supra* note 45; ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); WESTIN & BAKER, *supra* note 2; Kenneth L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342 (1966).

caption "BIG BROTHER IS WATCHING YOU."[121]

Big Brother demands complete obedience from its citizens and controls all aspects of their lives. It constructs the language, rewrites the history, purges its critics, indoctrinates the population, burns books, and obliterates all disagreeable relics from the past. Big Brother's goal is uniformity and complete discipline, and it attempts to police people to an unrelenting degree—even their innermost thoughts. Any trace of individualism is quickly suffocated.

This terrifying totalitarian state achieves its control by targeting the private life, employing various techniques of power to eliminate any sense of privacy. Big Brother views solitude as dangerous.[122] Its techniques of power are predominantly methods of surveillance. Big Brother is constantly monitoring and spying; uniformed patrols linger on street corners; helicopters hover in the skies, poised to peer into windows. The primary surveillance tool is a device called a "telescreen" which is installed into each house and apartment. The telescreen is a bilateral television—individuals can watch it, but it also enables Big Brother to watch them:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. . . . You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[123]

Citizens have no way of discovering if and when they are being watched. This surveillance both real and threatened is combined with swift and terrifying force and violence: "People simply disappeared, always during the night. Your name was removed from the registers, every record of everything you had ever done was wiped out, your one-time existence was denied and then forgotten."[124]

Orwell's Big Brother narrative brilliantly captures the horror of the world it depicts, and its images continue to be invoked in the legal discourse of privacy and information. "The ultimate horror in Orwell's imagined anti-utopia," observes Dennis Wrong, "is that men are deprived of the very capacity for cherishing private thoughts and feelings opposed to the regime, let alone acting on them."[125]

The telescreen functions similarly to the Panopticon, an architectural design for a prison, originally conceived by Jeremy Bentham in 1791.[126] In

---

121. ORWELL, *supra* note 6, at 3.

122. *See id.* at 70.

123. *Id.* at 4.

124. *Id.* at 20.

125. DENNIS H. WRONG, POWER: ITS FORMS, BASES AND USES 115 (1979).

126. DAVID LYON, THE ELECTRONIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 62 (1994).

Discipline and Punish, Michel Foucault provides a compelling description of this artifice of power:

> [A]t the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building . . . . All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible.[127]

The Panopticon is a device of discipline; its goal is to ensure order, to prevent plots and riots, to mandate total obedience. The Panopticon achieves its power through an ingenious technique of surveillance, one that is ruthlessly efficient. By setting up a central observation tower from which all prisoners can be observed and by concealing from them any indication of whether they are being watched at any given time, "surveillance is permanent in its effects, even if it is discontinuous in its action."[128] Instead of having hundreds of patrols and watchpersons, only a few people need to be in the tower. Those in the tower can watch any inmate but they cannot be seen. By always being visible, by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control. The Panopticon is so efficient that nobody needs to be in the tower at all.

As Foucault observed, the Panopticon is not merely limited to the prison or to a specific architectural structure—it is a technology of power that can be used in many contexts and in a multitude of ways.[129] In *Nineteen Eighty-Four*, the telescreen works in a similar way to the Panopticon, serving as a form of one-way surveillance that structures the behavior of those that are observed. The collection of information in cyberspace can be readily analogized to the telescreen. As we surf the Internet, information about us is being collected; we are being watched, but we do not know when or to what extent.

The metaphor of Big Brother understands privacy in terms of power, and it views privacy as an essential dimension of the political structure of society. The metaphor properly understands the problem of databases and privacy as concerning the very architecture of freedom and democracy—not merely individual reputations, feelings, and interests. Big Brother attempts to dominate the private life because it is the key to controlling an individual's

---

127. MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., Pantheon Books, 1st American ed. 1977).

128. *Id.* at 201.

129. *Id.* at 205.

entire existence: her thoughts, ideas, and actions.

Big Brother currently dominates the entire discourse of information privacy.[130] As one state supreme court justice observed:

> Our nation's current social developments harbor insidious evolutionary forces which propel us toward a collective, Orwellian society. . . . Government agencies . . . have acquired miles and acres of files, enclosing revelations of the personal affairs and conditions of millions of private individuals. Credit agencies and other business enterprises assemble similar collections.[131]

Paul Schwartz compares Internet "surveillance" to Orwell's telescreen, concluding that cyber-surveillance is even more insidious. While the telescreen lacked any capacity to store data, the "Internet creates digital surveillance with nearly limitless data storage possibilities and efficient search possibilities."[132] Further, instead of one Big Brother, today there are a "myriad" of "Big and Little Brothers" collecting personal data and "information technology has greatly encouraged the sharing of personal data between government and business."[133]

Even when not directly invoking the metaphor, commentators frequently speak in its language, evoke its images and symbols, and define privacy problems in similar conceptual terms. Commentators view databases as having many of the same purposes (social control, suppression of individuality) and employing many of the same techniques (surveillance and monitoring) as Big Brother. David Flaherty explains that the "storage of personal data can be used to limit opportunity and to encourage conformity."[134] He elaborates: "The existence of dossiers containing personal information collected over a long period of time can have a limiting effect on behavior; knowing that participation in an ordinary political activity may lead to surveillance can have a chilling effect on the conduct of a particular individual."[135]

In *Information Privacy in Cyberspace Transactions*, Jerry Kang observes:

> [D]ata collection in cyberspace produces data that are detailed, computer-processable, indexed to the individual, and permanent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper than in real space, and we have what Roger Clarke has identified as the genuine threat of "dataveillance."[136]

"Dataveillance," a term coined by Roger Clarke, refers to the "systematic use of personal data systems in the investigation or monitoring of the actions or

---

130. *See* notes 2-16 *supra* and accompanying text.

131. White v. California, 95 Cal. Rptr. 175, 181 (Cal. Ct. App. 1971) (1971) (Friedman, J., concurring in part and dissenting in part).

132. Schwartz, *supra* note 14, at 1657 n.294.

133. *Id*.

134. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 9 (1989).

135. *Id*.

136. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1261 (1998).

communications of one or more persons."[137] According to Colin Bennet, "[t]he term *dataveillance* has been coined to describe the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated."[138] Dataveillance is thus a new form of surveillance, a method of watching not through the eye or the camera, but by collecting facts and data. Drawing from Stanley Benn, Kang argues that surveillance is an attack on human dignity, interfering with free choice because observation "brings one to a new consciousness of oneself, as something seen through another's eyes."[139] Kang claims that "surveillance leads to self-censorship."[140] Likewise, Paul Schwartz claims that data collection "creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience."[141] According to this view, the problem with databases is that they are a form of surveillance that curtails individual freedom.

Despite the fact that the discourse appropriately conceptualizes privacy through metaphor and that the Big Brother metaphor has proven quite useful for a number of privacy problems, the metaphor has significant limitations for the database privacy problem. The metaphor depicts a particular technique of power—surveillance. Certainly, monitoring is an aspect of information collection, and databases may eventually be used in ways that resemble the disciplinary regime of Big Brother. However, most of the existing practices associated with databases are quite different in character. Direct marketers wish to observe behavior so they can tailor goods and advertisements to individual differences. True, they desire consumers to act in a certain way (to purchase their product), but their limited attempts at control are far from the repressive regime of total control exercised by Big Brother. The goal of much data collection by marketers aims not at suppressing individuality but at studying it and exploiting it.

The most insidious aspect of the surveillance of Big Brother is missing in the context of databases: human judgment about the activities being observed (or the fear of that judgment). Surveillance leads to conformity, inhibition, and self-censorship in situations where it is likely to involve human judgment.

---

137. Roger Clarke, *Information Technology and Dataveillance*, Nov. 1987 at 3, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html; *see also* Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, Sept. 16, 1999, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

138. Colin J. Bennet, *The Public Surveillance of Personal Data: A Cross-National Analysis*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 237 (David Lyon & Elia Zureik eds., 1996).

139. Kang, *supra* note 136, at 1260 (quoting Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 227 (Ferdinand David Schoeman ed., 1984).

140. *Id.* at 1260.

141. Schwartz, *Privacy and Participation*, *supra* note 11, at 560.

Being observed by an insect on the wall is not invasive for privacy; rather, privacy is threatened by being subject to *human* observation, which involves judgments that can affect one's life and reputation. Since marketers generally are interested in aggregate data, they do not care about snooping into particular people's private lives. Much personal information is amassed and processed by computers; we are being watched not by other humans, but by machines, which gather information, compute profiles, and generate lists for mailing, emailing, or calling. This impersonality makes the surveillance less invasive.

While having one's actions monitored by computers does not involve immediate perception by a human consciousness, it still exposes people to the possibility of future review and disclosure. In the context of databases, however, this possibility is remote. Even when such data is used for marketing, marketers merely want to make a profit, not uproot a life or soil a reputation.

I do not, however, mean to discount the dangerous effects of surveillance through the use of databases. Although the purposes of the users of personal data are generally not malignant, databases can still result in unintended harmful social effects. The mere knowledge that one's behavior is being monitored and recorded certainly can lead to self-censorship and inhibition. Foucault's analysis of surveillance points to a more subtle yet more pervasive effect: surveillance changes the entire landscape in which people act, leading toward an internalization of social norms that soon is not even perceived as repressive.[142] This view of the effects of surveillance raises important questions regarding the amount of normalization that is desirable in society. While our instincts may be to view all normalization as an insidious force, most theories of the good depend upon a significant degree of normalization to hold society together.

Although the effects of surveillance are certainly a part of the database problem, the heavy focus on surveillance miscomprehends the most central and pernicious effects of databases. Understanding the problem as surveillance fails to account for the majority of our activities in the world and web. A large portion of our personal information involves facts that we are not embarrassed about: our financial information, race, marital status, hobbies, occupation, and the like. Most people surf the web without wandering into its dark corners. The vast majority of the information collected about us concerns relatively innocuous details. The surveillance model does not explain why the recording of this non-taboo information poses a problem. The focus of the surveillance model is on the fringes — and often involves behaviors we may indeed want to inhibit such as cult activity, terrorism, and child pornography.

As I will illustrate in the next section, there is a serious problem caused by databases which is overlooked by the Big Brother metaphor, one that poses a threat not just to the freedom to explore the taboo, but to freedom in general. It is a problem that implicates the type of society we are becoming, the way we

142. FOUCAULT, *supra* note 127, at 217.

think, our place in the larger social order, and our ability to exercise meaningful control over our lives.

B. *An Alternative Metaphor: Kafka's* The Trial

Ascribing metaphors is not only a descriptive endeavor but also an act of political theorizing with profound normative implications. According to Richard Posner, however, "it is a mistake to try to mine works of literature for political or economic significance"[143] because works of literature are better treated as aesthetic works rather than "as works of moral or political philosophy."[144] To the contrary, literature supplies the metaphors by which we conceptualize certain problems, and Posner fails to acknowledge the role that metaphor plays in shaping our collective understanding. Metaphors function not to render a precise descriptive representation of the problem; rather, they capture our fears and concerns over privacy in a way that is palpable, potent, and compelling. Metaphors are instructive not for their realism but for the way they direct our focus to certain social and political phenomena.

Certainly, metaphors must have a certain fit to the experiences they structure, for metaphors are tools of understanding, and understanding is not an unfettered exercise but one involving interaction with what we experience. However, metaphors are never an exact fit; they are not identical to what they depict; and much philosophical discourse concerns which metaphors we use. As the understanding of experience is not a once-and-done activity but an ongoing process, we are in constant search for new metaphors to better comprehend our situation. Although we cannot arbitrarily cast out old metaphors and adopt new ones, we certainly can exercise control over the metaphors we use.

Franz Kafka's harrowing depiction of bureaucracy in *The Trial* is the most appropriate metaphor to capture the problem with databases. *The Trial* opens with the protagonist, Joseph K., awakening one morning to find a group of officials in his apartment, who inform him that he is under arrest. K. is bewildered at why he has been placed under arrest: "I cannot recall the slightest

---

143. Richard A. Posner, *Orwell Versus Huxley: Economics, Technology, Privacy, and Satire,* 24 PHILOSOPHY AND LITERATURE 1-2 (2000), *available at* http://papers.ssrn.com/paper.taf?abstract_id=194572.

144. *Id*. at 31. Specifically, Posner argues that *Nineteen Eighty-Four* as well as *Brave New World* do not provide much insight about privacy in the modern world. *See id*. at 2. Although Posner recognizes that the "telescreen is a powerful metaphor for the loss of privacy in a totalitarian state," *id*. at 19, he argues that Huxley was more accurate in predicting today's technology than Orwell. *See id*. at 35. However, despite its extreme portrait of a totalitarian society (so extreme that it at times resembles a caricature), the Big Brother metaphor has been indispensable to discussions about the Fourth Amendment and privacy in the law enforcement context. The Big Brother metaphor is important to the discourse because one of the central questions concerning privacy is what type of society we want to construct, and the metaphor speaks directly to this question.

offense that might be charged against me. But even that is of minor importance, the real question is, who accuses me? What authority is conducting these proceedings?"[145] When he asks why the officials have come to arrest him, an official replies: "You are under arrest, certainly, more than that I do not know."[146] Instead of taking him away to a police station, the officials mysteriously leave.

Throughout the rest of the novel, Joseph K. begins a frustrating quest to discover why he has been arrested and how his case will be resolved. A vast bureaucratic court has apparently scrutinized his life and assembled a dossier on him. The Court is clandestine and mysterious, and court records are "inaccessible to the accused."[147] In an effort to learn about this Court and the proceedings against him, Joseph K. scuttles throughout the city, encountering a maze of lawyers, priests, and others, each revealing small scraps of knowledge into the workings of the Court. In a pivotal scene, Joseph K. meets a painter who gleaned much knowledge of the obscure workings of the Court while painting judicial portraits. The painter explains to K.:

> "The whole dossier continues to circulate, as the regular official routine demands, passing on to the highest Courts, being referred to the lower ones again, and then swinging backwards and forwards with greater or smaller oscillations, longer or shorter delays . . . . No document is ever lost, the Court never forgets anything. One day—quite unexpectedly—some Judge will take up the documents and look at them attentively . . . ." "And the case begins all over again?" asked K. almost incredulously. "Certainly" said the painter.[148]

Ironically, after the initial arrest, it is Joseph K. who takes the initiative in seeking out the Court. He is informed of an interrogation on Sunday, but only if he has no objection to it: "Nevertheless he was hurrying fast, so as if possible to arrive by nine o'clock, although he had not even been required to appear at any specific time."[149] Although the Court has barely imposed any authority, not even specifying when Joseph K. should arrive for his interrogation, he acts as if this Court operates with strict rules and makes every attempt to obey. After the interrogation, the Court seems to forget all about K. Joseph K., however, becomes obsessed with his case. He wants to be recognized by the Court and to resolve his case; in fact, being ignored by the Court becomes a worse torment than being arrested.

As K. continues his search, he becomes increasingly perplexed at this unusual Court. The higher officials keep themselves hidden; the lawyers claim they have connections to Court officials but never offer any proof or results. Hardly anyone seems to have direct contact with the Court. In addition, its "proceedings were not only kept secret from the general public, but from the

---

145. KAFKA, *supra* note 21, at 16.
146. *Id.* at 17.
147. *Id.* at 146.
148. *Id.* at 199.
149. *Id.* at 42-43.

accused as well."[150] Yet K. continues to seek an acquittal from a crime he hasn't been informed of and from an authority he cannot seem to find. As Joseph K. scurries through the bureaucratic labyrinth of the law, he can never make any progress toward his acquittal: "Progress had always been made, but the nature of the progress could never be divulged. The Advocate was always working away at the first plea, but it had never reached a conclusion. . . ."[151] In the end, Joseph K. is seized by two officials in the middle of the night and executed.

Kafka's *The Trial* best captures the scope, nature, and effects of the type of power relationship created by databases. My point is not that *The Trial* presents a more realistic descriptive account of the database problem than Big Brother. Like *Nineteen Eighty-Four*, *The Trial* presents a fictional portrait of a harrowing world, often exaggerating certain elements of society in a way that makes them humorous and absurd. Certainly, most people are not told that they are inexplicably under arrest and they do not expect to be executed unexpectedly one evening. *The Trial* is in part a satire, and what is important for the purposes of my argument are the insights the novel provides about society through its exaggerations. In the context of computer databases, Kafka's *The Trial* is the better focal point for the discourse than Big Brother. Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process. This lack of control allows the trial to completely take over Joseph K.'s life. *The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process.

As understood in light of the Kafka metaphor, the primary problem with databases stems from the way the bureaucratic process treats individuals and their information. It is a problem that is at its heart about the nature of certain relationships in our society and their effects on individuals.

Generally, the term bureaucracy refers to large public and private organizations with hierarchical structures and a set of elaborate rules, routines, and processes.[152] For the purposes of this article, I will use the term to refer not to specific institutions but to a particular set of practices—specifically, how bureaucratic processes affect and influence individuals subjected to them. Bureaucratic processes are highly routinized, striving for increased efficiency, standardization of decisions, and the cultivation of specialization and expertise.

---

150. *Id.* at 147-48.

151. *Id.* at 157.

152. *See, e.g.*, MAX WEBER, FROM MAX WEBER: ESSAYS IN SOCIOLOGY 196 (H. H. Gerth & C. Wright Mills, trans. & eds., 1946) [hereinafter WEBER, FROM MAX WEBER]; *see also* MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 329-41 (A.M. Henderson & Talcott Parsons trans., 1947).

As Max Weber observes: "Precision, speed, unambiguity, knowledge of the files, continuity, discretion, unity, strict subordination, reduction of friction and of material and personal costs—these are raised to the optimum point in the strictly bureaucratic administration. . . ."[153]

Max Weber notes how bureaucracy can become "dehumanized" by striving to eliminate "love, hatred, and all purely personal, irrational, and emotional elements which escape calculation."[154] As I described elsewhere:

> Bureaucracy often cannot provide adequate attention to the individual—not because government officials are malicious but because they are busy, face extreme stress, must act within strict time constraints, have limited training, and are often not encouraged (or even authorized) to respond to idiosyncratic situations creatively.[155]

The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, resulting in a lack of meaningful participation in decisions about our information.[156] Bureaucratic decisionmaking processes are being exercised ever more frequently over a greater sphere of our lives, and we have little power or say within such a system, which tends to structure our participation along standardized ways that fail to enable us to achieve our goals, wants, and needs.

The power effects of this relationship to bureaucracy are profound; however, its effects cannot adequately be explained by resorting to the understanding of power in Orwell's *Nineteen Eighty-Four*. Orwell's Big Brother employs a coercive power that is designed to dominate and oppress. Power, however, is not merely prohibitive; as illustrated by Aldous Huxley in *Brave New World*,[157] it composes our very lives and culture. Huxley describes a different form of totalitarian society—one controlled not by force and propaganda, but by entertainment and pleasure. The population is addicted to a drug called Soma, which is administered by the government as a political tool to sedate the people. Huxley presents a narrative about a society controlled not by a despotic coercive government like Big Brother, but by manipulation and consumption, where people participate in their own enslavement. The government achieves obedience through social conditioning, propaganda, and other forms of indoctrination.[158] It does not use the crude coercive techniques of violence and force, but instead employs a more subtle scientific method of control—through genetic engineering, psychology, and drugs. Power works internally—the government actively molds the private life of its citizens,

---

153. WEBER, FROM MAX WEBER, *supra* note 152, at 214.

154. *Id.* at 216.

155. Daniel J. Solove, *The Darkest Domain: Deference, Judicial Review, and the Bill of Rights*, 84 IOWA L. REV. 941, 1017 (1999).

156. I am certainly not suggesting that all problems with bureaucracy are privacy problems or vice versa.

157. *See* ALDOUS HUXLEY, BRAVE NEW WORLD (1932).

158. *See generally id.* at 20-32.

transforming it into a world of vapid pleasure, of mindlessness, and numbness.[159]

Despite the differences, power for both Orwell and Huxley operates as an insidious force employed for a particular design. *The Trial* depicts a different form of power. The power employed in *The Trial* has no apparent goal; any purpose remains shrouded in mystery. Nor is the power as direct and manipulative in design as that depicted by Orwell and Huxley. The Court system barely even cares about Joseph K. at all. *The Trial* depicts a world that differs significantly from our traditional notions of a totalitarian state. Joseph K. was not arrested for his political views; nor did the Court manifest any plan to control people. Indeed, Joseph K. was searching for some reason why he was arrested, a reason that he never discovered. One frightening implication is that there was no reason, or if there were, it was absurd or arbitrary. Joseph K. was subjected to a more purposeless process than a trial. Indeed, the Court does not try to exercise much power over Joseph K. His arrest does not even involve his being taken into custody—merely a notification that he is under arrest—and after an initial proceeding, the Court makes no further effort even to contact Joseph K.

What is more discernible than any motive on the part of the Court or any overt exercise of power are the social effects of the power relationship between the bureaucracy and Joseph K. The power depicted in *The Trial* is not so much a force as it is an element of relationships between individuals and society and government. These relationships have balances of power. What *The Trial* illustrates is that power is not merely exercised in totalitarian forms, and that relationships to bureaucracies which are unbalanced in power can have debilitating effects upon individuals—regardless of the bureaucracies' purposes (which may, in fact, turn out to be quite benign).

Under this view, the problem with databases and the practices currently associated with them is that they disempower people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare.

C. *Forms of Dehumanization: Databases and the Kafka Metaphor*

Expounding on the Kafka metaphor, certain uses of databases foster a state of powerlessness and vulnerability created by people's lack of any meaningful form of participation in the collection and use of their personal information.

---

159. For Huxley's own commentary on his novel, see ALDOUS HUXLEY, BRAVE NEW WORLD REVISITED (1958). For an insightful comparison between Huxley and Orwell, see NEIL POSTMAN, AMUSING OURSELVES TO DEATH vii (1986).

Bureaucracy and power is certainly not a new problem, and it has been quite artfully depicted in the work of Max Weber. Databases do not cause the disempowering effects of bureaucracy; they exarcerbate it—not merely by magnifying of existing power imbalances but by transforming these relationships in profound ways that implicate our freedom. The problem is thus old and new, and its additional dimensions within the Information Age require extensive explication.

One of the great dangers of using information that we generally regard as private is that we often make judgments based on this private information about the person. As Kenneth Karst warned in the 1960s, one danger of "a centralized, standardized data processing system" is that the facts stored about an individual "will become the only significant facts about the subject of the inquiry."[160] Jeffrey Rosen aptly observes, "Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation."[161]

Although the facts do not capture our personalities, they still have power over us, for important decisions are often made about our lives on the basis of this information. The problem is that such records often fail to tell the entire story, yet an individual is frequently judged on the basis of this information and important facets about her life—whether she gets a loan, a job, or a license—are decided based upon this information.

Increased reliance upon such easily quantifiable and classifiable information is having profound social effects. The nature and volume of information affects the way people analyze, use, and react to information. Currently, we rely quite heavily on quantifiable data: statistics, polls, numbers, and figures. In the law alone, there is a trend to rank schools; to measure the influence of famous jurists by looking to citations to opinions;[162] to measure the importance of law review articles by looking at citations to them;[163] to rank law journals with an elaborate system of establishing point values for authors

160. Karst, *supra* note 120, at 361. For a very interesting account of the problems created by the use of personal information to categorize and sort individuals, see generally OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993).

161. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000).

162. *See, e.g.*, RICHARD A. POSNER, CARDOZO: A STUDY IN REPUTATION 74-91 (1990) (measuring Benjamin Cardozo's reputation by a Lexis search counting mentions of his name).

163. *See, e.g.*, Fred R. Shapiro, *The Most-Cited Law Review Articles Revised*, 71 CHI-KENT L. REV. 751, 751 (1996) (listing the "one hundred most-cited legal articles of all time"). For a humorous critique of this enterprise, see J.M. Balkin & Sanford Levinson, *How to Win Cites and Influence People*, 71 CHI-KENT L. REV. 843 (1996).

of articles;[164] and to rank the influence of academic movements by checking citations.[165] The goal of this use of empirical data is to eliminate the ambiguity and noncommensurability of many aspects of life and try to categorize them into neat tidy categories. The computer has exarcerbated this tendency, for the increase in information and the way computers operate furthers this type of categorization and lack of judgment.[166] Indeed, much of this tendency in legal scholarship is due to the advent of computer research databases, which can easily check for citations and specific terms.

Certainly, quantifiable information can be accurate and serve as the best way for making particular decisions. Even when quantifiable information is not exact, it is useful for making decisions because of administrative feasibility. Considering all the variables and a multitude of incommensurate factors might simply be impossible or too costly.

Nevertheless, the information in databases often fails to capture the texture of our lives. Rather than provide a nuanced portrait of our personalities, they capture the stereotypes and the brute facts of what we do without the reasons. For example, a record of an arrest without the story or reason is misleading. The arrest could have been for civil disobedience in the 1960s—but it is still recorded as an arrest with some vague label, such as disorderly conduct, slapped onto it. It appears no differently from the arrest of a vandal. In short, we are reconstituted in databases as a digital persona composed of data. The privacy problem stems paradoxically from the pervasiveness of this data—the fact that it encompasses much of our lives—as well as from its limitations—how it fails to capture us, how it distorts who we are.

Privacy concerns an individual's power in the elaborate web of social relationships that encompasses her life. Today, a significant number of these relationships involve interaction with public and private institutions. In addition to the myriad of public agencies that regulate the products we purchase, the environment, and the like, we depend upon private institutions such as telephone companies, utility companies, Internet service providers, cable service providers, and health insurance companies. We also depend upon companies that provide products that we view as essential to our daily lives: hygiene, transportation, entertainment, news, and so on. Our lives are

---

164. *See, e.g.*, Robert M. Jarvis & Phyllis G. Coleman, *Ranking Law Reviews: An Empirical Analysis Based on Author Prominence*, 39 ARIZ. L. REV. 15 (1997).

165. *See, e.g.*, Jane B. Baron, *Law, Literature, and the Problems of Interdisciplinarity*, 108 YALE L.J. 1059, 1061 n.9 (1999) (comparing Westlaw search of law reviews for terms "law and economics" and "law and literature" to measure comparative influence of each of these academic movements).

166. Oscar Gandy contends that the use of profiling to form predictive models of human behavior incorrectly assumes that "the identity of the individual can be reduced, captured, or represented by measurable characteristics." Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1085, 1100 (2000). The use of profiles is "inherently conservative" because such profiles "reinforce assessments and decisions made in the past." *Id.* at 1101.

ensconced in these institutions, which have power over our day-to-day activities (through what we consume, read, and watch), our culture, politics, education, and economic well-being. We are engaged in relationships with these institutions, even if on the surface our interactions with them are as rudimentary and distant as signing up for services, paying bills, and requesting repairs. With many firms—such as credit reporting agencies—we do not even take affirmative steps to establish a relationship.

Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan. It involves the ability to avoid the collection and circulation of such powerful information in one's life without having any say in the process, without knowing who has what information, what purposes or motives those entities have, or what will be done with that information in the future. Privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants certain data expunged. It is not merely the collection of data that is the problem—it is our complete lack of control over the ways it is used or may be used in the future.

Personal information can be put to extremely troubling uses. In *Paul v. Davis*,[167] the police distributed flyers with names and photographs to various stores erroneously listing the plaintiff as an active shoplifter. The plaintiff almost lost his job and was embarrassed and afraid to enter stores. In another example, an Internet site known as 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.[168] Doctors who were killed had a black line drawn through their names. Names of wounded doctors were shaded in gray. The doctors sued. At trial, they testified as to how their lives became riddled with fear, how some wore bulletproof vests and wigs in public. They won the suit and the site was shut down, but the appellate court reversed on First Amendment grounds.[169] The availability of personal data and the ease with which it can be traded, disclosed, and used can have devastating effects on the lives of individuals. The problem is not that such records are regularly disclosed, but that there is often such little care involved in protecting them and that people have no control over them.

This powerlessness is compounded by the fact that the process of information collection in America is clandestine, duplicitous, and unfair. The choices given to people over their information are hardly choices at all. People must relinquish personal data to gain employment, procure insurance, obtain a

167. 424 U.S. 693 (1976).

168. SYKES, *supra* note 47, at 42-44.

169. Planned Parenthood of the Columbia/Williamette, Inc. v. Am. Coalition of Life Activists, 244 F.3d 1007 (9th Cir. 2001).

credit card, or otherwise participate like a normal citizen in today's economy. Consent is virtually meaningless in many contexts. When people give consent, they must often consent to a total surrender of control over their information.[170]

Collection of information is often done by misleading the consumer. General Electric sent a supposedly anonymous survey to shareholders asking them to rate various aspects of the company. Unbeknownst to those surveyed, the survey's return envelope was coded so that the responses could be matched to names in the company's shareholder database.[171]

Some information is directly solicited via registration questionnaires or other means such as competitions and sweepstakes. The warranty registration cards of many products—which ask a host of lifestyle questions—are often sent not to the company that makes the product but to National Demographics and Lifestyles Company at a Denver post office box. This company has compiled information on over 20 million people and markets it to other companies.[172] Often, there is an implicit misleading notion that consumers must fill out a registration questionnaire in order to be covered by the warranty.

Frequent shopper programs and discount cards—which involve filling out a questionnaire and then carrying a special card that provides discounts—enable the scanner data to be matched to data about individual consumers.[173] This technique involves offering savings in return for personal information and the ability to track a person's grocery purchases.[174] However, there are scant disclosures that such an exchange is taking place, and there are virtually no limits on the use of the data.

Conde Nast Publications Inc. (which publishes the New Yorker, Vanity Fair, Vogue, and other magazines) recently sent out a booklet of 700 questions concerning detailed information about an individual's hobbies, health (including drugs used, acne problems, vaginal/yeast infections, etc.), shopping preferences, etc. Almost 400,000 people responded. In return for the data, the survey said: "Just answer the questions below to start the conversation and become part of this select group of subscribers to whom marketers listen first." Conde Nast maintains a database of information on 15 million people. Stephen Jacoby, the vice president for marketing and databases said: "What we're trying to do is enhance the relationship between the subscriber and their

---

170. For example, insurance release forms typically give insurance companies significant control over an individual's medical records. *See* BRANSCOMB, *supra* note 81, at 67.

171. Robert O'Harrow, Jr., *Survey Says: You're Not Anonymous*, WASH. POST, June 9, 1999, at E1.

172. *See, e.g.*, GIVENS, *supra* note 48, at 23; HUGHES, *supra* note 61, at 318 ("For many years, National Demographic and Lifestyles. . .has been compiling customer information from registration cards packed into more than 100 different consumer products.").

173. *See* LARSON, *supra* note 36, at 134-35.

174. Robert O'Harrow, Jr., *Bargains at a Price: Shoppers' Privacy; Cards Let Supermarkets Collect Data*, WASH. POST, Dec. 31, 1998, at A1.

magazine. In a sense, it's a benefit to the subscriber."[175]

There is no "conversation" created by supplying the data. Conde Nast does not indicate how the information will be used. It basically tries to entice people to give information for a vague promise of little or no value. While the company insists that it will not share information with "outsiders," it does not explain who constitutes an "outsider." The information remains in the control of the company, with no limitations on use. Merely informing the consumer that data may be sold to others is an inadequate form of disclosure. The consumer does not know how many times the data will be resold, to whom it will be sold, or what purposes it will be used for.

This lack of control is exacerbated by the often thoughtless and irresponsible ways that bureaucracies use personal information and their lack of accountability in using and protecting the data. In other words, the problem is not simply a lack of individual control over information, but "control out of control"—a situation where nobody is exercising meaningful control over the information.

In bureaucratic settings, privacy policy tends to fall into drift and be reactionary. In a detailed study of organizations such as banks, health and life insurance companies, and credit agencies, H. Jeff Smith concluded that all of the organizations "exhibited a remarkably similar approach: the policy-making process, which occurred over time, was a wandering and reactive one."[176] According to a senior executive at a health insurance company, "We've been lazy on the privacy [issues] for several years now, because we haven't had anybody beating us over the head about them."[177] According to Smith, most executives in the survey were followers rather than leaders: "[M]ost executives wait until an external threat forces them to consider their privacy policies."[178] Furthermore, there have been several highly publicized instances where companies violated their own privacy policies.[179]

More insidious than drifting and reactionary privacy policies are irresponsible and careless uses of personal information. For example, Metromail Corporation, a seller of direct marketing information, hired inmates

---

175. Robert O'Harrow, Jr., *Survey Asks Readers to Get Personal, and 400,000 Do*, WASH. POST, Dec. 16, 1998, at C18.

176. H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 55 (1994).

177. *Id.* at 67.

178. *Id.* at 93.

179. In 1998, the FTC charged GeoCities with lying to its subscribers about their privacy; the site had collected and sold information about children who played games on the site. SYKES, *supra* note 47, at 72. In 1999, a software program called RealJukebox created by RealNetworks, Inc., which enabled users to download digitial music, was secretly collecting personal information about its users and transmitting it to Real Networks in direct violation of their privacy policy that consumers would be informed about all information collected about them. Shannon P. Duffy, *Suit Says RealNetworks' 'RealJukeBox' Software is Right Out of RealBigBrother*, *at* http://biz.yahoo.com/law/991110/55122-7.html (Nov. 10, 1999).

to enter the information into databases. This came to light when an inmate began sending harassing letters that were sexually explicit and filled with intimate details of people's lives.[180] A television reporter once paid $277 to obtain from Metromail a list of over 5000 children living in Pasadena, California. The reporter gave as the name of the buyer the name of a well-known child molester and murderer.[181] These cases illustrate the complete lack of care and accountability by the corporations collecting the data.

McVeigh v. Cohen[182] best illustrates this problem. A highly decorated seventeen-year veteran of the Navy sought to enjoin the Navy from discharging him under the statutory policy known as "Don't Ask, Don't Tell, Don't Pursue."[183] When responding to a toy-drive for the crew of his ship, McVeigh accidentally used the wrong email account, sending a message under the alias "boysrch." He signed the email "Tim" but included no other information. The person conducting the toy-drive searched through the member profile directory of America Online ("AOL") where she learned that "boysrch" was an AOL subscriber named Tim who lived in Hawaii and worked in the military. Under marital status, he had identified himself as "gay." The information was forwarded to the captain of the ship. The ship's legal adviser began to investigate, suspecting that "Tim" was the plaintiff McVeigh. Before speaking to the plaintiff and without a warrant, the legal adviser had a paralegal contact AOL for more information. The paralegal called AOL's toll-free customer service number and, without identifying himself as a Navy serviceman, lied that he had received a fax sheet from an AOL customer and wanted to confirm who it belonged to. The AOL representative told him that the customer was the plaintiff. Despite a policy of not giving out personal information, AOL carelessly disclosed the data.[184]

In sum, the privacy problem created by the use of databases stems from an often careless and unconcerned bureaucratic process—one that has little judgment or accountability—and is driven by ends other than the protection of people's dignity. We are not heading toward a world of Big Brother or one composed of Little Brothers, but toward a more mindless process—of bureaucratic indifference, arbitrary errors, and dehumanization—a world that is beginning to resemble Kafka's vision in *The Trial*.

Viewing the database problem in terms of the Kafka metaphor as opposed to the Big Brother metaphor has important ramifications for the way we apply

---

180. WHITAKER, *supra* note 16, at 132-33; Nina Bernstein, *Lives on File: The Erosion of Privacy—A Special Report*, N.Y. TIMES, June 12, 1997, at A1.

181. GIVENS, *supra* note 48, at 176.

182. 983 F. Supp. 215 (D.D.C. 1998).

183. 10 U.S.C. § 654 (2000).

184. Under 18 U.S.C. § 2703(b)(1)(A)-(B), (c)(1)(B) (2000), a remote computing service such as AOL may only disclose email contents or customer records to a governmental entity if the governmental entity first obtains either a warrant or the consent of the customer.

legal concepts and craft policies. For example, Amazon.com—one of the largest retailers of books on the Internet—collects information about a customer's taste in books (based on its sales to the user) and then provides book recommendations tailored to the customer. If the problem is surveillance, then the most obvious solution would be to provide strict limits on Amazon.com's collection of information. This solution, however, would curtail much information collection that is necessary for business in today's society and that is put to beneficial uses. Indeed, many Amazon.com customers, myself included, find Amazon.com's book recommendation service to be very helpful. In contrast, if the problem is understood as I have depicted it, then the problem is not that Amazon is spying on its users or that it can use personal data to induce its customers to buy more books. What is troubling is the unfettered ability of Amazon.com to do whatever it wants with this information. Indeed, recently, this problem was illustrated when Amazon.com abruptly changed its privacy policy to allow the transfer of personal information to third parties in the event Amazon.com sold any of its assets or went bankrupt.[185]

IV. REGULATING INFORMATION

Understanding the problem with the Kafka metaphor is not merely a descriptive endeavor, but has profound implications for the law of information privacy as well as which legal approaches are taken to solve the problem. In this Part, I explore these implications.

A. *The Limits of Privacy Law*

Throughout this century, a distinctive domain of law relating to privacy has begun to develop.[186] Privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law. Privacy law is best described with the notion of the *bricoleur*—a person who uses whatever is at hand as a tool to solve problems.[187] Privacy law consists of legal tools at hand that are used by courts and policymakers to deal with the emerging problems created by the information revolution. Much of privacy law is interrelated, and as Ken

185. *See Amazon Draws Fire For DVD-Pricing Test, Privacy-Policy Change*, WALL ST. J., Sept. 14, 2000 at B4. Indeed, dot-com bankruptcies create a breakdown in the relationship between companies and consumers, resulting in little incentive for the bankrupt company to take measures to protect consumer data. Personal information databases are often a company's most valuable asset and could be sold to third-parties at bankruptcy to pay off creditors. *See* Susan Stellin, *Dot-Com Liquidations Put Consumer Data in Limbo*, N.Y. TIMES, Dec. 4, 2000, at C4.

186. *See* RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 1-3 (1999).

187. The notion of the *bricoleur* was used most famously by Claude Levi-Strauss, and is deftly explained in BALKIN, *supra* note 25, at 31.

Gormley observes, "various offshoots of privacy are deeply intertwined at the roots, owing their origins to the same soil."[188]

Although it is a relatively youthful body of law, privacy law emerged under an older paradigm for understanding privacy, one that was shaped by a different sort of privacy problem. Privacy law was developed largely to address privacy problems of disclosure and surveillance, and consequently was aimed at protecting secrets and concealed information. It was out of this paradigm that the Big Brother metaphor emerged. Under the paradigm, privacy is about concealment, and it is invaded by watching and by public disclosure of confidential information. Surveillance is one of the ways by which one's secrecy is invaded. Although surveillance does not always invade one's secrecy, the potential for such invasions is always present. In short, this paradigm understands privacy problems as invasions into one's hidden world.

With its extensive focus on surveillance, the Big Brother metaphor merely reinforces this old paradigm. My point is not that privacy law developed in the way it did because of the Big Brother metaphor. Rather, privacy law developed with a host of problems other than databases in mind. These problems are aptly captured by the Big Brother metaphor, but databases are not. In other words, the Big Brother metaphor reinforces this older paradigm in privacy law, and to some extent inhibits privacy law from breaking away from its excessive focus on secrecy, surveillance, and disclosure.

The highly influential 1890 article by Samuel Warren and Louis Brandeis, *The Right to Privacy*,[189] is considered by many as one of the primary foundations of privacy law in the United States. The article raised alarm at the intersection of "yellow journalism,"[190] with its increasing hunger for sensational human interest stories, and the development of "instantaneous photograph[y.]"[191] The focus of the article was on the press's ability to invade the "sacred precincts of private and domestic life."[192] The article argued that existing legal causes of action currently did not adequately protect privacy but

188. Ken Gormley, *One Hundred Years of Privacy*, WIS. L. REV. 1335, 1357 (1992).

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

190. William L. Prosser, *Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 104, 104 (Ferdinand David Schoeman ed., 1984) (noting rising popular dismay over "yellow journalism" at the time of Brandeis' and Warren's article).

191. The term "instantaneous photography" was used by Warren and Brandeis to describe the development of cameras that were smaller, cheaper, and more easy to use. The motivation of the authors in writing the article is widely disputed. The prevailing view that the article was inspired by the reporting of Warren's daughter's wedding originated with Prosser in his famous 1960 privacy article. *See* Prosser, *supra* note 190, at 104. Critics have pointed out that in 1890, Warren's oldest daughter was not even ten years old. *See* TURKINGTON & ALLEN, *supra* note 186, at 46. In his superb historical account of privacy in America, Robert Ellis Smith explains that Warren was upset at a number of articles in Boston's *Saturday Evening Gazette* reporting on the dinner parties thrown by his wife at their home. *See* SMITH, *supra* note 30, at 118-19.

192. Warren & Brandeis, *supra* note 189, at 195.

that legal concepts in the common law could be modified and combined to develop the proper protection of privacy.

As early as 1903, courts and legislatures responded to the Warren and Brandeis article by creating a number of privacy torts to redress the harms that Warren and Brandeis had noted.[193] By 1960, Dean William Prosser reported over 300 privacy cases in the seventy years since the Warren and Brandeis article had inspired the birth the privacy torts.[194] He concluded that the cases could be classified as protecting four distinct interests, which have become widely used and have formed the basis for the privacy torts of the Restatement (Second) of Torts.[195] These torts are commonly known collectively as "invasion of privacy" and specifically as (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or "publicity"; and (4) appropriation.[196] Today, whether by statute or common law, most states recognize some or all of the privacy torts.[197]

The tort of intrusion protects against the intentional intrusion into one's "solitude or seclusion" or "his private affairs or concerns" that "would be highly offensive to a reasonable person."[198] Although this tort could be applied to the information collection techniques of databases, most of the information collection is not "highly offensive to a reasonable person." Each particular instance of collection is often small and innocuous; the danger is created by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time. Indeed, courts have thrown out cases for intrusion involving the type of information that would likely be collected in databases. For example, courts have rejected intrusion for obtaining a person's unlisted phone number,[199] for selling subscription lists to direct mail companies,[200] and for collecting and disclosing an individual's past insurance history.[201] Further, intrusion must involve an invasion of "seclusion" and courts have thrown out intrusion suits when plaintiffs have been in public

193. *See, e.g.*, Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis,* 39 CATH. U. L. REV. 703, 704 (1990); Louis Lusky, *Invasion of Privacy: A Clarification of Concepts*, 72 COLUM. L. REV. 693, 694 (1972). Harry Kalven has even hailed it as the "most influential law review article of all." Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326, 327 (1966).

194. Prosser, *supra* note 190, at 107.

195. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B, 652C, 652D, 652E (1976) (discussing intrusion, misappropriation, publicity of private facts, and false light).

196. Prosser, *supra* note 190, at 107.

197. *See* Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998)(recognizing a common law tort action for invasion of privacy and noting that Minnesota had remained one of the few hold-outs).

198. RESTATEMENT (SECOND) OF TORTS § 652B (1976).

199. Seaphus v. Lilly, 691 F. Supp. 127, 132 (N.D. Ill. 1988).

200. Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

201. Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978).

places.[202] With regard to databases, much information collection and use occurs in public, and indeed, many parts of cyberspace may well be considered public places.

The tort of private facts (or invasion of privacy) creates a cause of action when one makes public "a matter concerning the private life of another" in a way that "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[203] Although this tort could conceivably be applied to certain uses of databases, such as the sale of personal information by the database industry, the tort of private facts appears designed to redress excesses of the press, and is accordingly focused on the widespread dissemination of personal information in ways that become known to the plaintiff. In contrast, the disclosure of personal information through the use and sale of databases is often small and done in secret. The trade in information is done behind closed doors in a kind of underworld that most people know little about. It would be difficult for a plaintiff even to discover that such sales or disclosures have been made. Even if marketers disclosed information widely to the public, the tort is limited to "highly offensive" facts, and most facts in databases would not be highly offensive if made public. Moreover, some marketing data may be deemed public record, or a plaintiff, by furnishing data in the first place, may be deemed to have assented to its public dissemination.[204]

The tort of false light is primarily a variation on the defamation torts of libel and slander, protecting against the giving of "publicity to a matter concerning another that places the other before the public in a false light" that is "highly offensive to a reasonable person."[205] Like defamation, this tort has limited applicability to the types of privacy harms created by the collection and use of personal information by way of computer databases. Both defamation and false light protect one's reputation, but the type of information collected in databases often is not harmful to one's reputation.

The tort of appropriation occurs when "[o]ne who appropriates to his own use or benefit the name or likeness of another. . . ."[206] This tort is akin to a form of intellectual property right in aspects of one's personhood. The interest

---

202. *See* Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 482-83 (D. Me. 1987) (noting that Maine recognizes no invasion of privacy action when photographers harassed and insulted plaintiff in a public place), *vacated in part on other grounds*, 845 F.2d 347 (1st Cir. 1988).

203. RESTATEMENT (SECOND) OF TORTS § 652D (1976).

204. "[T]here is no liability for giving publicity to facts about the plaintiff's life that are matters of public record, such as the date of his birth, the fact of his marriage, his military record, the fact that he is admitted to the practice of medicine or is licensed to drive a taxicab . . . . Similarly, there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye." RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1976).

205. RESTATEMENT (SECOND) OF TORTS § 652E (1976).

206. RESTATEMENT (SECOND) OF TORTS § 652C (1976).

protected is the individual's right to "the exclusive use of his own identity, in so far as it is represented by his name or likeness."[207] This tort could be applied to the use of targeted marketing, which can be viewed as the use of personal information for profit. However, the tort's focus on protecting the commercial value of personal information has often prevented it from being an effective tool in grappling with the database privacy problem. In *Dwyer v. American Express Co.*,[208] a court held there was no appropriation when American Express sold its cardholders' names to merchants because "an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess."[209] In *Shibley v. Time, Inc.*,[210] a court held that there was no action for appropriation when magazines sold subscription lists to direct mail companies because the plaintiff was not being used to endorse any product. The appropriation tort aims at protecting one's economic interest in a form of property, and is most effective at protecting celebrities who have created value in their personalities.[211] This is not the same interest involved with privacy, which can be implicated regardless of the economic value accorded to one's name or likeness.

Even if it were possible to eliminate the above difficulties with some minor adjustments to the privacy torts, the privacy problem with databases transcends the specific injuries and harms that the privacy torts are designed to redress. By its nature, tort law looks to isolated acts, to particular infringements and wrongs. The problem with databases does not stem from any specific act, but is a systemic issue of power caused by the aggregation of relatively small actions, each of which when viewed in isolation would appear quite innocuous. I refer to this as the "aggregation problem"—the fact that the whole is greater than the parts. In other words, the problem emerges when individual information transactions, combinations, lapses in security, disclosures, or abusive uses are viewed collectively. The problem is compounded by the fact that much of this activity occurs in secret outside the knowledge of the individual whose personal information is involved. Therefore, proposed solutions involving the retooling of tort law—such as Jessica Litman's proposal

207. RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1976).

208. 652 N.E.2d 1351 (Ill. App. Ct. 1995).

209. *Id.* at 1356.

210. 341 N.E.2d 337 (Ohio Ct. App. 1975).

211. According to the Restatement, the tort is "not limited to commercial appropriation. It applies also when the defendant makes use of the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one." RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1976). However, some states have limited liability under appropriation to commercial uses. *See id.* Further, the interest protected is not the protection of one's "personal feelings against mental distress" but a "property right." RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1976).

for a breach of trust tort remedy for companies that misuse information—will be severely limited in redressing the problem.[212]

Attempts to use the Constitution to protect information privacy have similarly failed for misconstruing the problem. At the outset, the Constitution only protects against state action, and many databases belong to the private sector. However, since the government is often a supplier of information to the private sector and is a major source of databases, constitutional protection could serve as a good potential tool for grappling with the problem. Although the Constitution does not explicitly provide for a right to privacy, a number of its provisions protect certain dimensions of privacy, and the Supreme Court has sculpted a right to privacy by molding together a variety of constitutional protections.

The Fourth Amendment protects only against government infringements, and does nothing to control the collection and use of information by private bureaucracies. To the limited extent to which the Fourth Amendment can be applied to databases, the Court has adhered rigidly to the notion of privacy as secrecy. In *Smith v. Maryland*,[213] the Court held that there was no reasonable expectation of privacy in the phone numbers one dials. The Court reasoned that such phone numbers were not secret because they were turned over to third parties (phone companies).[214] Similarly, in *United States v. Miller*, the Court held that financial records possessed by third parties are not private under the Fourth Amendment.[215] The Court's focus—which stems from the paradigm that privacy is about protecting one's hidden world—leads it to the view that when a third party has access to one's personal information, there can be no privacy expectation in that information.

In the landmark 1965 case *Griswold v. Connecticut*,[216] the Court declared that an individual has a constitutional right to privacy. The Court located this right within the "penumbras" or "zones" of freedom created by an expansive interpretation of the Bill of Rights.[217] During the remainder of the twentieth century, the Court handed down an inconsistent line of cases, protecting certain fundamental life choices, such as abortion but not the right to die, and protecting certain aspects of one's intimate sexual life, such as contraception but not homosexual conduct.[218]

---

212. *See* Jessica Litman, *Information Privacy / Information Property*, 52 STAN. L. REV. 1283, 1304-13 (2000) (recounting several egregious examples of companies' breach of trust and noting the inadequacy of current tort law in those cases).

213. 442 U.S. 735 (1979).

214. *Id.* at 743.

215. 425 U.S. 435, 442-43 (1976).

216. 381 U.S. 479 (1965).

217. *Id.* at 484 ("The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . . . Various guarantees create zones of privacy.").

218. *See, e.g.*, Bowers v. Hardwick, 478 U.S. 186 (1986) (holding that the right to privacy does not extend to homosexual sexual conduct); Roe v. Wade, 410 U.S. 113, 154

In the 1977 decision, *Whalen v. Roe*,[219] the Court extended its substantive due process privacy protection to information privacy. New York passed a law requiring that records be kept of people who obtained prescriptions for certain addictive medications.[220] Plaintiffs argued that the statute infringed upon their right to privacy.[221] The Court held that the constitutionally protected "zone of privacy" extends to two distinct types of interests: (1) "independence in making certain kinds of important decisions"; and (2) the "individual interest in avoiding disclosure of personal matters."[222] The former interest referred to the substantive due process fundamental life decisions line of cases beginning with *Griswold*. The latter interest, however, was one that the Court had previously not defined.

The plaintiffs argued that they feared the greater accessibility of their personal information and the potential for its disclosure. As a result of this fear, they argued, many patients did not get the prescriptions they needed and this interfered with their independence in making decisions with regard to their health. The Court, however, held that the constitutional right to information privacy required only a duty to avoid unreasonable disclosure, and that the state had taken adequate security measures.[223]

The plaintiffs' argument, however, was not that disclosure was the real privacy problem. Rather, the plaintiffs were concerned that the collection of and greater access to their information made them lose control over their information. A part of themselves—a very important part of their lives—was placed in the distant hands of the state and completely outside their control. This is similar to the notion of a chilling effect on free speech. The effect is not caused by the actual enforcement of the law but by the fear that the existence of the law creates. The Court acknowledged that the court record supported the plaintiffs' contention that some people were so distraught over the law that they were not getting the drugs they needed. However, the Court rejected this argument by noting that because over 100,000 prescriptions had been filled before the law had been enjoined, the public was not denied access to the drugs.[224] The problem with the Court's response is that the Court failed to indicate how many prescriptions had been filled before the law had been passed. Without this, there is no way to measure the extent of the deterrence.

(1973) (holding that the right to privacy extends to decision to have an abortion); Eisenstadt v. Baird, 405 U.S. 438 (1972) (stating that the right to privacy extends to sexual relationships between unmarried heterosexuals); Griswold, 381 U.S. at 485 (holding that the right to privacy extends to use of contraception among married couples.

219. 429 U.S. 589 (1977).

220. 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.

221. *Id.* at 600.

222. *Id.* at 599-600.

223. *Id.* at 601-02.

224. *Id.* at 603.

And even if there were only a few who were deterred, the anxiety caused by living under such a regime must also be taken into account.

After *Whalen*, the Court affirmed this notion of constitutional protection for information privacy in *Nixon v. Administrator of General Services*,[225] concluding that President Nixon had a constitutional privacy interest in records of his private communications with his family but not in records involving his official duties. From then on, however, the Court did 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."[226]

The constitutional right to information privacy is constrained by the paradigm of privacy as protecting one's hidden world, and hence has not worked well to address the database privacy problem. At most, a constitutional right to information privacy can limit the government's disclosure of information, but the fact that most government records are public precludes liability.[227] Lower courts have only found a constitutionally protected right to information privacy for records that are confidential. Thus, while medical records are generally protected under constitutional information privacy,[228] arrest and conviction records are not because this information is a matter of public record.[229]

---

225. 433 U.S. 425 (1977) (holding that although ex-president Nixon had a legitimate expectation of privacy in private communications with his family, doctor, and minister, it was outweighed by the public interest in Nixon's papers).

226. Davis v. Bucher, 853 F.2d 718, 719 (9th Cir. 1988).

227. In an interesting contrast, the Court in a Freedom of Information Act (FOIA) case recognized a different and more appropriate conception of privacy. In *United States v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989), the Court held that FBI "rap sheets" compiling criminal history information about millions of people (much of which had been previously disclosed) were protected under FOIA's privacy exemption because there is a difference "between scattered disclosure of bits of information contained in a rap sheet and revelation of the rap sheet as a whole." *Id.* at 763-64. This case will be discussed in more depth below. *Infra* text accompanying notes 344-348.

228. *See, e.g.*, United States v. Westinghouse Elec. Corp., 638 F.2d 570, 581 (3d Cir. 1980) (holding that government agency's request for medical records to investigate work-related health hazards justified a minimal intrusion into the privacy of employees' medical records, so long as the agency notified workers and allowed them a chance to contest the disclosure); Doe v. Borough of Barrington, 729 F. Supp. 376, 385 (D.N.J. 1990) (finding a violation of a constitutional right to privacy where police disclosed that a person had AIDS); Woods v. White, 689 F. Supp. 874, 876 (W.D. Wis. 1988) (stating that prisoner has a constitutional right to privacy in his medical records); Carter v. Broadlawns Medical Center, 667 F. Supp. 1269, 1282 (S.D. Iowa 1987) (holding that hospital's allowing chaplains access to medical records violated constitutional privacy).

229. Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (holding that community notification laws for sex offenders (known as Megan's Law) do not violate constitutional privacy because government's interest in preventing sex offenses is compelling); Russell v. Gregoire, 124 F.3d 1079, 1094 (9th Cir. 1997) (reasoning that Washington state's version of Megan's law does not violate constitutional privacy because the "information collected and disseminated by the Washington statute is already fully available to the public and is not constitutionally protected"); Cline v. Rogers, 87 F.3d 176, 179 (6th Cir. 1996) (holding that there is no constitutional privacy right in criminal records because "arrest and conviction

The famous case of *Doe v. Southeastern Pennsylvania Transportation Authority* (*SEPTA*)[230] best illustrates how the constitutional right to information privacy cannot comprehend the privacy problem of databases. There, the plaintiff Doe was HIV positive and told two doctors (Dr. Press and Dr. Van de Beek) at his work of his condition but nobody else. He strove to keep it a secret. His employer, SEPTA, a self-insured employer, maintained a prescription drug program with Rite-Aid as the drug supplier. SEPTA monitored the costs of its program. Doe was taking a drug used exclusively in the treatment of HIV, and he asked Dr. Press whether the SEPTA officials who reviewed the records would see the names for the various prescriptions. Dr. Press said no, and Doe had his prescription filled under the plan. Unfortunately, even though SEPTA never asked for the names, Rite-Aid supplied the names corresponding to prescriptions when it sent SEPTA the reports. Pierce, the SEPTA official reviewing the records, became interested in Doe's use of the drug and began to investigate. She asked Dr. Van de Beek about the drug, and he told her what the drug was used for but would not answer any questions about the person using the drugs. Pierce also asked questions of Dr. Press, who informed Doe of Pierce's inquiry.[231]

This devastated Doe. Doe began to fear that other people at work had found out. He began to perceive that people were treating him differently. However, he was not fired, and in fact, he was given a promotion. The court held that the constitutional right to information privacy had not been violated because there had not been any disclosure of confidential information.[232] Pierce had merely informed doctors who knew already. Doe offered no proof that anybody else knew, and accordingly, the court weighed his privacy invasion as minimal.

This, however, missed the nature of Doe's complaint. Regardless of whether he was imagining how his co-workers were treating him, he was indeed suffering a real palpable fear. His real injury was the powerlessness of having no idea who else knew he had HIV, what his employer thought of him, or how the information could be used against him. This feeling of unease changed the way he perceived everything at his place of employment. The privacy problem was not merely the fact that Pierce divulged his secret or that Doe himself had lost control over his information, but rather that the

---

information are matters of public record"); Scheetz v. The Morning Call, Inc., 946 F.2d 202, 207 (3d Cir. 1991) (finding no right to privacy for disclosure of information in police reports). In an important case before *Whalen*, a district court held that there was no constitutional violation for New York to sell its motor vehicle records since these were public. "What the State has done in practical effect is to tap a small source of much-needed revenue by offering a convenient 'packaging' service." Lamont v. Comm'r of Motor Vehicles, 269 F. Supp. 880, 883 (S.D.N.Y. 1967).

230. 72 F.3d 1133 (3d Cir. 1995).

231. *Id.* at 1136.

232. *Id.* at 1139-40.

information appeared to be entirely out of anyone's control. Doe was in a situation similar to that of Joseph K.—waiting endlessly for the final verdict. He was informed that information about him had been collected; he knew that his employer had been investigating; but the process seemed to be taking place out of his sight. To some extent, he experienced the desperation that Joseph K. experienced—knowing that information about him was out there in the hands of others and that these people were in fact doing something with that information, but having no participation in the process.

Understanding the database privacy problem in terms of the Kafka metaphor illustrates that the problem with databases concerns the use of information, not merely keeping it secret. Information about an individual is often not secret, but is diffused in the minds of a multitude of people and scattered in various documents and computer files across the country. Few would be embarrassed by the disclosure of much of the material they read, the food they eat, or the products they purchase. Few would view their race, ethnicity, marital status, or religion as confidential. Of course, databases may contain the residue of scandals and skeletons—illicit websites, racy books, stigmatizing diseases—but since information in databases is rarely publicized, few reputations are tarnished. For the most part, the data is processed impersonally by computers without ever being viewed by the human eye. Much of the privacy as secrecy conception focuses on breach of confidentiality, harmed reputation, and unwanted publicity. But since these harms are not really the central problems of databases, privacy law often concludes that the information in databases is not private and is thus not entitled to protection. Indeed, one commentator defended DoubleClick's tracking of web browsing habits by stating:

> Over time, people will realize it's not Big Brother who's going to show up [at] your door in a black ski mask and take your kids away or dig deep into your medical history. This is a situation where you are essentially dropped into a bucket with 40 million people who look and feel a lot like you do to the advertising company.[233]

This commentator, viewing privacy with the Big Brother metaphor, focuses on the wrong types of harms and implicitly views only secret information as private.

The problem with databases concerns the uses and practices associated with our information, not merely whether that information remains completely secret. Although disclosure can be a violation of privacy, this does not mean that avoiding disclosure is the sum and substance of our interest in privacy. What people want when they demand privacy with regard to their personal information is the ability to ensure that the information about them will be used only for the purposes they desire. Even regarding the confidentiality of

---

233. John Schwartz, *DoubleClick Takes It on the Chin; New Privacy Lawsuit Looms; Stock Price Drops*, WASH. POST, Feb. 18, 2000, at E1 (quoting Dana Sherman).

information, the judicial understanding of privacy as secrecy fails to recognize that individuals want to keep things private from some people but not others. The fact that an employee criticizes her boss to a co-worker does not mean that she desires that her boss know her comments. We often expect privacy even when in public. Not all activities are purely private in the sense that they occur in isolation and in hidden corners. When we talk in a restaurant, we do not expect to be listened to. A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities. Contrary to the judicial notion that any information in public records cannot be private, there is a considerable loss of privacy by plucking inaccessible facts buried in some obscure document and broadcasting them to the world on the evening news. In short, the problem as understood by the Big Brother metaphor views the harm in the inhibitory effects of surveillance or in having one's hidden world uncovered or invaded. The problem as understood by the Kafka metaphor views the harm as "control out of control." Privacy can be invaded even if no secrets are revealed and even if nobody is watching us.

In its privacy legislation, Congress has sometimes looked beyond the old paradigm of privacy as protecting one's hidden world, although its privacy statutes often have failed to address the problem adequately. Since the 1970s, Congress has grappled with the problem of databases, but has been slow to take action.[234] Unlike the European Union, which adopted a general directive providing for large-scale privacy protection,[235] the United States has not enacted measures of similar scope. Instead, Congress has passed a series of statutes narrowly tailored to specific privacy problems.

The Fair Credit Reporting Act ("FCRA") of 1970,[236] which regulates the information use practices of credit reporting companies, fails to adequately restrict secondary uses and disclosures of that information. Although inspired by allegations of abuse and lack of responsiveness of credit agencies,[237] the FCRA was severely weakened due to the effective lobbying of the credit-reporting industry.[238] The FCRA permits credit reporting companies to sell the "credit header" portion of credit histories (which contains names, addresses, former addresses, telephone number, Social Security number, employment

234. *See* REGAN, *supra* note 4, at xi-xii.

235. Directive of the European Parliament and the Council of Europe on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995), *reprinted in* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 219-45 (1999) [hereinafter Directive]. For an excellent analysis of the Directive, see PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998). The Directive became effective on October 25, 1998. *Id.* at 2.

236. 15 U.S.C. § 1681 (2001).

237. SMITH, *supra* note 176, at 23.

238. REGAN, *supra* note 4, at 101.

information, and birthdate) to various commercial entities.[239] The FCRA does little to equalize the unbalanced power relationship between individuals and credit reporting companies.

Congress' most significant piece of privacy legislation in the 1970s—the Privacy Act of 1974[240]—regulates the collection and use of records by federal agencies, giving individuals the right to access and correct information held by federal agencies.[241] The Privacy Act was a good beginning, but it remains incomplete. The Privacy Act is limited only to the public sector, having no applicability to the use of databases by marketers. The Act applies only to federal, not state and local agencies.

The Family Educational Rights and Privacy Act of 1974 ("FERPA"),[242] also known as the "Buckley Amendment," regulates the accessibility of student records. FERPA remains quite narrow, only applying to a subset of records in one limited context (i.e., education). Excluded are records maintained by school law enforcement officials[243] and health and psychological records.[244]

The Cable Communications Policy Act ("CCPA") of 1984[245] requires cable operators to inform subscribers about the nature and uses of personal information collected.[246] The law prohibits any disclosure that reveals the subscriber's viewing habits,[247] and it is enforced with a private cause of action.[248] The statute, however, applies only to cable operators and it has a broad exception where personal data can be disclosed for a "legitimate business activity."[249] Nevertheless, the CCPA is an important first step in giving consumers control over their cable records.

In 1986, Congress modernized wiretapping and eavesdropping laws when it passed the Electronic Communications Privacy Act ("ECPA") of 1986.[250] The ECPA extends the protections of the Federal Wiretap Act of 1968[251] to new forms of voice, data, and video communications, including cellular phones, and email or other computer transmissions. The ECPA restricts the interception of

---

239. *See* Gindin, *supra* note 84, at 1157.

240. Pub. L. No. 93-579, 88 Stat. 1896 (2000) (codified at 5 U.S.C. § 552a (2001)).

241. 5 U.S.C. § 552a(d).

242. Pub. L. No. 93-380, 88 Stat. 484, (codified at 20 U.S.C. § 1232g (2000)).

243. 20 U.S.C. § 1232g(a)(4)(B)(ii) (2000).

244. § 1232g(a)(4)(B)(iv).

245. § 551 (2000).

246. § 551(a)(1).

247. § 551(c)(2)(C)(ii).

248. § 551(f)(1).

249. § 551(c)(2)(A).

250. 18 U.S.C §§ 2510-2522, 2701-2709, 2711 (2000).

251. In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (commonly referred to as "Title III" or "The Federal Wiretap Act"). This law "nationalized the law of federal, state and private electronic surveillance of conversations." TURKINGTON & ALLEN, *supra* note 194, at 229.

transmitted communications[252] and the searching of stored communications.[253] The focus of the law, which draws heavily from the Big Brother metaphor, is on eavesdropping and monitoring of communications; the ECPA does not otherwise limit the collection and use of personal data. Furthermore, providers of Internet services are exempted from the ECPA and are free to examine the email of their subscribers.[254]

After reporters obtained Supreme Court Justice nominee Robert Bork's video cassette rental data, Congress passed the Video Privacy Protection Act ("VPPA") of 1988,[255] which has become known as the "Bork Bill." The VPPA prohibits video tape service providers from knowingly disclosing personal information, such as titles of video cassettes rented or purchased, without the individual's written consent.[256] The VPPA creates a private cause of action only for knowing disclosures in violation of its terms.[257] The statute, however, permits the disclosure of the subject matter of video rentals to marketers.[258] The VPPA only applies to video cassette tapes,[259] and no similar restrictions are placed on bookstores, record stores, or any other type of retailer, magazine producer, or catalog company.

The Telephone Consumer Protection Act ("TCPA") of 1991[260] permits individuals to sue a telemarketer for damages up to five hundred dollars for each call received after requesting not to be called again.[261] If the telemarketer knowingly broke the law, then the penalty is trebled.[262] The TCPA, however, aims at redressing the aggravation of disruptive phone calls, and it does not govern the collection, use, or sale of personal data.

In 1994, Congress finally addressed the longstanding practice of many states of selling personal information in their motor vehicle records to marketers.[263] The Driver's Privacy Protection Act of 1994 ("DPPA")[264] limits this practice, forcing states to acquire a driver's consent before disclosing

252. 18 U.S.C. §§ 2510-2522 (2000).

253. 18 U.S.C. §§ 2701-10 (2000).

254. *See* Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) ("§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage.").

255. Pub. L. No. 100-618, 102 Stat. 3195, (codified at 18 U.S.C. §§ 2710-11 (2000)).

256. 18 U.S.C. § 2710(b) (2000).

257. §§ 2710(b)(1), (c)(1).

258. 18 U.S.C. § 2710(b)(2)(D)(ii).

259. §§ 2710(a)(4), (b).

260. Pub. L. No. 102-243, 105 Stat. 2394, (codified at 47 U.S.C. § 227 (2000)).

261. 47 U.S.C. § 227(c)(5) (2000).

262. *Id.*

263. For more information about the sale of motor vehicle information by states, see Rajiv Chandrasekaran, *Governments Find Information Pays,* WASH. POST, Mar. 9, 1998, at A1.

264. 18 U.S.C. §§ 2721-2725 (2000).

personal information to marketers.[265] Although the DPPA is an important step in controlling government disclosures of personal information to the private sector, it applies only in the context of motor vehicle records. States are not limited in disclosing information contained in the numerous other forms of records they maintain.

In 1996, Congress finally addressed the issue of health privacy in the Health Insurance Portability and Accountability Act ("HIPAA") of 1996.[266] HIPPA required the Department of Health and Human Services (HHS) to promulgate regulations to govern the privacy of medical records.[267] HHS issued regulations which, among other things, require authorization for all uses and disclosures beyond those for treatment, payment, or health care operation (such as for marketing purposes).[268]

The first federal law directly addressing privacy in cyberspace, the Children's Online Privacy Protection Act ("COPPA") of 1998,[269] regulates the collection of children's personal information on the Internet.[270] Websites targeted at children must post privacy policies[271] and must obtain "parental consent for the collection, use, or disclosure of personal information from children."[272] But the law's reach is limited. The COPPA applies only to "an operator of any website or online service directed to children, . . . or the operator . . . that has actual knowledge that it is collecting personal information from a child."[273] Moreover, the law applies only to website operators who collect personal information from children under age thirteen.[274]

The Gramm-Leach-Bliley Act of 1999,[275] permits banks, insurers, and investment companies that are affiliated to share the "nonpublic personal information" that each affiliate possesses. Affiliates must tell customers that they

---

265. *See* 18 U.S.C. § 2721(b)(12).The statute was recently upheld by the Supreme Court against a federalism challenge. *See* Reno v. Condon, 528 U.S. 141 (2000).

266. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

267. 110 Stat. at 2033-34.

268. 45 C.F.R. § 164.508(a). The regulations do not permit health care entities to condition the provision of treatment or eligibility for benefits on the individual's authorization of such uses of personal information. *See* 45 C.F.R. § 164.508(b)(iv). The regulations were finalized at the end of the Clinton Administration. Although the Bush Administration initially criticized the regulations and vowed to delay their implementation, *see* Robert Pear, *White House Plans to Revise New Medical Privacy Rules*, N.Y. TIMES, Apr. 8, 2001, at 22, the Administration recently announced that the regulations would go into effect but would be modified at a later date. Robert Pear, *Bush Accepts Rules to Guard Privacy of Medical Records*, N.Y. TIMES, Apr. 13, 2001, at A1.

269. 15 U.S.C. §§ 6501-06 (2000).

270. § 6502(a)(1).

271. § 6502(b)(1)(A)(i).

272. § 6502(b)(1)(A)(ii).

273. § 6502(b)(1)(A).

274. § 6501(1).

275. Pub. L. No. 106-102, 113 Stat. 1338, (codified at 15 U.S.C. §§ 6801-6809 (2001)).

are sharing this information, but there is no way for individuals to block this sharing of information. People can only opt-out of the disclosure of their data to third parties.[276] Given the large conglomerates of today's corporate world, affiliate sharing is significant. For example, Experian, one of the three largest credit reporting companies, was purchased by Great Universal Stores, a British retail corporation, which also acquired Metromail, Inc., a direct-marketing company.[277] Further, the Act applies only to "nonpublic" information, and much of the information aggregated in databases (such as one's name, address, and the like) are traditionally considered to be public.

In sum, the federal laws are a start, but they often misapprehend the nature of the problem because they give people only a very limited form of control over only some of their information and often impose no system of default control on other holders of such information. Although the statutes help in containing the spread of information, they often fail to adequately address the underlying power relationships and contain broad exceptions and loopholes that limit their effectiveness.

Furthermore, the federal statutes cover only a small geography of the database problem. They form a complicated patchwork of regulation with significant gaps and omissions. For example, federal regulation covers federal agency records, educational records, cable television records, video rental records, and state motor vehicle records, but it does not cover most records maintained by state and local officials, as well as a host of other records held by libraries, charities, and merchants (i.e., supermarkets, department stores, mail order catalogs, bookstores, and the like). The COPPA protects the privacy of children under thirteen on the Internet, but there is no protection for adults. As Colin Bennett observes, "[t]he approach to making privacy policy in the United States is reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent. There may be a lot of laws, but there is not much protection."[278]

Second, in practice many of Congress' laws are difficult to enforce. It is often difficult, if not impossible, for an individual to find out if information has been disclosed. A person who begins receiving unsolicited marketing mail and email may have a clue that some entity has disclosed her personal information, but that person often will not be able to discover what entity was the culprit. Indeed, the trade in personal information is a clandestine underworld, one that is not exposed sufficiently by federal privacy regulation to enable effective enforcement.

In short, the Kafka metaphor illustrates that the problem runs deeper than

---

276. 15 U.S.C. § 6802(a), (b) (2001).

277. *See* SMITH, *supra* note 30, at 327.

278. Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99, 113 (Philip E. Agre & Marc Rotenberg eds., 1997).

disclosure and that at the core it concerns "control out of control"—the fact that our personal information is not only out of our control but also is often placed within a bureaucratic process that lacks control and discipline in handling and using such information. Although the federal statutes are better at addressing this problem than the privacy torts, the constitutional right to information privacy, or the Fourth Amendment, they remain severely limited.

B. *Misgivings of the Market*

The implications of depicting the privacy problem of databases with the Kafka metaphor go further than throwing into question the conception of privacy underlying most of privacy law. The implications suggest that the existing solutions advocated by the discourse on information privacy are inadequate to deal with the problem. In this Part, I analyze and critique the solutions advocated by the discourse, solutions which are predominantly market-based, relying on property rights or contractual defaults to regulate the flow of information. As I argue, understanding the problem in terms of the Kafka metaphor highlights the shortcomings of the market-based solutions currently being advocated and suggests new directions for the law.

Perhaps the most appropriate notion of privacy for databases is that of "control of personal information," one of the most dominant conceptions of privacy.[279] In the most famous formulation of this concept, Alan Westin declared: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[280] Numerous other scholars embrace this definition.[281] Arthur Miller declared that "the basic attribute of an effective

---

279. One commentator has referred to the conception of privacy as "control over information about oneself" as the "classic notion" of privacy. JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 24 (1997).

280. WESTIN, PRIVACY AND FREEDOM, *supra* note 120, at 7.

281. *See, e.g.*, ADAM CARLYLE BRECKENRIDGE, THE RIGHT TO PRIVACY 1 (1970) (Privacy is "the individual's right to control dissemination of information about himself."); Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1810-1990*, 80 CALIF. L. REV. 1133, 1135 (1992) ("I will advance a concept of privacy based on the individual's control of information. . . ."); Oscar M. Ruebhausen & Orville G. Brim, Jr., *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1189 (1965) ("The essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others."). Anne Wells Branscomb, in a recently published book, focuses almost exclusively on the importance of control over information for privacy. *See* BRANSCOMB, *supra* note 81. Even in 1890, Warren and Brandeis appear at one point to intimate a control over information conception of privacy: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. . . . [E]ven if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them." Warren & Brandeis, *supra* note 189, at 198.

right to privacy is the individual's ability to control the circulation of information relating to him."[282] According to Charles Fried, "Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."[283] Similar to Westin, Miller, and Fried, President Clinton's Information Infrastructure Task Force defined privacy as "an individual's claim to control the terms under which personal information—information identifiable to an individual—is acquired, disclosed, and used."[284] The Supreme Court has even echoed this conception by stating that privacy "encompass[es] the individual's control of information concerning his or her person."[285]

Theorists who view privacy as control over information frequently understand it within the framework of property and contract concepts. This is not the only way control can be understood, but the leading commentators often define control in terms of ownership—as a form of property right in information.[286] Understood in such terms, control over something entails a bundle of legal rights of ownership, such as rights of possession, alienability, exclusion of others, commercial exploitation, and so on.[287] This is what leads Westin to conclude: "[P]ersonal information, thought of as the right of decision over one's private personality, should be defined as a property right. . . ."[288] The market discourse focuses the debate around who should own certain kinds of information as well as what the appropriate contractual rules should be for trading personal information.

Although some might argue that personal information is owned by the individual to whom it pertains based on a natural rights theory or some form of inherent connection, many commentators who approach privacy in terms of property rights assign initial entitlements instrumentally. They claim that the market will achieve the ideal amount of privacy by balancing the value of personal information to a company (i.e., its commercial value in the marketplace) against the value of the information to the individual and the

---

282. MILLER, *supra* note 45, at 25.

283. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

284. INFORMATION INFRASTRUCTURE TASK FORCE: PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (June 6, 1995), *available at* http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html.

285. United States v. Reporters' Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

286. *See* Litman, *supra* note 212, at 1287 ("The proposal that has been generating the most buzz, recently, is the idea that privacy can be cast as a property right."); Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1132 (2000) ("In recent years, a number of economists and legal commentators have argued that the law ought now to grant individuals property rights in their personal data.").

287. *See* Litman, *supra* note 212, at 1295 ("The raison d'etre of property is alienability. . . .").

288. WESTIN, PRIVACY AND FREEDOM, *supra* note 120, at 324.

larger social value of having the information within the individual's control.[289] The role of law is to assign the initial entitlements. Thus, the debate in this discourse centers around who should own certain kinds of information.[290]

In addition to discussing how the initial entitlements to information should be assigned, the debate also focuses on the basic contractual default rules for the sale or transfer of personal information. Contractual default rules are the initial set of rules that regulate market transactions. These rules are merely a starting point; they govern only when the parties to a transaction do not negotiate for a different set of rules. As Ian Ayres and Robert Gertner explain, "default rules" are rules "that parties can contract around by prior agreement" while "immutable rules" (or inalienablity rules) are rules that "parties cannot change by contractual agreement."[291] Most market proponents favor default rules that can be bargained around.

Market solution proponents are certainly not in agreement over the types of property entitlements and contractual default rules that should be required. Some—especially people in the database industry—argue that the market is functioning optimally and is already adequately accounting for privacy concerns.[292] According to this argument, there are market incentives for companies to keep their data secret and to be honest about their data collection. There have been a number of instances where companies have canceled various initiatives due to public outcry over privacy. For example, in response to privacy concerns, Yahoo! eliminated the reverse telephone number search from its People Search site.[293] In the early 1990s, in response to a public outcry, Lotus Corporation scrapped plans to sell a database containing the names, addresses, income brackets, and lifestyle data of 120 million citizens.[294] In 1996, Lexis-Nexis announced its P-TRAK Personal Locator which would provide addresses, maiden names, and Social Security numbers of millions of people. After an intensive 10-day outcry by Internet users, Lexis-Nexis

289. *See, e.g.*, JOHN HAGEL III & MARC SINGER, NET WORTH: SHAPING MARKETS WHEN CONSUMERS MAKE THE RULES 19-20 (1999) (advocating for an "infomediary" between consumers and vendors who would broker information to companies in exchange for money and goods to the consumer); Paul Farhi, *Me Inc.: Getting the Goods on Consumers*, WASH. POST, Feb. 14, 1999, at H1.

290. *See, e.g.*, BRANSCOMB, *supra* note 81.

291. Ian Ayres & Robert Gertnert, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 87 (1989).

292. *See Privacy in Commercial World*, 106th Cong. (2001) (statement of Paul H. Rubin, Professor of Law and Economics, Emory University School of Law), *available at* http://www.house.gov/commerce/hearings/0301200143/Rubin66.htm.; Direct Marketing Ass'n, Inc., Consumer Privacy Comments Concerning the Direct Marketing Association Before the Federal Trade Commission (July 16, 1997); FRED H. CATE, PRIVACY IN THE INFORMATION AGE 113 (1997).

293. Gindin, *supra* note 87, at 1160.

294. LARSON, *supra* note 36, at 9-10; *see also* SYKES, *supra* note 47, at 32; Gindin, *supra* note 87, at 1160; Lawrence M. Fisher, *New Data Base Ended by Lotus and Equifax*, N.Y. TIMES, Jan. 24, 1991, at D4.

canceled its plans.[295] In 1997, AOL canceled its plans to sell customers' phone numbers to direct marketing firms.[296]

According to market purists, to the extent that consumers want their privacy protected, the market will respond to this demand and appropriately balance it against other interests. The fact that privacy is not afforded much protection demonstrates that people value other things more than privacy—such as efficient and convenient transactions. Furthermore, people want targeted marketing and enjoy receiving information about products more tailored to their wants and tastes.

Moreover, due to consumer worries over privacy, companies have increasingly been adopting privacy policies, which operate as a form of notice as to how information will be used and a contractual promise limiting the future uses of the information.[297] Finally, the argument goes, in many contexts, the market is already treating personal information as a property right owned by individuals. The exchange of personal information for something of value is already beginning to take place. Many web sites require people to supply personal information in order to gain access to information on the web site. Under the market approach, this practice can be justified as an information trade.[298] In order to receive such services as book recommendations, software upgrades, free email, and personal web pages, users must relinquish personal information not knowing its potential uses. In short, useful information and services are being exchanged for personal information, and this represents the going "price" of privacy.

Other market-solution proponents are less sanguine. They recognize problems in the existing market and argue that certain default contractual rules and property rights must be established in order to protect privacy. For example, Richard Murphy claims that personal information, "like all information, is property."[299] "The assignment of the property right to the

---

295. SYKES, *supra* note 47, at 31-32.

296. *Id.* at 32.

297. In 1997, the Electronic Privacy Information Center ("EPIC") reviewed 100 of the most frequently visited web sites. Almost half of the websites collected personal data; however, only seventeen sites had explicit privacy policies. *See* ELECTRONIC PRIVACY INFORMATION CENTER, REPORT: SURFER BEWARE: PERSONAL PRIVACY AND THE INTERNET (June 1997), *available at* http://www.epic.org. None of the sites using cookies informed the user that information about the user was being placed on the user's system. *See id.* In 1999, a study by the Georgetown Internet Privacy Policy Survey of 361 sites revealed that over 90% collected personal information, with over half collecting demographic information. GEORGETOWN INTERNET PRIVACY POLICY SURVEY: REPORT TO THE FEDERAL TRADE COMM'N 6 (June 1999), *available at* http://www.msb.edu/faculty/culnanm/gippshome.html. Of the sites that collected personal information, 65.9% posted some form of privacy policy. *Id.* Although these two studies involved a different group of sites, they reflect a trend: more personal information is being collected and more sites are posting privacy policies.

298. For a justification of this practice, see Justin Matlick, *Don't Restrain Trade in Information*, WALL ST. J., Dec. 2, 1998, at A22.

299. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383-84 (1996).

information," observes Murphy, "is a question of contract, either explicit contract, or in the absence of express terms, implied contract."[300] Murphy engages in an instrumental analysis of privacy, determining that "there are, also, substantial economic benefits to personal privacy"[301]—benefits which might in many cases outweigh the value of the information to a third party. He concludes that in many instances, contractual default rules mandating that personal information not be disclosed are more efficient than a default rule permitting disclosure.[302]

Likewise, Jerry Kang views personal information as a form of property and advocates for a market solution.[303] He recognizes that there are compelling non-market perceptions of privacy that view privacy as a human value and that this way of understanding privacy is "poorly translated, if at all, into efficiency terms."[304] "This approach," observes Kang, "would view the right to privacy as less like a property right—which we comfortably peddle away in the marketplace—and more like a civil or human right."[305] Nevertheless, he favors the market approach, since the human rights approach suggests adopting inalienability rules, which "risk[] surrendering control over information privacy to the state."[306] Kang recognizes that merely assigning a default rule as to the ownership in information is insufficient. Kang concludes that it is not efficient for individuals to have to find out what information about them is collected and how it is used.[307] Thus, he advocates a contractual default rule that "personal information may be processed in only functionally necessary ways" and that parties are "free to contract around the default rule."[308] Kang claims that inalienability rules would be too paternalistic. "[C]ontrol is at the heart of information privacy," he claims, and control means that individuals should be able to sell or disclose their information if they desire.[309] Inalienability rules will risk "surrendering control over information privacy to the state."[310] Although Kang clearly recognizes the problems of translating personal information into a form of personal property, the effects of his market solution force such a translation. His solution creates a property right in personal information through a contractual default rule that limits the way personal

---

300. *Id*. at 2402.
301. *Id*. at 2416.
302. *Id*.
303. Kang, *supra* note 136, at 1267.
304. *Id*. at 1260.
305. *Id*. at 1266.
306. *Id*.
307. *Id*. at 1256-57.
308. *Id*. at 1268.
309. *Id*. at 1266. To be fair, Kang is not absolutist in this view, and recognizes that in some limited circumstances (emergency room data), inalienability rules are preferable. *See id*. at n.302.
310. *Id*.

information is used after being transferred to another.

Lawrence Lessig also advocates a market approach. He argues that a property regime permits each individual to decide for herself what information to give out and "protects both those who value their privacy more than others and those who value it less. . . ."[311] Lessig notes that our existing system of posting privacy policies and enabling consumers to opt in or out has high transaction costs because people do not have "the time or patience to read through cumbersome documents describing obscure rules for controlling data."[312] Therefore, Lessig recommends that computer software be crafted to act akin to an "electronic butler," negotiating our privacy concerns: "The user sets her preferences once—specifies how she would negotiate privacy and what she is willing to give up—and from that moment on, when she enters a site, the site and her machine negotiate. Only if the machines can agree will the site be able to obtain her personal data."[313] In other words, Lessig offers a technological implementation for a market system where people have property rights in their information.

Similarly, Judge Richard Posner translates control of information into property concepts, but with much different results than Murphy, Kang, and Lessig.[314] Posner views privacy as a form of withholding true information from the marketplace. He views privacy law as typically concerning the question "whether a person should have a right to conceal discreditable facts about himself. . . ."[315] "The economist sees a parallel to the efforts of sellers to conceal defects in their products."[316] Society should provide individuals a property right in true information about themselves when it will foster more efficient transactions.[317] With regard to list renting, Posner argues that "the costs of obtaining subscriber approval would be high relative to the value of the list."[318] "If, therefore, we believe that these lists are generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to subscribers, we should assign the property right to the magazine; and the law does this."[319]

Understanding the privacy problem of databases in terms of the Kafka metaphor reveals that there are several deficiencies in the market solution. The argument that the market is already providing the optimal level of privacy protection fails because there are vast inequalities in knowledge and much data collection is clandestine. Despite the few instances where information

311. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 161 (1999).
312. *Id.* at 160.
313. *Id.*
314. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE, 233 (1981).
315. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. 1998).
316. *Id.*
317. Posner, *supra* note 314 at 235.
318. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 398 (1978).
319. *Id.*

collection initiatives were canceled due to public complaints over privacy, many new ambitious information collection endeavors occur outside of the public eye. At any given time, one of thousands of companies or government agencies could decide on a new use of information or on a new form of collection. People should not always have to be ready to mount a large campaign any time such an eruption could occur. Many of the activities of the database industry are not well known to the public, and will remain that way under default notions of corporate privacy and trade secrets unless something is changed. Ironically, corporate bureaucracies sometimes have more privacy rights than individuals.

Although more companies that routinely collect and use personal information are posting privacy policies, these policies hardly amount to a meaningful contract. Rather, privacy policies tend to be self-indulgent, making vague promises such as the fact that a company will be careful with data; that it will respect privacy; that privacy is its number one concern. These public-relations statements are far from reliable and are often phrased in a vague, self-aggrandizing manner to make the corporation look good. What is not given to consumers is a frank and detailed description of what will and will not be done with their information, of what specific information security measures are being taken, of what specific rights of recourse consumers have. People must rely on the good graces of companies that possess their data to keep it secure and to prevent its abuse. They have no say in how much money and effort will be allocated to security; no say in which employees get access; and no say in what steps are taken to ensure that unscrupulous employees do not steal or misuse their information. Instead, privacy policies only vaguely state that they will treat information securely. Specific measures are not described, and individuals have no control over those measures.

Most privacy policies have no way to prevent changes in policy or a binding enforcement mechanism. Although the Direct Marketing Association (DMA) maintains standards for self-regulation, polls suggest that less than twenty-five percent of DMA members will adhere to self-regulatory practices.[320] One employee at a bank stated: "We joke about it all the time because we officially say that we don't reveal information and we treat it with the utmost respect. What a crock. I hear people laughing in the elevator about credit reports they've pulled!"[321]

Frequently, companies change their privacy policies, making it even more difficult for an individual to keep track. Yahoo!'s privacy policy indicates that it "may change from time to time, so please check back periodically."[322] AOL

320. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNTIED STATES DATA PROTECTION 309 (1996).

321. SMITH, *supra* note 176, at 80.

322. Yahoo!, Privacy Policy, *available at* http://docs.yahoo.com/info/privacy/us (last visited Mar. 11, 2001).

recently told its subscribers that their privacy preferences had expired and that if they did not fill out a new opt-out form, then their personal information would be distributed to marketers and other parties.[323] Further, personal information databases can be sold to other businesses with less protective privacy policies, especially when a company goes bankrupt and its database is among its largest assets.[324]

Even market approaches favoring a more pro-privacy regime of contractual default rules neglect to account for the core of the database problem as illustrated by the Kafka metaphor—the power inequalities that pervade the world of information transfers between individuals and bureaucracies.

A market approach has difficulty assigning the proper value to personal information. It is difficult for the individual to adequately value specific pieces of personal information. The value of one's Social Security number lies not in its intimacy, not in its immediate revelations of selfhood, and not in the fact that the individual has authored it or given it special value. Rather, the value is in the power of this number over the individual; the ability it provides to others to gain power and control over an individual, to invade an individual's private life, to make the individual vulnerable to fraud, identity theft, prying, snooping, and the like. Because this value is linked to uncertain future uses, it is difficult, if not impossible, for an individual to adequately value her information. Since the ownership model involves individuals relinquishing full title to the information, they have little idea how such information will be used when in the hands of others.

Furthermore, the aggregation problem severely complicates the valuation process. An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information. It is the totality of information about a person and how it is used that poses the greatest threat to privacy. As Julie Cohen notes, "[a] comprehensive collection of data about an individual is vastly more than the sum of its parts."[325] From the standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision. The potential future uses of that information are too vast and unknown to enable individuals to make the appropriate valuation.

Further, the value of the information cannot merely be measured from the

---

323. Doug Brown, *AOL To Users: Opt Out Again*, Yahoo! News *at* http://dailynews.yahoo.com/h/zd/19991129/tc/1991129031.html (last visited Nov. 29, 1999).

324. Recently, Toysmart.com filed for bankruptcy and attempted to auction off its personal information database of over 200,000 customers. *See* Stephanie Stoughton, *FTC Sues Toysmart.com to Halt Data Sale, Bankrupt E Retailer Made Privacy Vow to Customers*, BOSTON GLOBE, July 11, 2000, at E2; *Judge Shelves Plan for Sale of Online Customer Database*, N.Y. TIMES, Aug. 18, 2000, at C2.

325. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000).

individual's perspective. As Byford aptly observes, assigning property rights in information "values privacy only to the extent it is considered to be of personal worth by the individual who claims it."[326] This method of valuation is too individualistic, ascribing value to information solely upon the sentiments of the individual. Thus, the value of privacy is not located in particular information and defined by the individuals to whom that information pertains; rather the value of privacy lies in its systemic effects on power and powerlessness in society.

These inadequacies with a property rights solution are manifested in *Dwyer v. American Express Co*.[327] American Express cardholders sued American Express for renting their names to merchants under both invasion of privacy and misappropriation. The court held that by using the credit card, "a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences."[328] Thus, there was no invasion of privacy. As for misappropriation, the court reasoned:

> Undeniably, each cardholder's name is valuable to defendants. The more names included on a list, the more that list will be worth. However, a single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess.[329]

This case indicates what is omitted when information privacy is reduced to property rights in information. The court struggled with the fact that the information was shared and that value was not created by the individuals alone. The court only focused on the value of the information to each individual, not on the systemic harms that American Express' practices contributed to—namely, the powerlessness of the individuals to have any meaningful control over information pertaining to their personal lives. The problem with databases is not that information collectors fail to compensate people for the proper value of personal information. The problem is people's lack of control, their lack of knowledge about how it will be used in the future, and their lack of participation in the process. It is not merely sufficient to allow people to sell their information, relinquish all title to it and allow companies to use it as they see fit. This provides people with an all-or-nothing type of exchange, which they are likely to take when they are unaware of how information can or might be used in the future. Nor is it enough to attach some default contractual rights to information transactions such as nondisclosure obligations or a requirement of notification when a future use of information is employed. These solutions

---

326. Byford, *supra* note 15, at 56.
327. 652 N.E.2d 1351 (Ill. App. Ct. 1995).
328. *Id*. at 1354.
329. *Id*. at 1356.

cannot work effectively in a situation where the power relationship and information distribution between individuals and public and private bureaucracies is so greatly unbalanced. In other words, the problem with market solutions is not merely that it is difficult to commodify information (which it is), but also that a regime of default rules alone (consisting of property rights in information and contractual defaults) will not enable fair and equitable market transactions in personal information.

A market solution will also experience difficulty because information transactions are often grossly unfair and unequal. As Peter Swire observes, it is difficult for consumers to bargain with large corporations about their privacy because they lack expertise in privacy issues and it takes substantial time and effort.[330] Information collection is duplicitous, clandestine, and often coerced. The law currently does not provide meaningful ability to refuse to consent to relinquish information. The FCRA, for example, mandates that individuals consent before an employer can obtain their credit report. According to Joel Reidenberg: "Frequently, individuals will be asked to sign blanket consent statements authorizing inquiry into credit reporting agency files and disclosures of information for any purpose. These consents rarely identify the credit reporting agencies or all the uses to which the personal information will be put."[331] This consent is virtually meaningless. When people seek medical care, among the forms they sign are general consent forms which permit the disclosure of one's medical records to anyone with a need to see them. Giving people property rights or default contract rules is not sufficient to address the problem because it does not address the underlying power inequalities that govern information transactions. Unless these are addressed, any privacy protections will merely be "contracted" around, in ways not meaningful either to the problem or to the contract notions supposedly justifying such a solution. People will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought. As Julie Cohen correctly contends, "[f]reedom of choice in markets requires accurate information about choices and other consequences, and enough power—in terms of wealth, numbers, or control over resources—to have choices."[332]

Due to the problems with ascribing a value to personal information and because privacy is an issue about societal structure involving our relationships with public and private bureaucracies, some form of regulation is necessary that exceeds the narrow measures proposed by proponents of a market solution. There are certain rights we cannot bargain away because they are not mere

---

330. *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *at* http://www.osu.edu/units/law/swire1/psntia6.htm, at 10 (containing the draft submitted to NTIA on Dec. 12, 1996).

331. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 212 n.87 (1992).

332. Cohen, *supra* note 325, at 1396.

individual possessions but are important for the structure of society as a whole.

Inalienability rules do not necessarily have to limit a person's ability to disclose or sell certain information; nor must they limit many forms of information collection. These rules should focus on our relationships with bureaucracies, for unless these relationships are equalized, markets in information will not consist of fair, voluntary, and informed information transactions. The problem with databases goes to the very structure of the information market itself. I am not arguing that some form of market mechanism cannot work; rather, I am arguing that a precondition of a successful market is establishing rules governing our relationships with bureaucracies.

C. *An Agenda for a Solution*

Some commentators argue that things have already progressed too far for law to curtail the collection and use of information. Amitai Etzioni observes that "as long as Americans wish to enjoy the convenience of using credit cards and checks (as opposed to paying cash) and of ordering merchandise over the phone and the Internet (rather than shopping in person), they will leave data trails that are difficult to erase or conceal."[333] "To be realistic," Etzioni states, "the probability of returning the genie to the bottle is nil."[334] In his recent book, *The Transparent Society,* David Brin echoes the same sentiment: "[I]t is already far too late to prevent the invasion of cameras and databases. The *djinn* cannot be crammed back into its bottle."[335] Brin suggests that we abandon privacy in favor of a transparent society, one where everything is out in the open, where we watch the watchers, where we have the power to monitor the elites—the politicians and the corporate leaders—just as much as they have the ability to monitor us. We should thus regulate in favor of more laws such as the Freedom of Information Act to expose information held by government and corporations. A truly transparent society would hold those who would violate our privacy accountable.[336]

The difficulty with Brin's solution is made manifest when the problem of databases is no longer seen as predominantly one of surveillance. One aspect of the problem is that inequalities in power relationships are increased significantly by the use of databases. The problem stems from a group of disempowering practices associated with databases. Affording more mutuality of access to information will do little to alter this power imbalance because information is much more of an effective tool in the hands of a large

---

333. AMITAI ETZIONI, THE LIMITS OF PRIVACY 131 (1999).

334. *Id*.

335. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 8 (1998)

336. *Id*. at 23-24.

bureaucracy. Information is not the key to power in the Information Age—knowledge is. Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed. The mere possession of information does not give one power; it is the ability to process that information and the capabilities to use the data that matters. In order to solve the problem, a transparent society would have to make each individual as competent as bureaucratic organizations in processing information into knowledge.

Therefore, a set of laws and rights is necessary to govern our relationship with bureaucracies. These laws must consist of more than default rules that can be contracted around or property entitlements that can be bartered away. The market-based solutions work within the existing market; the problem with databases is the very way that the market deals with personal information—a problem in the nature of the market itself that prevents fair and voluntary information transactions.

First, in light of the revolution in accessibility provided by modern computer capabilities and the Internet, we must rethink the accessibility of the information in public records. The privacy torts have been severely weakened by a series of Supreme Court decisions upholding First Amendment interests. As one commentator has observed, "the tort of invasion of privacy is probably best described as alive, but on life support."[337] In *Cox Broadcasting Corp. v. Cohn*,[338] 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. In *Smith v. Daily Mail Publishing Co.*,[339] the Court struck down a statute prohibiting the publication of the names of juvenile offenders. In *Florida Star v. B.J.F.*,[340] a newspaper that had published the name of a rape victim obtained from a publicly released police report successfully challenged a Florida law prohibiting the mass communication of the name of rape victims. The Supreme Court 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. . . ."[341]

Given these First Amendment limitations, governments must rethink what records and information they make publicly available and which ones they refuse to make publicly available. Currently, states vary in what information they make publicly available. Death certificates are public in California but not

337. Murphy, *supra* note 299, at 2388. Several other commentators have called for the abolition of several of the privacy torts. *See, e.g.*, Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 294 (1983) ("Is it possible that the seemingly elegant vessel that Warren and Brandeis set afloat . . . is in fact a leaky ship which should at long last be scuttled?").

338. 420 U.S. 469 (1975).

339. 443 U.S. 97 (1979).

340. 491 U.S. 524 (1989).

341. *Id.* at 541.

in New York.[342] Often such decisions are made by agencies and bureaucrats. Certain records are considered confidential: tax, social welfare, criminal history. Others are public: property records, birth, death, marriage certificates, court records, motor vehicle records, voter registration records. The privacy case law neglects to examine the unlimited power of the government officials to determine what information is public. People do not have much choice in refusing to supply much of the information in these records. When records are made publicly available, access to them vastly increases. As discussed earlier, a number of sites on the Internet are beginning to amass public records into central databases.[343]

Second, courts must abandon the notion that privacy is limited to concealing or withholding information, and must begin to recognize that accessibility and uses of information—not merely disclosures of secrets—can threaten privacy. In one context, the Court appeared to understand the necessity of breaking away from the privacy-as-secrecy model. In *United States v. Reporters Comm. for Freedom of the Press*,[344] the Court held that the release of FBI rap sheets was an invasion of privacy within the privacy exemption of FOIA. The FBI maintains rap sheets (which contain date of birth, physical description, and a history of arrests, charges, and convictions) on over twenty-four million people.[345] FOIA exempts law enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[346] The reporters claimed that the events summarized in the rap sheet had previously been publicly disclosed. 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.[347]

The Court concluded, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[348]

In *Reporters Committee,* the Court properly departed from a privacy as

---

342. BRANSCOMB, *supra* note 81, at 65.
343. *See* note 102 *supra* and accompanying text.
344. 489 U.S. 749 (1989).
345. *Id.* at 749.
346. 5 U.S.C. § 552(b)(7)(C) (2000).
347. 489 U.S. at 763-64.
348. *Id.* at 764.

secrecy conception, understanding that it is the extent of publicity, not merely complete secrecy, that matters. Unfortunately, this was one of the few instances in which the Court has done so. Efforts to restrict the use of public information may run into First Amendment problems, and some difficult trade-offs may have to be made between privacy and free expression (particularly in the form of commercial speech) as well as free access to public records. In *Los Angeles Police Department v. United Reporting Publishing Corp.*,[349] the Court began to address this issue when it upheld a California law that restricted targeted marketers from obtaining law enforcement records of the names and addresses of arrestees and crime victims.[350] 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" which it was under no duty to disclose.[351]

Third, the current self-regulatory and legislative solution of enabling people to opt out of having their data collected or disseminated is ineffectual. In an opt-out system, the default rule is that personal data can be collected and used unless the individual expressly states a preference not to have information collected or used. Opt-out systems require individuals to check a box, send a letter, make a telephone call, or take other affirmative steps to indicate their preferences. However, there are too many collectors of information for a reasonable right of opt-out to be effective. Without a centralized mechanism for individuals to opt-out, individuals would have to spend much of their time guarding their privacy like a hawk.

Opting-out is often time consuming and not very effective. The Direct Marketing Association ("DMA") establishes a Mail Preference System, by which consumers request the service to ask businesses to stop soliciting them. This is essentially a database of people who do not want to be in databases. The service records their preference, but does not remove their name from any list.[352] The database is then sent to the subscribing companies so that they can stop mailings to those names.[353] However, many people are unaware of this option, numerous companies are not members of the DMA, and many members fail to comply with DMA guidelines. As Jeff Sovern argues, opt-out systems provide little incentive to companies to make opting-out easy; "companies will incur transaction costs in notifying consumers of the existence of the opt-out option and in responding to consumers who opt out."[354]

Indeed, as Sovern notes, the incentive for companies in an opt-out system

---

349. 528 U.S. 32 (1999).

350. *See* CAL. GOV'T CODE § 6254(f)(3) (2000).

351. 528 U.S. at 40.

352. Fenrich, *supra* note 78, at 962-63.

353. *See* GIVENS, *supra* note 48, at 19.

354. Jeff Sovern, *Opting in, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1082 (1999).

may in fact be to make opting-out more difficult for individuals.[355] When companies and websites inform individuals of their ability to opt-out, their privacy policies are often vague, "overloaded" with extraneous information, and difficult to understand.[356] Further, opt-out systems often provide individuals with an all-or-nothing choice: either agree to all forms of information collection and use or to none whatsoever. Such a limited set of choices does not permit individuals to express their preferences accurately. Individuals frequently consent to certain uses of their personal information, but they do not want to relinquish their information for all possible future uses. A more complete range of choices must permit individuals to express their preferences for how information will be protected, how it will be used in the future, and with whom it will be shared.

Thus, providing people with opt-out rights and privacy policies does little to give individuals much control over the information collected and used. Regulation mandating that consumers opt-in rather than opt-out will more effectively control the flow of information between unequal parties. Under a system where individuals opt-in, the default rule is that personal information cannot be collected or used about an individual unless the individual provides consent. As Sovern contends, an opt-in system will place the incentive on entities that use personal information to "make it as easy as possible for consumers to consent to the use of their personal information."[357] Even with an opt-in system, steps must be taken to ensure that consent amounts to more than a "notice and choice" system, which as Marc Rotenberg argues, "imagines the creation of perfect market conditions where consumers are suddenly negotiating over a range of uses for personal information."[358] This problem, which Julie Cohen terms the "privacy-as-choice model"[359] and which Paul Schwartz terms the notion of "privacy-control,"[360] emerges because of information inequalities between individuals and the bureaucracies that collect and use data, and because of an individual's lack of meaningful choices over the uses of her personal information.[361] As Schwartz aptly states: "[W]hen faced with standardized terms, individuals left by privacy-control to fend for themselves will frequently accept whatever industry offers them."[362] Therefore, effective privacy regulation must require an opt-in system which requires a meaningful range of choices as well as addresses inequalities in knowledge and power and other impediments to voluntary and informed

355. *See id*. at 1101.

356. *See id*. at 1085-87.

357. *Id*. at 1118.

358. Rotenberg, *supra* note 368, at 32.

359. *See* Cohen, *supra* note 325, at 1396-99.

360. Paul M. Schwartz, *Internet Privacy and the State*, 32 Conn. L. Rev. 815, 820-27 (2000).

361. *See id*. at 821-24.

362. *Id*. at 822-23.

consent.

Fourth, regulation is necessary to ensure that the private sector undertakes adequate security measures. Although frequently used by companies as passwords for access to sensitive personal records, an individual's Social Security number and mother's maiden name are not always private. Birth records typically contain mothers' maiden names, and they are public in every state. Public records also contain Social Security numbers, such as lawsuit filings, bankruptcy records, death certificates, driving records, and lien documents. Governments are keeping this information public despite the widespread practice of using such information to gain access to other, more personal information. At the same time, governments are not doing anything to regulate what types of information companies can use as security passwords. As a result, there is little security over our personal information—which affects our professions, our finances, and our reputations.

The European Union has taken steps more in line with the view of the database privacy problem in this Article. In 1996, the European Union issued the *European Community Directive on Data Protection*,[363] which outlines the basic principles for privacy legislation for European Union member countries. Although the Directive is far from perfect, it recognizes some of the dimensions of the problem that are neglected by United States' privacy law. For example, Article 15 provides:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[364]

Further, Article 8 prohibits, subject to a number of necessary exceptions, "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[365] The two provisions of the Directive quoted above limit specific uses of information and address the problem of the way personal information is used to make important decisions affecting individual's lives. An exhaustive appraisal of the Directive is beyond the scope of this article, but the Directive contains important differences that should be considered by policy-makers in the United States.[366] The Directive was influenced by the Fair Information Practices developed in 1973 by the United States Department of Health Education and Welfare (HEW). The HEW Code of Fair Information Practices articulated a number of basic information

---

363. See Directive, *supra* note 235, for information on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

364. *Id*. at 236.

365. *Id*. at 232.

366. For a comprehensive analysis of the Directive, see SWIRE & LITAN, *supra* note 235.

privacy principles such as the transparency of personal data record-keeping systems; the right of the individual to access her records and to be informed of the uses of her personal information; the right of individuals to correct erroneous personal information in her records; the duty of entities holding records to ensure the reliability and safety of personal data; and the right of the individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.[367] The Fair Information Practices have, as Marc Rotenberg notes, "played a significant role in framing privacy laws in the United States,"[368] and influenced privacy law around the world. Subsequent sets of information privacy principles, such as those of the Organization of Economic Cooperation and Development (OECD), have expanded the Fair Information Practices.[369] Unfortunately, in the United States the Fair Information Practices have only been selectively incorporated into various statutes in a limited number of contexts. A more comprehensive incorporation of the Fair Information Practices, as developed by HEW and expanded upon by the OECD and the European Union Privacy Directive, would go far towards addressing the privacy problem as I have characterized it.

V. CONCLUSION

I have argued that the problem with databases is one of power and bureaucracy. The implications of this view are that certain solutions which appear adequate when viewed with other understandings of the problem in mind, are inadequate when one understands the problem as I have depicted it. The problem with databases is not our being watched, controlled, or inhibited. Nor is it our lack of ownership in our personal information. Rather, it is a problem that involves power and the effects of our relationship with public and private bureaucracy—our inability to participate meaningfully in the collection and use of our personal information. As a result, we must focus on the structure of power in modern society and how to govern such relationships with bureaucracies. What is missing from the current debate is a focus on the effects of databases on our daily lives—the way that they are changing the way we think, judge, and decide.

Solving the problem requires meaningful limits on how data can be used—limits that are clear rather than ambiguous and amorphous. It involves the basic guarantees to people that their information is being treated thoughtfully, that they are being treated with respect and dignity, that they are informed when they disclose information, and that they have meaningful participation in

---

367. *See* U.S. DEP'T OF HEALTH, EDUC. AND WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTERS, AND RIGHTS OF CITIZENS viii (1973).

368. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1, P44.

369. *See* OECD Privacy Guidelines (1980), *in* MARC ROTENBERG, PRIVACY LAW SOURCEBOOK 1999, at 179 (1999).

the use of the information. This means more than an opt-out system, which requires too much vigilance and effort on the part of consumers and almost always provides them with a limited choice between blocking all uses of the information and enabling the unfettered use of that information. It means that even when information is provided, it is not owned by its corporate collectors for any use they might devise. It means that personal information cannot be bartered and sold like any other commodity.

Too often, commentators and policy makers have been focusing on the wrong evils when addressing the database problem—a focus that has led to more apprehension than action. Today, we are living a precarious existence, at the mercy of impersonal bureaucracies that have an unprecedented amount of power over us. While we fear sinister motives and designs for social control, we neglect to see the harrowing world that is actually being created by the thoughtless and impersonal practices of bureaucracy. That world is not merely a frightening possibility like Big Brother—it is more and more the world we are currently living in.