Washington Law Review

Volume 78 | Number 1

2-1-2003

Recognizing the Societal Value in Information Privacy

James P. Nehf

RECOGNIZING THE SOCIETAL VALUE IN INFORMATION PRIVACY

James P. Nehf*

Abstract: Much has been written about database privacy in the Internet Age, most of it critical of the way in which the American legal system addresses the issue. In this article, Professor Nehf maintains that one of the fundamental difficulties with the public policy debates is that information privacy is often discussed as a typical consumer problem rather than a problem of more general societal concern. As a result, arguments over appropriate resolutions reduce to a balancing of individual rights against more general societal interests, such as increased efficiency in law enforcement, government operations or commercial enterprise. Although privacy scholars discussed the "societal value" of information privacy in the 1960s and early 1970s, the concept was not fully developed. More recently, political theorists have revived the idea and argue the importance of recognizing privacy as a societal norm. Professor Nehf adopts a functional analysis that compares information privacy to other societal values, such as environmental protection, and concludes that privacy policy could take a different form if the issue were viewed in this way.

Information about us—countless bits and bytes[1]—exists in computer databases that are seemingly everywhere. Government records hold our salary histories and track our changes of address, and state motor vehicle departments maintain our driving histories. Much more information is now held in the private sector. It seems that everyone from the local grocery store to GOOGLE.com is collecting information about each of us at every point of contact.

---

* Professor of Law, Cleon H. Foust Fellow, and Director of the European Law Program at Indiana University School of Law, Indianapolis. The author would like to thank Professor Yves Demeer at the Université de Lille II for support on European resource materials, Professor Nicolas Georgakopoulos, law students Melissa Lindley, Anthony Hahn and Liz Parnell, and the faculty at the School of Law at Mercer University for their comments and research support. Special thanks to Indiana University, and the Dean Rusk Center and School of Law at the University of Georgia, for sabbatical support during the research and writing of this article.

1. For most computer users, the terms bit and byte are interchangeable. There is a technical distinction. A bit is simply a binary representation of 0 or 1. In current use, the word byte is a collection of eight bits. The word bit in this context appears to have been a creation of John Tukey, a computer technician who in 1949 was searching for a short term for a "binary digit." Bit (contracted from binary digit) already carried the definition of a "small part." The need for a term representing a collection of bits soon became apparent, since a set of bits was necessary to store, process or transfer any useful character. Although there is some dispute about the origin of "byte," it seems that Werner Bucholz coined the term in the 1950s as a six-bit unit during the development of the IBM "stretch computer." In 1956, the term was used in the development of the IBM System 360 to represent an eight-bit set, and has carried this meaning to the present. According to the Oxford English Dictionary, the word "byte" first appeared in the IBM "systems journal" of 1964. LINDA & ROGER FLAVELL, THE CHRONOLOGY OF WORDS AND PHRASES 246 (1999).

Americans have only the vaguest idea how much of their lives is recorded in databases, and how little control they have over the collection and sharing of that data. People understand that scattered data exist in government and business computers, but they are only beginning to understand the power of information technology, the widespread and fast-growing data aggregation industry, and the harm that can result from information collection and sharing.[2]

Although information about us has been recorded, filed, and manipulated by government authorities and businesses for decades, the database problem took a leap forward with the proliferation of Internet-linked computers[3] in virtually every office and home. As new

2. *See* Jeff Sovern, *Opting in, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1057–63 (1999). Public concern about information privacy has remained consistently high over the last several years. *See* Am. Soc. Newspaper Editors, *at* http://www.epic.org/privacy/survey/ (April 2001) (51% of respondents "very concerned" and 30% "somewhat concerned" that a company might violate their personal privacy); First Amend. Center and Am. Soc. Newspaper Editors Freedom of Info. Comm., Freedom of Information in the Digital Age, *at* http://www.freedomforum.org/publications/first/foi/foiinthedigitalage.pdf (April 2001) (61% of respondents were "very concerned" about "personal privacy," 38% were "more concerned" about personal privacy since they gained access to the Internet); John Schwarz, *Government Is Wary of Tackling Online Privacy*, N.Y. TIMES, Sept. 6, 2001, at C1 (characterizing privacy as one of the most challenging issues for policy makers); Forrester Research, Inc., *Forrester Technographics Finds Online Consumers Fearful Of Privacy Violations* (Oct. 1999) ("Nearly 90% of online consumers want the right to control how their personal information is used after it is collected.") (quoting Christopher M. Kelley, associate analyst in Technographics Data & Analysis), *at* http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html (last visited Jan. 5, 2003); Susan Fox, *Trust and Privacy Online: Why Americans Want To Rewrite The Rules*, THE INTERNET LIFE REPORT, *at* http://www.pewinternet.org/reports/toc.asp?Report=19 (Aug. 20, 2000) (60% of all Americans are "very concerned about privacy"); Electronic Privacy Information Center (EPIC), *Public Opinion on Privacy*, *at* http//:www.epic.org/privacy/survey/ (last updated July 16, 2002) (summarizing a collection of recent survey results).

A 1998 survey showed that 89% of the public was concerned about threats to personal privacy. ALAN F. WESTIN & DANIELLE MAURICI, E-COMMERCE & PRIVACY: WHAT NET USERS WANT 7 (1998). Another survey conducted in the same year found that 88% of consumers were concerned. *See* Executive Summary: 1998 Privacy Concerns & Consumer Choice Survey, *at* http://www.privacyexchange.org/iss/surveys/1298execsum.html (December 15, 1998). *See also* Alan F. Westin, *Whatever Works: The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, Conference Report, DATA PROTECTION IN THE GLOBAL SOCIETY, *available at* http://www.privacyexchange.org/iss/confro/aicgsberlin.html (November 15, 1996); Simson L. Garfinkel, *How Computers Help Target Buyers*, CHRISTIAN SCI. MONITOR, July 25, 1990, at 13 (quoting Bonnie Guiton, Special Advisor for Consumer Affairs to President George Bush: "A major concern of mine is that consumers are uninformed . . . . In most cases, they don't even know that [information on them] is being collected.").

3. Although the word "internet" dates from the late 19th Century (in an 1883 volume of NATURE, an author wrote of "[t]he marvelous maze of internetted motions"), the Internet as we know it began in 1969 when researchers at UCLA, Stanford, UC-Santa Barbara and Utah linked computers to form part of the Advanced Research Projects Agency. Until the early 1980s, however, the users of the

technologies allow businesses and public authorities to collect and process information with increasing speed and sophistication, we can expect the data collection and dissemination problem to become more threatening in the years to come. There is an enormous amount of information about us in other people's hands, and one thing is certain—some of us will be harmed by it. We just don't know who, when, or how badly.

Our perception of the database problem is conflicting and ambiguous because many uses of our information are benign, or even beneficial. Yet, however, other uses (or misuses), such as identity theft, can have devastating consequences.[4] The problem we currently face is thus not merely that a vast amount of information is resting in databases, but that we have very little control over that information—how it is used, shared, and manipulated—once it is "out there."[5] We are at the mercy of those who hold our data.[6] We trust them to guard it and use it in ways that will help and not hurt us.

---

linked computer network were limited to a small number of scientists using large, mainframe computers. As smaller, less expensive computers became available to universities, businesses and individuals, commercial, consumer and academic exploitation of the Internet grew rapidly. Acceptance of the TCP/IP standard language in 1982 accelerated Internet usage, allowing previously incompatible systems to communicate with a common set of protocols. FLAVELL, *supra* note 1, at 255–56.

4. According to the Federal Trade Commission (FTC), identity theft represented 42% of all consumer fraud complaints in 2001, making it the fastest growing category. The FTC Theft Data Clearinghouse received more than 86,000 identity theft complaints in 2001, more than doubling the number from the previous year. *See* Kelly Lucas, *Losing Identity, Saving Face*, 13 IND. LAWYER, July 3–16, 2002, at 9. *See also* the FTC website for identity theft at http//:www.consumer.gov/idtheft/ (last updated Jan. 3, 2003). The identity theft problem hit the front pages in November 2002 when the federal government filed a criminal indictment against several defendants for allegedly stealing the personal, credit and banking information of approximately 30,000 individuals and selling it in a vast criminal conspiracy, resulting in millions of dollars of losses. United States v. Cummings, No. 02 MAG 2354 S.D.N.Y. (Nov. 22, 2002).

5. With modern data processing technology, the original reason for collecting the data becomes irrelevant. Once it has been stored, it can be used or shared in a variety of ways unconnected with the original purpose. *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 711 (1987). According to a study of 1,017 Internet users, 86% of respondents were concerned that personal information about them or their families could end up in the hands of businesses or people they did not know. *See* Fox, *supra* note 2.

6. Disclosure of information can be intentional or accidental, but the potential for injury is the same in either situation. In July 2000, as part of its bankruptcy plan, online toy retailer Toysmart attempted to sell information in its customer list despite language in its privacy policy to the contrary. Greg Sandoval, *Toysmart Creditor Targets Disney in Lawsuit*, CNET News.Com, *at* http://news.cnet.com/news/0-1007-200-2759944.html (Sept. 12, 2000). In April 2000, the DeBeers website, www.adiamondisforever.com, exposed the names, home addresses and e-mail addresses of 35,000 of its customers. *See* Stephanie Olsen, *DeBeers Security Hole Reveals Customer Information*,

Surveys dating from the 1970s show that public support for information privacy has been consistently strong.[7] Americans will not tolerate abuse or misuse of information technology at the expense of their personal privacy, and they overwhelmingly support action to do something about it.[8] Yet survey results also reveal that a great number of us understand that our interests in privacy must be balanced against other interests, i.e., the multitude of benefits resulting from more efficient government, business, and law enforcement functions when information in digital form is readily accessible.[9] Government program administrators can process claims and detect fraud more easily if employment, personal history, and salary data are cross-referenced.[10] Medical treatment can be more effective if physicians have access to our medical histories and prescription records online.[11] Law enforcement can be strengthened if criminal records, employment, education, and immigration data can be accessed, matched, sorted, and correlated more easily.[12] Direct marketing

---

CNET News.Com, *at* http://www.landfield.com/isn/mail-archive/2000/Apr/0000.html (Apr. 4, 2000)). In February 2001, Indiana University accidentally exposed the personal identifying information of thousands of students to a hacker who gained access to university records. *See Hacker Gets Student Data*, CHICAGO TRIBUNE, Feb. 26, 2001, News Section 3.

7. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 60–62 (1995) (discussing polling data from various sources). An October 2000 study at UCLA concluded that almost two-thirds of Internet users and three-fourths of non-Internet users fear that going online endangers their privacy. Reuters, *Web Privacy Tops List of Consumer Concerns*, CNET News.Com, *at* http://news.cnet.com/news/0-1005-200-3293032.html (Oct. 25, 2000). *See also* UCLA Center for Communication Policy, *The UCLA Internet Report: Surveying the Digital Future* at 45, *at* http://www.ccp.ucla.edu/pages/internet-report.asp (October 25, 2000) (discussing concern about privacy of personal data was the number one worry about shopping online).

8. *See supra* note 2.

9. *See* REGAN, *supra* note 7, at 64, 66–67 (discussing responses to survey questions about the need to weigh privacy interests against countervailing interests of government in having access to information).

10. *See* Bowen v. Roy, 476 U.S. 693, 710–11 (1986) (concluding that the use of social security numbers to match database records is the "Federal Government's most cost-effective tool for verification or investigation in the prevention and detection of fraud, waste and abuse").

11. *See* Lawrence O. Gostin, James G. Hodge, Jr., & Mira S. Burghardt, *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule*, 46 ST. LOUIS U. L.J. 5, 6 (2002) (stating "significant benefits may flow from the electronic health information infrastructure," including faster and more accurate diagnoses, increased checks on medical procedures, enhanced public health surveillance, more cost-effective health services, and increased prevention of adverse drug events). In addition, electronic security tools such as personal access codes, encryption programs and audit trails can more efficiently monitor health care fraud and abuse, and protect data from unauthorized uses and disclosures. *Id.*

12. Indeed, the tendency in the past year has favored the strengthening of law enforcement powers at the expense of individual privacy. Shortly after the attacks of September 11, 2001, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272

can be better tailored to individual preferences if our preferences are better known to the marketing organization.[13]

Since there are benefits and risks associated with information collection and data sharing, policy makers must attempt to strike a balance. In doing so, they must first define the problem. This is a critical step in the formulation of public policy because the way in which a problem is defined on the public agenda will affect its ultimate resolution.[14] In the United States, information privacy has historically been defined as an individual concern rather than a general societal value or a public interest problem.[15] This has influenced the resulting public policy solutions, yet it may not be the most effective way to approach modern privacy concerns.

Most consumer problems (e.g., defective goods, unfair trade practices, predatory lending, etc.) are viewed primarily as individual concerns. This means that public policy resolutions are characterized by laws that impose legal obligations on businesses, but injuries are seen as individual in nature (though sometimes aggregated for convenience in a class action). Enforcement largely depends on individuals recognizing an injury and seeking redress when the legal norms are breached. "Lemon Laws" or the consumer credit acts are examples of this regulatory approach. Although there may be important agency oversight (Federal Trade Commission, state attorneys general, or Federal Reserve Board), consumers assume a large responsibility for identifying their own injuries, policing the market by making informed decisions, and enforcing their rights, usually through litigation, when legal norms are breached.[16]

In contrast, when a problem is viewed as a general societal concern, and a resolution in the public interest is sought, enforcement of the legal norm is primarily through government agency oversight and regulation. Resolutions are characterized by the imposition of general standards, reporting requirements, periodic audits, government investigations, and

---

(2001), to aid law enforcement in identifying terrorist activities and other criminal enterprises. Much of the Act seeks to enhance law enforcement efficiencies by expanding government access to financial, student, medical, travel and other records for surveillance purposes. *Id.*

13. *See* Martin Evans, et al., *The Direct Marketing-Direct Consumer Gap: Qualitative Insights*, 4 QUALITATIVE MARKET RESEARCH 17 (2001) (finding ambiguous and conflicting responses of consumers to targeted direct marketing practices).

14. *See* REGAN, *supra* note 7, at xiii.

15. *See* discussion *infra* at Part II.C.

16. *See infra* note 342 and accompanying text.

remedies sought for the general welfare rather than for specific individuals.[17] Moreover, to manage general societal concerns, our elected representatives create a regulatory regime in hopes of minimizing our collective injury before it occurs, not relying as heavily on individual enforcement and compensation for those who are injured by breach of the law.[18] Environmental policy and food and drug laws are illustrative. We do not expect, as the primary control mechanism, individuals to seek redress for injuries resulting from contaminated water or dangerous pharmaceuticals. Although private remedies are an important supplement to the regulatory scheme, a foundation of government regulatory oversight is designed to minimize harm in the first instance.[19]

During the 1960s and 1970s, there was some discussion in debates and commissioned studies about information privacy having a general societal value as well as being a matter of individual concern.[20] Congress ultimately concluded, however, that privacy policy should begin with a voluntary, market-oriented approach, with reliance on individual self-policing as the dominant means of control.[21] Proposals for a federal "Privacy Board," for example, were rejected.[22]

To this day, information privacy legislation in the United States has placed heavy reliance on individuals policing their own data records and protecting their own information from unintended use. For example, the

17. *See generally* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995). *See also infra* notes 334–341.

18. *See* Stephen Breyer, *Analyzing Regulatory Failure: Mismatches, Less Restrictive Alternatives, and Reform*, 92 HARV. L. REV. 549, 556, 560 (1979) (recognizing that government action may be called for when individual use of available remedies is expensive or impractical as an effective means of addressing a problem).

19. *Cf.* Alexander D. Eremia, *When Self-Regulation, Market Forces, and Private Legal Actions Fail: Appropriate Government Regulation and Oversight is Necessary to Ensure Minimum Standards of Quality in Long-Term Health Care*, 11 ANNALS HEALTH L. 93, 104 (2002) ("self-regulation, market forces, and private tort actions all serve important roles in the promotion of quality [long term health care]," yet "long-term care providers have had trouble sustaining quality standards, absent some level of government intervention").

20. *See infra* note 143 and accompanying text. *Cf.* Joseph I. Rosenbaum, *Privacy On the Internet: Whose Information is it Anyway?*, 38 JURIMETRICS J. 565, 566 (1998) (noting that our notion of privacy has been and always will be a moving target, dependent on technological capability, societal values and cultural norms).

21. *See infra* notes 144–57 and accompanying text.

22. *See* UNITED STATES SENATE COMMITTEE ON GOVERNMENT OPERATIONS, PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE, AND DISCLOSURE OF INFORMATION, S. REP. NO. 93-1183, at 26 (1974). *See generally, infra* notes 171–200 and accompanying text.

Fair Credit Reporting Act of 1970 (FCRA)[23] imposes limits on the collection and sharing of credit histories by credit bureaus. Success of the FCRA depends largely on individuals monitoring compliance by keeping their credit reports complete and accurate. More recently, the Gramm-Leach-Bliley Act of 1999[24] imposes limitations on the sharing of information in the financial services industry. The Gramm-Leach-Bliley Act allows affiliated companies to share data among each other and requires individuals to take affirmative action to prevent data sharing outside the affiliated group (so-called "opt out" legislation).[25]

This article argues that, in the modern digital world, information privacy should be viewed as a societal value justifying a resolution in the public interest, much like environmental policy and other societal concerns, with less emphasis on individual self-policing and market-based mechanisms. In doing so, this article does not invoke abstract notions of natural rights, fundamental values, or the preservation of human dignity, as other defenders of privacy protection have argued in recent years.[26] Its point is more functional and pragmatic. If we look at the way in which information is collected and used in today's society, we see that the problems presented are not typical consumer issues that we can expect individuals to police for themselves with the aid of prohibitory laws. The policy issues have much more in common with societal problems that we have historically regulated in a fundamentally different way. Policy makers should recognize this relationship in the formulation of privacy legislation and create a regulatory environment that provides meaningful protection of our collective privacy interests.

Part I discusses the reasons why we have difficulty thinking about information privacy as a public policy issue, and concludes that we are only beginning to focus on the most troubling aspect of the problem—lack of control over our information once it has been revealed or

---

23. 15 U.S.C. § 1681 (2000); *see also generally* UNITED STATES SENATE COMMITTEE ON GOVERNMENT OPERATIONS, *supra* note 22.

24. 15 U.S.C. §§ 6801–6827.

25. *Id.* § 6802.

26. *See, e.g.*, Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2393 (1996) (discussing the economic implications of treating personal information as a property right); Glenn Negley, *Philosophical Views on the Value of Privacy*, 31 LAW & CONTEMP. PROBS. 319, 320 (1966) (modern thinkers have proposed and now reject the idea that privacy is a "natural right"); Moore v. City of East Cleveland, 431 U.S. 494, 503–05 (1977) (noting privacy is a basic value, part of the nation's history and traditions); Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1000–07 (1964). *See also infra* at Part III.A.

gathered. Part II examines the origins of privacy law in the United States that resulted in our treating information privacy as a problem of individual, rather than societal, concern. The principle control mechanisms—a combination of self-regulation, individual self-policing, and market-driven controls—are a natural consequence of this conception of privacy, and they are unlikely to produce the degree of privacy protection that most Americans deserve and expect. Part III makes a case for viewing information privacy as a more general societal concern justifying a higher level of protection (or at least a different way of seeking public policy resolutions). This Article concludes that regulation similar to the European model of privacy protection, in which the issue is framed as a foundation of social protection, should prevail in the United States.

I. CONCEPTUALIZING THE DATABASE PRIVACY PROBLEM

A. Why Does Data Collection Bother Us?

Public concern about information collection and storage is an ancient problem. In the 11th century, William the Conqueror compiled a "Doomsday" survey, which collected information on each of his English subjects, ostensibly for taxation and other state purposes.[27] For centuries thereafter, government authorities and commercial enterprises have collected, organized, and shared information about the general population or certain segments of it. Only recently, however, have new information technologies amplified the problem to an unprecedented degree.

Technology usually enables and empowers people to perform tasks that they could not previously perform, thus producing many benefits to individuals and society at large. Yet technological developments can also introduce previously unknown problems. For example, the printing press allowed information to spread rapidly among the citizenry and undermined the authority of those who previously controlled its

27. REGAN, *supra* note 7, at 69. The people of England referred to William's survey as the Domesday book, a Middle English spelling of doomsday. The root "dōm" meant "law or decree" during this period but it could also mean "judgment, sentence or condemnation." *See* FLAVELL, *supra* note 1, at 30. Historical evidence suggests that William's subjects probably were not concerned about the Doomsday book infringing on their privacy, since privacy as a societal concern developed centuries later. *See* FERNAND BRAUDEL, CAPITALISM AND MATERIAL LIFE, 1400–1800, 224 (1973) (describing the idea of privacy as an "an eighteenth century innovation").

dissemination. Yet the press could be censored, misinformation could be spread, and publications could be used to expose damaging facts or spread rumors about a person to a wider audience than was previously possible. The telephone opened communication links to the world, but phone lines could be tapped or recorded, calling records traced, and personal information revealed. Radio and television have been powerful instruments for education and information sharing, but also can be used for manipulation, pacification, and political propaganda.[28]

Today's information technologies present tradeoffs as well. While some individuals object to the collection and distribution of personal information for virtually all purposes,[29] most recognize and appreciate the many benefits of data storage and information sharing technologies. We appreciate the efficiencies brought about by the revolution in information processing, but we are concerned about how personal information might be used. We may not care if a grocery store computer "knows" that a woman buys three bottles of wine and a carton of cigarettes each week if the store uses the information to send her some useful discount coupons. However, most of us would object if the store

---

28. *See generally* RONALD J. DEIBERT, PARCHMENT, PRINTING, AND HYPERMEDIA: COMMUNICATIONS IN WORLD ORDER TRANSFORMATION 47–110 (1997).

29. *See* Fox, *supra* note 2 (stating that 27% of Internet users are "hard-core privacy protectionists" that would never provide personal information, 10% would be willing to provide it under the right circumstances, and 54% of Internet users have provided personal information in order to use a Web site). Alan Westin divided the American public into three groups regarding attitudes towards privacy:

> "Fundamentalists," about twenty-five percent of the American public, who rate privacy as an extremely high value, are loathe to trade this for promised benefits to them or to society, and generally favor legislative standards and government regulation.
>
> At the opposite pole are the "privacy unconcerned," about twenty percent of the American public, who are generally ready to give personal information about themselves in order to get consumer benefits and support government programs, and are not at all worried about intrusiveness.
>
> This leaves the "privacy pragmatists," fifty-five percent of the American public and clearly the "swing group" in setting public norms. The pragmatists are willing to listen to possible benefits to them or to society from disclosing their personal information and weigh those values against the important privacy interests involved. If they feel the benefits are meaningful, they next look for meaningful safeguards—basically, the fair information practices elements—and decide whether they trust these to be provided by private standards or whether they feel laws are needed. Whether private standards are accepted generally depends on the trust the public has in particular industries or government agencies to handle their information in a responsible way.

Alan F. Westin, *Whatever Works: The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, Conference Report, DATA PROTECTION IN THE GLOBAL SOCIETY, *available at* http://www.privacyexchange.org/iss/confro/aicgsberlin.html (November 15, 1996).

gives or sells that information to a health insurance company for purposes of evaluating her insurable risk. We may not mind that a dinner guest can log onto Anywho.com and get a map to our home or office simply by inputting a last name and home town. Yet we likely would not feel the same about a stranger who overheard a young girl's name in a casual conversation at the shopping mall.

Because of these concerns about how personal information is used, the most often quoted definition of database privacy is "the right to *control* information about ourselves."[30] The lack of control over information has long been a concern of privacy advocates. Many have invoked the "Big Brother" metaphor from George Orwell's novel *1984* to describe the threat to privacy that databases present.[31] Orwell's fictional citizenry feared the totalitarian government in part because they lost control over vast amounts of personal information that Big Brother had collected, and

30. *See, e.g.*, Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2120 (2001) (discussing privacy in terms of the "ability to exercise control over personal information"). One of the first to discuss information privacy in these terms was Charles Fried, in *Privacy*, 77 YALE L.J. 475, 482 (1968) (discussing information privacy as "the *control* we have over information about ourselves") (emphasis in original). Privacy has been defined in various other ways. *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS AND THE RISE OF TECHNOLOGY 58 (1997) ("whatever is not generally . . . a legitimate concern of others"); THOMAS M. COOLEY, THE LAW OF TORTS 29 (1888) (defining privacy as the "right to be let alone"); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980) ("limitation of others' access to any individual").

31. The list of writers who have invoked the "Big Brother" metaphor in privacy literature is endless. *See, e.g.*, REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 160 (1999) (chapter titled "Big Brother Outsourced: The Globalized Panopticon"); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1396 (2001) ("[c]ommentators have adapted the Big Brother metaphor to describe the threat to privacy"); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000) (noting that at least since George Orwell's 1984, the image of the all-seeing eye has been synonymous with the power to exercise repression); 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) ("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"); 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) ("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."); Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values*, 72 CHI.-KENT L. REV. 271, 273 (1996) (expressing skeptisism that the creation of government data protection boards would be like "calling on 'Big Brother' to protect citizens from 'Big Brother'"). *See also* McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998) ("[i]n these days of 'big brother,' where through technology or otherwise the privacy of individuals from all walks of life are being ignored or marginalized").

they feared how it might be used against them.[32] Since Orwell's Big Brother was a pervasive government surveillance mechanism, writers have sometimes referred to private sector databases as an amalgamation of "Little Brothers" or similar metaphors that invoke the same overpowering surveillance concern.[33]

Along the same lines, writers in recent times have reached further back in literary history to recall Jeremy Bentham's horrific "Panopticon" vision,[34] which describes the ultimate utilitarian prison that consisted of a central watchtower surrounded by a multi-storied ring of prison cells. The inner wall of each cell is a clear window, floor to ceiling, facing the watchtower. Each prisoner is completely exposed through the window twenty-four hours a day, so a single guard in the watchtower can see every movement.[35] Just knowing that one *could* be observed, a prisoner would behave in accordance with the expected norm.[36] A modern variant of the Panopticon vision is the "nannycam," a surveillance product marketed to anxious parents who want their child care provider to know that his or her every move is being monitored and recorded.[37]

---

32. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1101–02 (2002) (citing Margaret Raymond, *Rejecting Totalitarianism: Translating the Guarantees of Constitutional Criminal Procedure*, 76 N.C. L. REV. 1193, 1198 (1998) (noting that throughout history, totalitarian governments have instilled fear by creating elaborate systems for collecting data about people's private lives).

33. *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. L.J. 357, 377 (2000); Marsha Morrow McLaughlin & Suzanne Vaupel, *Constitutional Right of Privacy and Investigative Consumer Reports: Little Brother is Watching You*, 2 HASTINGS CONST. L.Q. 773, 776 (1975).

34. JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovi ed., 1995). *See* WHITAKER, *supra* note 31, at 32–33 ("The image of the Panopticon permeates all contemporary discussions of surveillance."); DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 62 (1994); OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); Solove, *Privacy and Power*, *supra* note 31, at 1415–16.

35. The Panopticon metaphor in modern privacy literature is invoked almost as frequently as Big Brother. *See, e.g.*, Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, n.111 (2002); Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 28 (1995).

36. *See* WHITAKER, *supra* note 31, at 32; Michel Foucault, *Surveiller et Punir: Naissance de la Prison*, *in* DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., 1979); Solove, *Privacy and Power*, *supra* note 31, at 1415 (discussing Foucault's description and observing that the Panopticon is "so efficient that nobody needs to be in the tower at all").

37. *See* WHITAKER, *supra* note 31, at 80–81 (1999).

One difference between modern "dataveillance" and the pervasive observation of the Orwellian and Panopticon worlds is that we are "watched" not through a camera or guard tower, but by a computer collecting facts and data.[38] The effect on human behavior may be similar, however. Data collection can restrain our free will.[39] We experience this in everyday life. Parents of a teenage child may assume that if they learn a lot about their child's behavior, living habits, and activities, and the child knows about the continual observation, the child is more likely to obey the rules of the house. Workers whose telephone calls are monitored may make fewer personal calls on the job. The database problem can thus be viewed as a shifting in the balance of power from the individual to the entities that collect and control information about us.[40] Viewed in this way, the problem with databases is similar to the surveillance of Big Brother or the Panopticon. Databases are a form of observation that curtails individual freedom and enhances the power employers, governments, insurance companies, and others have (or hold) over our lives.

Yet as Daniel Solove observed, Big Brother, Panopticon, and other surveillance metaphors do not entirely capture the current concern with database technologies.[41] Orwell's Big Brother and Bentham's Panopticon demanded obedience from their subjects and sought to control important aspects of their behavior. The goal was conformity and discipline. Through continual surveillance, the technologies policed individuals to the point where individualism would be suppressed. By constantly living under the possibility that one could be observed at any time, people would do what authorities wanted them to do.

The collection of information in cyberspace can only roughly be analogized to the Orwellian or Panopticon worlds. As we apply for jobs or government benefits or surf the Internet information about us is collected.[42] We are being watched in a sense, and we do not know

38. *See* Roger Clarke, *Information Technology and Dataveillance* 3, *at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html (Nov. 1987).

39. *See* Paul M. Schwartz, *supra* note 17, at 560.

40. *See* Rosa Ehrenreich, *Privacy and Power*, 89 GEO. L. J. 2047, 2053 (2001) ("[W]hat certainly *should* bother us [about data collection] and confidentiality has a great deal to do with power. More specifically, what should bother us are balances of power that are damaging or inequitable.").

41. Solove, *supra* note 31, at 1422.

42. *See* Rosenbaum, *supra* note 20, at 571 ("Individuals cruising on the information highways often are blind to the electronic footprints they leave. Every post to a bulletin board, every electronic message, every Web page accessed and item purchased can be monitored and tracked."); *see also infra* notes 69–81.

precisely when or to what extent. But for the most part we are not being observed by anyone who has any interest in controlling our behavior, minimizing individualism, or keeping us from uprising against authoritarian power. With the exception of FBI-type of law enforcement surveillance, an issue outside the scope of this Article, the people collecting and sharing information today are usually just looking for better and more efficient ways to run their businesses or government departments or to market their goods or services.[43] Motives are largely benign, or at worst greedy.

Solove argues that the database problem is better captured by Franz Kafka's depiction of prosecutorial bureaucracy in *The Trial*.[44] The protagonist, Joseph K, is arrested yet never told what crime he is accused of committing. The novel is an anxiety-ridden nightmare during which nameless authorities actually do little to Joseph K, although he is constantly fearful of what they might do. He feels powerless to find answers or participate meaningfully in the bureaucratic process. Joseph K becomes obsessed with his predicament. He wants the court to treat him like an individual and he wants the case to reach finality. However, he does not know who has information about him, what that information is, or how it might be used.[45]

The Trial captures the sense of helplessness and vulnerability we may experience when large bureaucratic organizations—or a multitude of smaller, private ones—collect information about us and possess the power to use it against our interests.[46] Governments, employers, and businesses continually make decisions based on our data, and we may

---

43. Joel Reidenberg, Jennifer Barrett, Evan Hendricks, Solveig Singleton, and David Sobel, *Panel II: The Conflict Between Commercial Speech and Legislation Governing the Commercialization of Private Sector Data*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 59, 67 (2000) (noting that the collection and storage of personal information about consumers is a means that businesses use to improve the relationship they have with these very consumers); Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 648 (2000) (the primary use of personal data is marketing).

44. *See* Solove, *supra* note 31, at 1419–23.

45. *See* FRANZ KAFKA, THE TRIAL: A NEW TRANSLATION BASED ON THE RESTORED TEXT 35–54 (Breon Mitchell trans., 1999).

46. The Kafka metaphor was invoked recently by a public university professor whose e-mails were read by university administrative officials pursuant to a state "open door" law that considered e-mail to be a public record. "I felt like a person in a Kafka novel," the professor lamented after witnessing the perusal of his private messages by school administrators. *See* Andrea L. Foster, *Your E-Mail Message to a Colleague Could Be Tomorrow's Headline*, CHRONICLE OF HIGHER EDUCATION, *available at* http://chronicle.com/free/v48/i41/41a03101.htm (June 21, 2002).

have no knowledge of the process or an ability to challenge outcomes.[47] Like Joseph K, we might not even know if and when important decisions are being made. We are at the mercy of an unknowable digitized process—a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of information that can cause them harm.

Yet *The Trial* metaphor also fails to describe the modern database problem as most of us perceive it because, unlike Joseph K, we voluntarily participate in the data collection system because we see benefits from participating. My son cannot get a job unless he fills out an application form. I do not receive discounts from the grocery store unless I use the store "convenience" card. My research assistant cannot get information from a web site without divulging some personal information. None of us can get money from the ATM without leaving footprints that reveal where we were and what we were doing at that point in time. We cannot use a credit card on line to avoid the shopping mall traffic without transmitting a name and card number. We are not coerced but *seduced* to reveal personal information by the pleasures we derive from living in the modern world and consuming the goods and services that others offer. A better literary metaphor would be from the story *Hansel and Gretel*.[48] We are happily eating all the cookies, candy, and gingerbread, enjoying what we think are the benefits of sharing personal bytes of data in the information society. As we do so, we may be fattening ourselves for someone else's feast, unaware of the fate that may await us.

---

47. *See* Froomkin, *supra* note 31, at 1463 (employers continually seek new ways to monitor employees for efficiency and honesty; businesses search databases for information about new customers); Mary W.S. Wong, *Electronic Surveillance and Privacy in the United States After September 11 2001: The USA Patriot Act*, 2002 SING. J. LEGAL STUD. 214, n.142 and accompanying text (noting that one criticism of the FBI's e-mail reviewing software program, the Carnivore system (referred to as "DCS 1000" by the FBI), is that the FBI does not disclose details about how the system works).

48. The Brothers Grimm, *Hansel and Gretel* (1889), *reprinted in* THE BLUE FAIRY BOOK (Andrew Lang ed., 1965). Along the same lines, see Pamela Paul, *What Are Americans Afraid Of? Mixed Signals; When It Comes to Issues of Privacy, Consumers Are Fraught With Contradictions*, AM. DEMOGRAPHICS 46 (July 2001) (using "big bad wolf" as a metaphor for information privacy invasion). *See generally*, FRED H. CATE, PRIVACY IN THE INFORMATION AGE 30–31 (1997) (noting that this tradeoff is not limited to Internet use: "Instant credit, better targeted mass mailings, lower insurance rates, faster service when ordering merchandise by telephone, special recognition for frequent travelers, and countless other benefits come only at the expense of some degree of privacy.").

There is another difference with database surveillance. Since marketers and other users of databases generally are interested in aggregating data and selling products or services, they do not usually care much about snooping into the private lives of particular individuals. We are being watched not by other humans, but by machines, which gather information, compute profiles, and generate lists for postal delivery, e-mailing, or phone solicitations. This impersonality makes the surveillance seem less personally invasive than the leering of a "Peeping Tom," an FBI wiretap, or Aunt Edna looking at your credit card bill when she stops by for a visit. A large portion of our personal information involves facts that are hardly embarrassing at all: our financial information, race, marital status, hobbies, occupation, and the like.

Indeed, most information collected about us in cyberspace concerns relatively innocuous and boring facts and details. Even so, there is a real and justified concern about how even this seemingly innocent information might be used in ways we would not prefer. We hope that our data will be accurate, complete, relevant, and current in every database in which it resides. We want the data used only for the right purposes (those to which we consent or would consent if asked), and which are permitted by law. We want it used by the right people (those who need to use the data for permissible purposes), and by no others. If any of these conditions is missing, we feel that important rights and interests have been jeopardized.[49] Privacy literature is sprinkled with horror stories about inaccurate, incomplete, irrelevant, or derogatory information in files, and unauthorized access to files containing information that can be dangerous in the wrong person's hands.[50] The

---

49. *See* PAUL SIEGHART, PRIVACY AND COMPUTERS 76 (1976) (referring to this as the "instrumental" value in privacy protection); COLIN J. BENNETT, REGULATING PRIVACY 33–35 (1992).

50. *See, e.g.*, William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, n.24 (2001) (citing McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998) (refrencing homosexual sailor who discussed his sexual orientation in a seemingly anonymous online profile, only to have it revealed to his military superiors, who commenced discharge proceedings)). For additional illustrations, see Margot Williams & Robert O'Harrow, Jr., *Online Searches Fill in Many Holes*, WASH. POST, Mar. 8, 1998, at A19, reporting on free web service that found consumer's address, phone number, names, and addresses of 20 neighbors, and provided map and directions to consumer's home; another service provided for $9.50 consumer's previous addresses and for $12.00 consumer's Social Security number and birthday; another service provided driving record for $15.50. In a 1999 article, Jeff Sovern warned about the types of lists that are for sale, including: lists of people who have bought skimpy swimwear; college students sorted by major, class year, and tuition payment; millionaires and their neighbors; people who have lost loved ones; men who have bought fashion underwear; women who have bought wigs; callers to a 900-number national dating service; rocket scientists; children who have subscribed to magazines or have sent in

reason data collection bothers us is not complicated: we live in fear that we may be the next storyline.

B. Evolution of the Database

Our fears are heightened by a vague awareness of the absolute enormity of information residing in databases. Federal agencies alone control hundreds of databases on immigration, bankruptcy, Social Security histories, military personnel, and countless other subjects of legitimate government activity.[51] The federal government has a database containing the Social Security numbers, addresses, and wages of nearly everyone who obtains a job in the United States.[52] State governments keep digitized records on prescription drug purchases, automobile ownership, car insurance, births, criminal records, marital status, real estate holdings, liens and easements, voter registration, worker compensation claims, and many other aspects of our lives that are recorded, stored, and sorted.[53] Licensing offices keep records on a variety of occupations from bail bondsmen to beauticians.[54] Federal and state governments are encouraged to seek new, more efficient ways of integrating and aggregating these databases to serve their public mandates, but we can never be sure who has access to all of that information, and whether adequate security procedures are in place to guard it from theft, sale, or unauthorized use.

---

rebate forms included with toys; people who have had their urine tested; medical malpractice plaintiffs; workers' compensation claimants; people who have been arrested; impotent middle-aged men; epileptics; people with bladder-control problems; buyers of hair removal products or tooth whiteners; people with bleeding gums; high-risk gamblers; people who have been rejected for bank cards; and tenants who have sued landlords. Sovern, *supra* note 2, at 1034.

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

52. *See* 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.

53. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

54. States are also creating an increasing number of DNA databases. *See* Amy Argetsinger & Craig Whitlock, *Maryland Seeks the DNA of Violent Criminals: Critics Cite Threat to Privacy Rights*, WASH. POST, Mar. 24, 1999, at B1. States had intended to use DNA to track sexual offenders, but some are expanding their databases to include genetic information on other felons. *Id.* The Department of Defense established a DNA database to identify remains of soldiers. CHARLES J. SYKES, THE END OF PRIVACY 128 (1999). Iceland made headlines by selling the genetic information of the general population to a biotech company. 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. *See* Solove, *supra* note 31, at 1403.

Although the build up of government databases has been extraordinary, the most revolutionary developments have occurred in the direct marketing industry and the private sector trade in personal information. This is where the "information superhighway"[55] merges into the Autobahn,[56] and where the speed is limited only by the power of the data processing machines driving it. As computers, software and data manipulation methodologies grow more powerful and sophisticated, data collection in the private sector will be an increasingly dangerous threat to information privacy interests.

Direct marketing to individuals was an inefficient and comparatively costly business practice for most of the twentieth century.[57] One of the reasons for its slow development was the low response rate compared to the cost of compiling contact lists, printing and mailing solicitation letters, and hiring workers to make individual contacts by phone.[58] To increase positive response rates, marketers realized that they needed to target their customers more accurately. Firms began compiling research on consumer preferences in various geographic areas and devising ways to analyze, sort, and use the collected data more effectively.[59]

Improvements in direct marketing were aided by the federal government. When the postal service began using the five-digit zip code in the 1960s, direct marketers began grouping consumers by zip code to

---

55. Most sources credit former Vice-President Albert Gore for coining the term "information superhighway" in a 1994 speech. *See* ComputerHope.com Online Dictionary, *at* http://www.xmission.com/~comphope/jargon/i/infosupe.htm (last visited Jan. 20, 2003) (defining "information superhighway" as a term coined by Vice President Gore when giving a speech January 11, 1994).

56. *See* Ronald J. Krotoszynski, Jr., *Identity, Privacy, and the New Information Scalpers: Recalibrating the Rules of the Road in the Age of the Infobahn: A Response to Fred H. Cate*, 33 IND. L. REV. 233, 251 (1999).

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

58. *See* Solove, *supra* note 31, at 1405–06; Sovern, *supra* note 2, at 1046–47; Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 364 (2000) (noting that an important cost of marketing activity is the time and inconvenience suffered by consumers, particularly those who never requested the information); *cf.* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 337–39 (2001) (stating e-mail "spammers," unlike senders of traditional non-electronic communications, have little incentive to compare the expected benefits of the communication against the cost, as the cost of sending unsolicited bulk e-mail is negligible).

59. *See* Solove, *supra* note 31, at 1405.

determine the best areas to target particular product lines.[60] Sorting data by zip codes proved to be a rough but inexpensive way to reach certain demographic subgroups.[61] A decade later, the government began selling census data in electronic form. In an effort to protect the privacy in individuals identified in the census, the Census Bureau sold the information in bundles of several hundred households, providing addresses but not names.[62] Businesses reattached many of the names, however, by matching census addresses to addresses in telephone directories and other databases such as voter registration lists. As a result of these and other developments, by the early 1990s consumers on average were included in nearly one hundred mailing lists, and the number was growing at a rapid pace.[63]

Cyberspace technologies and the widespread use of the Internet profoundly affected the data collection business by the late 1990s. Government agencies placed individual records on their websites, although this practice is now receding due to public complaints about the disclosure.[64] These government-held records used to be maintained in filing cabinets physically scattered in offices across the country. As a legal matter, these records were available to the public, but as a practical matter they were accessible only to local authorities and the occasional news reporter or ardent researcher. Now many of these records can be searched by anyone with a personal computer and some basic instructions on the system's search logic.[65] To make searching for personal information even easier, several Internet websites collect and

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

61. Solove, *supra* note 31, at 1405–06; Douglas A. Kysar, *Kids & Cul-De-Sacs: Census 2000 and the Reproduction of Consumer Culture*, 87 CORNELL L. REV. 853, 875–77 (2002) (book review).

62. SHAVER, *supra* note 60, at 29–32.

63. *See* ANN WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 11 (1994); Solove, *supra* note 31, at 1408.

64. William Matthews, *Access Denied*, FEDERAL COMPUTER WEEK, *at* http://www.fcw.com/fcw/articles/2000/0529/cov-access-05-29-00.asp (May 29, 2000) ("Information once eagerly posted on government Web sites to promote environmental safety, assist military personnel or help retirees is now being viewed as dangerous if found by terrorists, hackers and other criminals. . . . [A]gencies and Congress are tightening controls over federal Internet sites. Federal Webmasters who once enthusiastically posted information now anxiously take some of it down.").

65. *See* Solove, *supra* note 53, at 1139; Steven C. Carlson & Ernest D. Miller, Comment, *Public Data and Personal Privacy*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 83, 84 (1999) (warning that federal, state, and local governments are currently pursuing ambitious programs to upgrade and integrate their information technology systems into unified data networks, making vast holdings of data far more accessible to government officials and to the general public).

compile public records from across the country and sell it online from a single source.[66]

Currently, most personal information in cyberspace is collected in one of two ways. An organization may directly solicit and collect information from individuals who contact the organization and provide information voluntarily.[67] Alternatively, and increasingly more common, the organization might surreptitiously track and record individual's surfing activity on the Internet.[68]

Direct solicitation of information has been with us for years in various forms. We have all completed job or credit applications or filled in surveys. Many consumers have completed and returned "warranty registration" cards to the manufacturer, which volunteer valuable data that can be used for marketing purposes.[69] In the modern age, more information is directly solicited online as an increasing number of websites require registration and the disclosure of personal information before a user can access the site's content. Amazon.com, for example, uses registration information to help keep track of its customers' purchases of books, CDs, electronics, toys, and other items.[70]

---

66. KnowX.com and Locateme.com, for example, sell information on airplane ownership, court filings, death certificates, pilot licenses, judgments, liens, professional licenses, foreclosures, refinancings, driver and voter registrations, and credit "headers" (part of a credit report), *at* http://www.knowx.com (last visited Jan. 20, 2003); http://www.locateme.com (last visited Jan. 20, 2003). Focus USA claims to have information on 203 million people and offers demographic lists such as "Tech-Savvy Hispanics," "Big-Spending Parents," "Proven Patriots," "Rural Riches," and "Pet Lovers Online." *See* http://www.focus-usa-1.com/lists_az.html (last visted Jan. 20, 2003). *See generally* Solove, *supra* note 31, at 1409.

67. *See* Solove, *supra* note 32, at 1094 (noting that Web sites collect data when people fill out online questionnaires pertaining to their hobbies, health, and interests).

68. *See* Joel Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 201–02 (1992).

69. Warranty registration cards for many products ask a host of lifestyle questions in addition to product-related queries. Other surveys are more direct. The author received a mailing called the "Consumer Product Survey of America" asking the "main grocery shopper in your household" to fill out the form and mail it. The questionnaire asked dozens of questions ranging from the kind of bladder-leakage products used to the name of the consumer's auto insurance company. It also asked for name, home address, phone numbers and e-mail addresses. *See* Letter from Laura David, Shopper's Voice, Consumer Product Survey of America (undated) (original on file with author).

70. Andrew Shen, *Online Profiling Project*, EPIC, *at* http://www.epic.org/privacy/internet/Online_Profiling_Workshop.PDF (last visited Dec. 17, 2002) (citing an article from *The Economist* in which Jeff Bezos, CEO of Amazon.com, describes Amazon as an "information broker", acting as the connection between consumers looking for books and publishers looking for consumers; according to Bezos, Amazon's vast database of customers' preferences and buying patterns is tied to their e-mail and postal addresses); Alan Murray, *Net Effect: Is Service Getting Too Personal?*, WALL ST. J., July 19, 1999, at A1. "[T]he next wave of Internet innovation is in the area of personalized marketing and services. Companies such as

Surreptitious collection of information from web users is even more common. Many websites secretly track a customer's surfing practices through the use of "cookies" and similar technologies.[71] When a user explores a site, the user leaves electronic footprints behind. By following the footprints, the site can record information about the user, such as the Internet service provider used, and the type of hardware and software the user employed. The site can also record some behavioral information about the user's Internet habits, such as the website previously visited, the amount of time spent on each web page, and the length of time spent visiting different parts of the site.[72]

To make this information more useful, the web site might connect the "clickstream" data to particular Internet users.[73] This can be done by either requiring users to register or branding them with cookies that will report identifying information back to the website the next time the user visits.[74] Using either method, the site can compile a profile of individual

---

Amazon.com are eagerly assembling and sorting massive amounts of information on customer preferences. Their aim is to know what book, record or other product you want before you know it, and then market it directly to you.").

71. A "cookie" is a small file of codes that is dispatched to a user's computer when a web page is viewed. The site puts an identification mark in the file, and the cookie is stored on the user's hard drive. When the user visits the site again, the site locates the cookie and matches the file code with information previously collected about the user's surfing activity. While privacy advocates object to the use of cookies, the problem with banning them is that they have practical uses other than secretly collecting information about surfing activity. They can store passwords, for example, which speeds access to frequently used websites. *See generally* Viktor Mayer-Schönberger, *The Internet and Privacy Legislation: Cookies for a Treat?*, 1 W. VA. J.L. & TECH. 1.1 (1997) (discussing cookie technology and its impacts on privacy); Lori Eichelberger, *The Cookie Controversy*, COOKIE CENTRAL, *at* http://www.cookiecentral.com/ccstory/cc2.htm (Apr. 8, 1998).

Indeed, the much maligned cookie can even enhance online privacy. The electronics retailer Future Shop switched to the use of cookies on its site in November 2000 after learning that unauthorized people could log on and view other customers' names, addresses, phone numbers, and possibly credit card numbers. The company claimed that cookie technology would have prevented a breach of security and an invasion of privacy. *See* Future Shop Homepage, *at* http://www.futureshop.ca (last visited Jan. 20, 2003); T. Hamilton, *Price Snafu Stings Web Retailer*, THE TORONTO STAR Nov. 17, 2000, at C01.

72. *See* Solove, *supra* note 31, at 1411.

73. Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 559 (1999) (explaining "clickstream" data are series of detailed transactional information that improve targeted online advertising; some firms, such as Adfinity, combine clickstream data, or "mouse-droppings," with personal information collected from other sources to create profiles of a person's Web browsing behavior).

74. *See supra* note 71. Internet users usually associate clickstream and cookie technology with private sector websites, but they have been frequently used in government websites as well. Despite a ban on federal government use of these information gathering tools, a survey in October 2000 found cookies in use in 11 of 65 government websites, 3 of them passing information to third parties without the permission of users. *See* Ronna Abramson, *Federal Agencies Caught With Hand in the*

interests, concerns, and general web surfing habits.[75] Savvy online marketing firms can even draw inferences about how we respond to web page presentations. For example, an online travel service could keep track of every destination to which a person requested a fare or every city in which hotel information was sought.[76] A medical information site could track the number of times a user linked to pages providing information on osteopathic remedies. Clickstream data can thus reveal lots of useful marketing information about all who use the Internet.

Another form of user-tracking technology is the "web bug," also known as a web beacon or clear graphic image file (GIF) tag. Web bugs are image files secretly imbedded in a web page and are invisible to the person browsing the page.[77] The bug sends information about the user's browsing habits and interaction with the page back to the home server. Internet advertisers also can capture the search terms a person uses to find web sites on a subject of interest. The process, known as "banner ad leakage," allows an advertiser to record search terms as the user submits them to the search engine.[78] Banner ad leakage allows the advertiser to collect an enormous amount of potential marketing data and to tailor ads

---

Cookie Jar, THE STANDARD, *available at* http://www.thestandard.com/article/display/0,1151,19600,00.html (Oct. 23, 2000); *Associated Press, Study: Government Web Sites Track Users*, NYTIMES.com, *available at* http:www.nytimes.com/aponline/technology/AP-Internet-Privacy.html (Oct. 21, 2000); John B. Kennedy & Mathew H. Meade, *Privacy Policies and Fair Information Practices: A Look at Current Issues Regarding Online Consumer Privacy and Business Practices*, 632A PLI/Pat 321 (June 2001). Privacy policies of data collectors may openly acknowledge that they collect information via cookie or clickstream technology. *See, e.g.*, GAP Credit Card, "Our Privacy Commitment," Monogram Credit Card Bank of Georgia, PRIV-GAP [92391GA] 01/01 (on file with author).

75. *See* Steven J. Barber & Jennifer Quinn-Barabanov, *Statutory and Common Law Theories Asserted by Plaintiffs in Online Privacy Cases*, 5 INTERNET NEWSL. 1 (Aug. 2001).

76. *See* Solove, *supra* note 31, at 1412.

77. A web bug is invisible because it is only one pixel square in size and blends into the background on a web page or HTML e-mail message. The only way to detect a web bug is to locate the source code for the web page or e-mail message and discover that the web bug image comes from a different server than everything else. The server sending the bug might belong to an advertising network that uses it to obtain information, including the Internet Protocol (IP) address of the computer that accepted the web bug, the URL of the page on which the web bug appears, the time the web bug was viewed, the type of browser that accepted the web bug image, and any previously set cookie data. (The cookie can link the bug and the information it has obtained back to the online profile associated with that cookie.) Web bugs are common in HTML e-mail and are used to tell if an e-mail has been read or forwarded to another person. *See* R. Smith, *FAQ: Web Bugs*, *at* http://www.privacyfoundation.org/resources/webbug.asp (last visited Jan. 20, 2003); Robert O'Harrow Jr., *Fearing a Plague of 'Web Bugs': Invisible Fact-Gathering Code Raises Privacy Concerns*, WASH. POST, Nov. 13, 1999, at E01.

78. *See* Barber & Quinn-Barabanov, *supra* note 75.

to the user's specific interests more quickly and accurately than cookie technology would permit.[79]

The data aggregation industry also developed technology for sharing information between websites, thereby making the aggregated data considerably more useful to merchants, advertisers, direct marketers and other entities that see value in personal information. The best known provider of this type of service is probably DoubleClick, a service that distributes client advertisements to various web sites.[80] When a user clicks on a client's advertisement banner on a web site, a message is automatically sent back to DoubleClick reporting that the banner had achieved some success with a particular user. This lets DoubleClick determine which ads are being seen and which user is seeing them. DoubleClick can then create a profile of a user and search its list of subscribing companies for advertisements that match the user's interests. When the user browses the Internet later, the user will see advertisements tailored to his or her revealed preferences. Using this process, DoubleClick compiled eighty million customer profiles by the end of 1999.[81]

Even with knowledge of the astounding amount of digital information that is collected, manipulated, and shared every day, we still have difficulty discussing precisely what harm is being done. We see the benefits of the data processing revolution, yet we still have an uneasy

79. *See id.*

80. *See* Berman & Mulligan, *supra* note 73.

81. Heather Green, *Privacy Online: The FTC Must Act Now*, BUSINESS WEEK, Nov. 29, 1999, at 48. DoubleClick's notoriety is due in large part to an investigation of the company's practices by the FTC in 2000. The FTC initiated a "routine" investigation after learning that the company planned to merge its database with the database of Abacus Direct Corp., a direct marketing company that had information on most U.S. households. Charles L. Kerr & Oliver Metzger, *Online Privacy: New Developments and Issues in a Changing World*, Third Annual Institute on Privacy Law: New Developments & Issues in a Security-Conscious World, 701 PLI/PAT 303, 330-31 (2002); Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 109 (2002). The FTC was concerned that DoubleClick might be disclosing sensitive information about consumers in violation of its privacy policy, which would be a violation of the FTC Act. *See* In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 505 (S.D.N.Y. 2001). The FTC closed its investigation in January 2001, finding no evidence of illegal conduct. Robert G. Bagnall, *Privacy: Investment Company Regulation and Compliance*, SG100 ALI-ABA 255, 265 (2002). DoubleClick ultimately declared that it would not pursue the plan to merge information, and agreed to require all new clients and web sites to disclose their use of DoubleClick's services. Anthony Rollo, *The New Litigation Thing: Consumer Privacy*, 1301 PLI/CORP 9, 56-59 (2002); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 867 (2002). It also agreed to modify its privacy policy to explain its practices more clearly and to provide a better explanation of its opt-out procedures. *See* Barber & Quinn-Barabanov, *supra* note 75.

sense of foreboding. What exactly are we afraid of? This question is not easy to answer because we are not entirely sure how much of the collected data can be traced to us as individuals and used in a harmful way. Online firms, for example, maintain that the bits of information gleaned from cookies, web bugs, and the like cannot be associated with specific persons. At most, they can be used to identify computers at particular locations. That is hardly comforting news, however, because it will not be long before information about a computer location will be matched with individual owners or users of the computer.[82] This uncertainty about how personal information might be used in the future is cause for concern,[83] especially because once data is collected and stored, the shelf life is indefinite.

C. Conceptualizing the Harm

There are several ways to conceptualize the types of injury that can result from data collection and sharing.[84] One of the most discussed harms is the mischaracterization of an individual.[85] Other people,

---

82. Individual identification is already feasible to some extent. *See* Junkbusters, *How Web Servers' Cookies Threaten Your Privacy: You Can be Tracked From Your Mouse Clicks*, *at* http://internet.junkbuster.com/cookies.html (last visited Jan. 20, 2003). ("All they may need is your email address because various databases let them look up your name and address from it . . . . Any web site that knows your identity and has cookie for you could set up procedures to exchange their data with the companies that buy advertising space from them, synchronizing the cookies they both have on your computer. This possibility means that once your identity becomes known to a single company listed in your cookies file, any of the others might know who you are every time you visit their sites.") (emphasis omitted).

83. Studies have shown that the percentage of Internet users who balk at giving any personal information to web sites at 17 to 27%. Over 50% of Internet users are willing to provide information under the right circumstances. A third group would provide information to web sites under almost any circumstance. *See* John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?*, 39 ALBERTA L. REV. 346, 352 (2001) (citing L.F. Cranor, J. Reagle & M.S. Ackerman, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, at* http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm (Apr. 14, 1999)).

84. David Flaherty identified thirteen different privacy interests that deserve protection: the right (1) to individual autonomy, (2) to be "left alone," (3) to a "private life," (4) to control information about oneself, (5) to limit access to oneself, (6) to exclusive control of one's "private realms," (7) to minimize intrusiveness, (8) to expect confidentiality, (9) to enjoy solitude, (10) to enjoy intimacy, (11) to enjoy anonymity, (12) to enjoy reserve, and (13) to ensure secrecy. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 7–8 (1989).

85. *See* Jeffrey Rosen, *supra* note 30 (discussing the concepts of privacy—dignity, autonomy, "creation of knowledge," and mischaracterization problem).

The most influential book discussing information policy in the late 1960s was ALAN WESTIN, PRIVACY AND FREEDOM (1967), which examined the meaning of privacy in an historical, sociological and legal context. Westin maintained that privacy was a basic need of all human beings

businesses, or governmental institutions examine information that we generally regard as private, and they use that information to make judgments about us. Since the information used to form the judgment is not the complete set of relevant facts about us, we can be harmed (or helped) by the stereotyping or mischaracterization.[86] Jeffrey Rosen observed in his influential work, *The Unwanted Gaze*, that "[p]rivacy 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."[87] Our data records cannot tell the whole story about us, yet we are frequently judged on the basis of small bits of information in important aspects of our lives.

We are aware of the mischaracterization problem in many areas of life. For example, in the legal education community, we sometimes measure the importance of law review articles by looking at the number and type of citations made to them in judicial opinions.[88] Each spring, law school deans, faculties, and alumni lament (or quietly cheer) the release of a national "ranking" of law schools by *U.S. News and World Report,* which uses selected facts and figures to divide schools into four "tiers" of descending prestige.[89] College athletic teams are ranked by a computerized data system that relies on a handful of variables, including margin of victory and the relative strength of each team's opponents.[90]

---

and was important even to primitive societies. Westin also observed that privacy was in jeopardy even then by developments in information technology.

86. Kenneth Karst warned in the 1960s that one problem with a large database of personal information is that the facts in the database "will become the only significant facts about the subject of the inquiry." Kenneth L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 L. & CONTEMP. PROBS. 342, 361 (1966). *See* Solove, *supra* note 31, at 1424.

87. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000). The book was the subject of a symposium in 89 GEORGETOWN LAW JOURNAL (2001).

88. *See* Solove, *supra* note 31, at 1424.

89. *See Best Graduate Schools*, U.S. NEWS AND WORLD REPORT, *available at* http://www.usnews.com/usnews/edu/grad/rankings/law/lawindex.htm (last visited Jan. 20, 2003). *Cf.* Stephen P. Klein, and Laura Hamilton, *The Validity of the U.S. News and World Report Ranking of ABA Law Schools*, *at* http://www.aals.org/validity.html (Feb. 18, 1998) (noting many problems with the U.S. News survey methodology); *cf.* Mitchell Berger, *Why the U.S. News and World Report Law School Rankings Are Both Useful and Important*, 51 J. LEGAL. EDUC. 487 (2001) (justifying the rankings as useful for students, lawyers and law schools).

90. *See* http://collegerpi.com (last visited Jan. 20, 2003). *Cf.* Dan Wetzel, *National Notes: RPI Flawed, Inaccurate and Unfair*, CBS SPORTSLINE, *at* http://ww3.sportsline.com/b/page/pressbox/0,1328,3553019,00.html (Feb. 22, 2001) (criticizing the RPI for giving an advantage to well-funded athletic programs that are willing to pay opponents to play in their arena).

The reasons for stereotyping are easy to appreciate. The objective is to place people, groups, or other subjects in specific categories that can give us some measure of confidence that judgments based on the categorization will be well founded. For example, only if a consumer's credit score rises above a certain threshold will she be considered a good credit risk and then receive a "pre-approved" credit card. The card issuer has confidence that individuals in the higher scoring groups will be more likely to pay their bills on time.[91] While stereotyping has been with us for ages, computer databases encourage the practice by making it much easier to collect vast amounts of data quickly and sort it in countless ways. The resulting judgments might be proved correct in the aggregate (for example, the overall default rate on credit accounts may decrease), but they can be unfair in individual cases. A bankruptcy filing or criminal arrest record can be misleading without knowing the story behind it or the ultimate disposition of the case, but the record's appearance on a credit report will adversely affect a credit decision regardless of the background details.

If mischaracterization were the main problem with information collection and storage, however, it is by no means clear that the appropriate public policy response would be to restrict data flows. A logical solution would be to encourage the collection of more, not less, information about each of us. We could reduce the likelihood of misjudgments if our data files were more complete, so we should encourage greater aggregation of data and more extensive sharing of information among data processors. The FCRA essentially embraces this approach. If a consumer believes that her credit report contains inaccurate or incomplete information, she can supply the missing facts and have them added to the report in hopes of providing a more accurate picture.[92]

---

91. *See generally* The Credit Scoring Site, *at* http://www.creditscoring.com (last visited Jan. 20, 2003); Daniel Mendel-Black & Evelyn Richards, *Peering into Private Lives: Computer Lists Now Profile Consumers by Their Personal Habits*, WASH. POST, Jan. 20, 1991, at H01 ("Details . . . are sorted, digested and compiled so that computers can plop you into neatly defined categories to help determine the likelihood that you'll pay your Visa bill on time or buy a new brand of detergent or cigarettes within the next few months."); David Rameden, *When the Database Is Wrong . . . Do Consumers Have Any Effective Remedies Against Credit Reporting Agencies and Information Providers?*, 100 COM. L.J. 390, n.10 (1995) (citing *Consumer Problems With Credit Reporting Bureaus: Hearings Before the Senate Subcomm. on Consumers of the Comm. on Commerce, Science & Technology*, 102 Cong., 2d Sess. 2 at 47 (1992) (testimony of Mary Santina, retail representative)); *What Price Privacy?*, 56 CONSUMER REP. 356, 357 (1991) (credit scoring example).

92. *See* 15 U.S.C. § 1681(i)(b) (2000).

Other categories of injury from data collection and sharing have been described in anthropological or sociological terms. Loss of privacy can be seen as an affront to human dignity,[93] a loss of personal autonomy,[94] and other terms that reference the value of one's "core self."[95] These concepts focus on the objectification of an individual resulting from pervasive surveillance and seemingly unlimited access to personal information in modern society. Protecting privacy, and contracting those aspects of our lives that are open to searching and monitoring, is an important way of showing that individuals are worthy of respect.[96] The promotion of this ideal is central to the modern view of a liberal society. It bolsters John Stuart Mill's vision that "over himself, over his own body and mind, the individual is sovereign."[97]

For most of us, though, the more troubling problem is not a mischaracterization of our complex persona or a reduction of our humanity to a set of electronic bits and bytes. The more cognizable and immediate problem with a loss of information privacy, and the problem that is most likely to produce a political resolution, is our inability to avoid circumstances in which others control information that can affect us in material ways—whether we get a job, become licensed to practice in a profession, obtain a critical loan, or fall victim to identity theft.[98] We cannot avoid the collection and circulation of information that can profoundly affect our lives. We feel that we have little or no voice or choice in the data collection and sharing process. We do not know who has what information, how they got it, what purposes or motives those

93. *See generally* Robert Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2088, 2092–98 (2001) (discussing Jeffrey Rosen's book, THE UNWANTED GAZE, *see supra* note 87). Post views privacy as connected to three distinct concepts: dignity, autonomy and the creation of knowledge.

94. *See* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 300 (Shoeman ed., 1982).

95. WESTIN, *supra* note 85, at 32.

96. *See* Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 223 (Shoeman ed., 1982); Rosen, *supra* note 30, at 2121.

97. John Stuart Mill, *On Liberty*, *in* UTILITARIANISM 135 (Mary Warnock ed., 1962).

98. In the area of privacy and technology, part of the explanation of why privacy did not draw more congressional advocates in the 1960s and early 1970s is that it is difficult to agree on a definition of the problems presented. *See* WESTIN, *supra* note 85, at 7 ("Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."); Judith Jarvis Thomson, *The Right to Privacy*, 4 PHILOS. & PUBLIC AFFAIRS 295, 295 (1975) ("[T]he most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."); REGAN, *supra* note 7, at 3. The definition of privacy in the U.S. that has formed the basis of most of the policy discussion is the right to control information about and access to oneself. *Id.* at 4.

entities have, or what will be done with that information in the future.[99] Even if the information in a database is accurate and complete in all relevant respects, it can still harm us if it falls into the wrong hands or if it is used for a purpose we did not envision when we disclosed it.[100]

What compounds our discomfort is the likelihood that as technological developments improve, we can expect to lose more control over the collection and sharing of information about us. Advances in genomics are fueling the creation of DNA databases.[101] The trend in

---

99. In 1969, Alexander Solzhenitsyn described the relationship between an individual and an authority that controls information about him:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. A man's answer to one question on one form becomes a little thread, permanently connecting him to the local center of personnel records administration. There are thus hundreds of little threads radiating from every man, millions of threads in all.... Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads... and for these people's authority.

ALEXANDER SOLZHENITSYN, CANCER WARD 192 (1969).

100. *See* Robert S. Peck, *The Right to Be Left Alone*, 15 HUM. RTS. 26, 28 (1987) ("information collected for one purpose may be shared with other agencies and used for entirely different purposes... [and] assembled into a complete personality profile at the touch of a computer button").

101. Many companies have begun commercializing genomic information for therapeutic and other purposes. As early as 1995, over 50 biotechnology companies were developing or providing tests to diagnose genetic disorders or to predict the risk of their future occurrence through identification of "susceptibility-conferring genotypes." *See* Neil Holtzman, *Are Genetic Tests Adequately Regulated?*, SCIENCE 286, 409 (October 15, 1999).

The web site for Celera Genomics, Inc. describes its function as that of a "leading provider of information based on the human genome and related biological and medical information." *See* http://www.celera.com (last visited Jan. 20, 2003); Scott Hensley, *Celera's Genome Anchors it Atop Biotech*, WALL ST. J., Feb.12, 2001, at A3 ("Three-year-old Celera, it now is clear, has produced a [genome] map that drug and biotech companies, hungry for gene information that will help them find new treatments, are plunking down millions of dollars a year for the right to sift through."). Other recent literature documents the worldwide scope of these activities. For example, an August 2000 article notes proposals for the creation of "phenotype" databases (databases containing information about the physical characteristics of patents for whom genetic information is known) in the United Kingdom, Italy, and Estonia; and a recent $200 million agreement between Reykjavik-based decode Genetics and Hoffman-LaRoche, Inc. based on a database based on the medical records of Iceland's 275,000 citizens. *See* Daniel Machalaba, *Burlington Northern Ceases its Genetic Testing*, WALL ST. J., Feb. 13, 2001, at B10; Antonio Regalado, *Medical Records, Inc.*, TECHNOLOGY REVIEW (July/August, 2000); Editorial, *Gene Library*, BOSTON GLOBE, Sept. 17, 2000.

Several states have taken action to guard genetic information more zealously than other medical records. *See, e.g.*, Cal. CIV. CODE § 56.17 (West 2002); N.J. STAT. ANN. § 10:5-45 (West 2002). *Cf.* GA. CODE ANN. § 33-54-6 (2002) (research facilities may use the information derived from genetic testing for scientific purposes so long as the identity of any individual tested is not disclosed to any third party, except that the individual's identity may be disclosed to the individual's physician with the consent of the individual).

business is to use technology to create "human-centered computing"[102] and new technologies designed to benefit consumers by making their lives more efficient and their work more productive. Yet while the potential efficiencies of new technologies are trumpeted, the societal cost of these technologies is hardly noticed. Examples include: biometric signatures that can make air travel, banking, and other activities more secure and efficient as they enhance customer convenience;[103] "smart cards" that can be carried like a digital passport, which are useful because a stolen credit card is much less valuable when the person attempting to use it could be immediately identified as an imposter;[104] palm or retinal scanners that businesses could install to verify every customer's identity; and even "smart buildings" that can follow the whereabouts of all employees and visitors, all day long, and record the data for future use.[105]

Video analysis and scanning systems can pick out a face in the crowd that matches a digital imprint of an escaped convict, a father behind on child support, a terrorist, or a missing person.[106] Every time a person moves in front of a surveillance camera, a database could record the location of the person and at precisely what time she walked by.[107]

---

102. *See* Dick Brown, Chief Executive Officer, EDS Corporation, COMDEX 2001 Keynote Address, *available at* http://www.eds.com/thought/thought_speeches_brown111301.html (Nov. 13, 2001).

103. *See* Lisa Jane McGuire, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441, 447–49 (2001) (investigating privacy implications of using biometrics in the banking industry); U.S. Senate Special Committee on Aging, "Identity Theft: The Nation's Fastest Growing Crime Wave Hits Seniors," 107th Cong., 2d sess, at 147–57 (2002) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center (EPIC)) (advocating government regulation of biometric signatures before vast stores of data are built and privacy interests compromised further).

104. *See* Steven A. Bercu, *Smart Card Technologies, Novel Privacy Concerns and the Legal Response*, 7 J. PROPRIETY RTS. 2, 3 (1995); Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 992–93 (1999); Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 398–99 (1994).

105. *See* Deirdre K. Mulligan, *Privacy Past, Present, and Future*, THIRD ANNUAL INSTITUTE ON PRIVACY LAW: NEW DEVELOPMENTS & ISSUES IN A SECURITY-CONSCIOUS WORLD, 701 PLI/Pat 63 (2002).

106. *See* WHITAKER, *supra* note 31, at 140–42 (discussing new surveillance technologies that "render individuals 'visible' in ways that Bentham could not even conceive"); John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns-Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, n.203 (1997) (hypothesizing that a state legislature could decide to require all children attending private day care to be biometrically scanned for identification purposes).

107. *See* WHITAKER, *supra* note 31, at 140–42.

Global Positioning System (GPS) technology[108] can take the concept further. With a fairly low-cost receiver, a computer can pinpoint a person's location anywhere on earth within a few feet. Lost automobile drivers and hikers in remote areas can benefit immensely from this technology. With some enhancements, a computer chip could be attached to a small child, an Alzheimer's patient, or a parolee, and the person could be tracked anywhere he or she goes.[109]

Of course, all of these developments have two sides. One is convenience, efficiency, and empowerment; the other is continual surveillance and loss of individual control once information is revealed. We like the information used for some purposes, but we dread its use for others. This dynamic is typical of most public policy problems that find a resolution in our legal system. How do our laws work to preserve the benefits of information collection and storage, but minimize the risks of its misuse?

II. THE LEGAL LANDSCAPE IN THE UNITED STATES

A. Inadequacy of Common Law Torts and the United States Constitution

Privacy law in the United States did not begin to develop until the middle of the twentieth century.[110] As it developed, the legal doctrine addressed problems fundamentally different from those presented by digital databases. Courts and legislatures created a number of torts designed to redress injuries caused by unwelcome interlopers, such as an overly aggressive press or a political enemy, who invaded what Warren

---

108. A Global Positioning System (GPS) can transmit information about an object's three-dimensional position, velocity and time to anyone equipped with a GPS receiver. GPS can also provide precise guidance and targeting information for missiles. *See* Shaun B. Spencer, *Reasonable Expectations and the Erosions of Privacy*, 39 SAN DIEGO L. REV. 843, 882–83 (2002) (explaining that the Department of Defense developed the GPS in the early 1970s as a satellite-based positioning and navigation system).

109. *See* WHITAKER, *supra* note 31, at 140–42; Froomkin, *supra* note 31, at 1496–98 (noting that satellite tracking is being used to monitor convicted criminals on probation, parole, home detention, and work release, at a daily cost of only about $12.50 per target); Mark G. Young, Note, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1035–36 (2001).

110. Although the U.S. Supreme Court recognized a Fourth Amendment right to privacy as early as 1886 in *Boyd v. United States*, 116 U.S. 616 (1886), most of the case law development in tort and constitutional law emerged decades later. *See generally* Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289 (1981).

and Brandeis called "the sacred precincts of private and domestic life."[111] Depending on the jurisdiction, variously named "privacy torts" ordered the payment of compensation for the most egregious harms resulting from disclosure of facts that most would consider purely private matters. These torts included invasion of privacy, intrusion upon seclusion, public disclosure of private facts, false light or false publicity, and misappropriation.[112]

Because these torts developed to address injuries resulting from the release of private and embarrassing facts,[113] they were not intended, and are not well suited, to redress the harms caused by the collection and sharing of information in databases.[114] Most of the injuries caused by the misuse of data in modern society are not particularly embarrassing or emotionally disturbing. Even when they are, because data can be aggregated, stolen, or transferred with the click of a keystroke, tracing the injury to the source of the information leak, and then establishing the requisite mens rea for the tort, will often be impossible.[115] A remedy in

111. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890). Justice Brandeis later referred to privacy as "the most comprehensive of rights and the right most valued by civilized men." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

112. *See* REGAN, *supra* note 7, at 32–33; ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 189 (1971) ("[M]ost significantly, the existing common law structure does nothing to give the data subject a right to participate in decisions relating to personal information about him, a right that is essential if he is to learn whether he has been victimized by a privacy invasion."); Solove, *supra* note 31, at 1432.

Defamation is another tort that can be alleged in some cases of unauthorized information sharing. For example, privacy and defamation torts were being combined in cases where the use of a person's name without consent was held to be offensive. *See* Harry Kalven Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 333 (1966). This comes close to judicial recognition of Charles Fried's definition of privacy as "that aspect of social order by which persons control access to information about themselves." Charles Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968). Still, courts seldom adopted this reasoning. *See* REGAN, *supra* note 7, at 34.

113. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383–423 (1960) (isolating four distinct torts for invasion of privacy interests).

114. Although many writers discount the effectiveness of privacy torts as a mechanism for redressing misuse of personal information, others believe that tort law has simply been underutilized in information privacy cases. *See, e.g.*, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, *at* http://www.privacilla.org/releases/Torts_Report.html (July 2002) (maintaining that greater use of privacy torts would more effectively protect information privacy than would government regulation); Denise G. Callahan, *Courts Make Better Privacy Law*, 13 IND. LAWYER, Aug. 14–27, 2002, at 1 (noting that litigation may be the best way to discover harmful information practices, citing tobacco litigation as an example of successful litigation strategies).

115. *See* Solove, *supra* note 32, at 1085 (noting that harms resulting from the misuse of personal data often do not result from malicious intent or the desire for domination); Catherine Therese

tort, assuming precedent would support one, will often be unobtainable as a practical matter.

More recently, other torts have been alleged in litigation over the collection and misuse of information in databases. Although some show promise for database protection, to date they have proved unsuccessful. Fraud (or deceit), and unjust enrichment, for example, have been asserted in situations where information was collected surreptitiously or used in ways contrary to the data collector's privacy policy.[116] Fraud is difficult to prove because of the requirement that the tortfeasor act with intent to defraud or at least with reckless disregard for the truth.[117] In the fast moving and often depersonalized world of digital data transfers, this can be difficult to establish.

The equitable doctrine of unjust enrichment has more promise as a vehicle for redressing the harms caused by unlawful data collection and sharing. Unjust enrichment requires a showing of economic benefit to one party at the expense of the other, plus a finding that the enrichment was somehow unfairly or unjustly obtained.[118] In the context of digital

---

Clarke, *From CrimiNet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Mens Rea on the Internet*, 75 OR. L. REV. 191, 205 (1996).

116. Seth R. Lesser, *Privacy Law in the Internet Era: New Development and Directions*, 632A PLI/Pat 187, 218, June 2001 (unjust enrichment is a potential claim against an Internet defendant's surreptitious collection of information and/or online profiling). *See* Healey v. DoubleClick, No. 0CIV.00641 (S.D.N.Y. 2000) (complaint alleged violations of the federal Electronic Communications Privacy Act and other federal statutes, deceptive advertising under New York law, and common law unjust enrichment and invasion of privacy for DoubleClick's alleged practice of surreptitiously using cookies to create profiles of Internet users); Judnick v. DoubleClick, No. CV-421 (Marin Cty. Sup. Ct., 2000) (copy available at http://legal.web.aol.com/decisions/dlpriv/doubleclick.pdf). *See generally* Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97 (2001).

117. *See e.g.*, Cao v. Nguyen, 607 N.W.2d 528, 532 (Neb. 2000) (stating that to maintain an action for fraudulent misrepresentation, a plaintiff must prove: (1) that a representation was made; (2) that the representation was false; (3) that when made, the representation was known to be false or made recklessly without knowledge of its truth and as a positive assertion; (4) that it was made with the intention that the plaintiff should rely upon it; (5) that the plaintiff reasonably did so rely; and (6) that the plaintiff suffered damage as a result); Suiter v. Mitchell Motor Coach Sales, Inc., 151 F.3d 1275, 1282 (10th Cir. 1998) (concluding that "intent to defraud" may be inferred if it is shown that the defendant lacked such knowledge only because he displayed reckless disregard for the truth or because he closed his eyes to the truth). *See generally* 37 AM. JUR. 2D, *Fraud and Deceit* § 107 (2002) (explaining that proof of a mere naked falsehood or representation is ordinarily not enough, but in addition to the false representation, the false statement must have been made intentionally to deceive).

118. *See* Lesser, *supra* note 116. A cause of action for unjust enrichment lies where someone has conferred a benefit and it would be inequitable or unjust for the recipient to retain that benefit. RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT §§ 1, 2 (2000); United Coastal Indus., Inc. v. Clearheart Const. Co., 802 A.2d 901, 905 (Conn. App. Ct., Aug. 13, 2002)

databases, this doctrine has potential for success when, for instance, a web site violates its privacy policy by selling information to a marketing firm, or storing information that the site said it would not store.[119] Aggrieved web site users would have to show that the site obtained an economic benefit from the information obtained, and that the collection or transfer of information was otherwise inequitable and unjust.[120] Proving both elements is difficult in many circumstances, which may explain why unjust enrichment is generally considered a relatively ineffective doctrine in this and other contexts.

As a public policy matter a more important problem with common law principles is that they do not protect the individual prior to injury. When our privacy is threatened by public or private sector data collection and sharing, lawsuits only offer a means of redress after the invasion; they do not provide a sufficient deterrent that will prevent the invasion from occurring.[121] Since most of us are not going to pursue damage remedies for privacy invasion except in the most extreme circumstances, these doctrines cannot do much to redress the dangers of information collection and exchange that most Americans fear.

Federal constitutional protections have proved equally unhelpful for most database privacy problems, at least at the federal level.[122] Like tort

---

("[r]ecovery is proper if the defendant was benefited, the defendant did not pay for the benefit and the failure of payment operated to the detriment of the plaintiff"); State Dep't of Human Servs. *ex rel.* Palmer v. Unisys Corp., 637 N.W.2d 142, 154–55 (Iowa 2001) ("[r]ecovery based on unjust enrichment can be distilled into three basic elements of recovery. They are: (1) defendant was enriched by the receipt of a benefit; (2) the enrichment was at the expense of the plaintiff; and (3) it is unjust to allow the defendant to retain the benefit under the circumstances").

119. Lesser, *supra* note 116; Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1134 (2000) (arguing that "a property rights approach [will] . . . halt the unjust enrichment that compilers of personal information now enjoy"); Natalie L. Regoli, *A Tort for Prying Eyes*, 2001 J.L. TECH. & POL'Y 267, 287 (2001) (envisioning an Internet profiling tort that would provide restitution as a baseline recovery, and arguing that the unjust enrichment that was obtained at the user's expense should be measured by the aggregate enrichment gained from all users' information).

120. RESTATEMENT (THIRD) OF RESTITUTION, *supra* note 118.

121. *See* Guy J. Sternal, Comment, *Information Privacy and Public Records*, 8 PAC. L.J. 25, 27 (1977).

122. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 33–35 (1996) (discussing the limited availability of constitutional law in protecting privacy interests in the private sector). Indeed, to the extent the U.S. Constitution is invoked in privacy litigation or public policy debate, it is often to invoke the First Amendment in support of those who support less onerous restrictions on access to information and fewer impediments to exchange of information once they obtain it. *See, e.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People*

law, to the extent there is a constitutional remedy, it arrives only after the injury has occurred. Moreover, the U.S. Constitution protects only against unlawful government action, and many of the more powerful and potentially injurious databases are maintained in the private sector.[123]

The U.S. Supreme Court has recognized constitutionally protected privacy interests in various contexts, deriving the right from the First, Third, Fourth, Fifth and Ninth Amendments.[124] However, most of the Court's decisions have only marginal relevance to the problem of databases.[125] The Fourth Amendment comes closest to encompassing a right of information privacy against government misuse of data, but thus far it has not been construed broadly enough to protect against most harms that result from the data collection, use, and distribution.[126] The Supreme Court has assumed that privacy is about protecting highly personal information.[127] Thus, we have no constitutionally protected expectation of privacy when we permit our information to be accessed by a third party (such as an online search engine) or when we voluntarily give the information to someone else (such as filling out a job

---

from Speaking About You, 52 STAN. L. REV. 1049 (2000); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173 (1999).

A right of privacy appears in some state constitutions that could be construed more broadly than the federal constitution, which does not recognize the right expressly. *See, e.g.*, ALASKA CONST. art. 1, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, § 7; LA. CONST. art. I, § 5; ILL. CONST. art. I, § 6. Of course, to the extent there is a conflict with the First Amendment, free speech rights would override any privacy protection in state constitutions or case law. *See* John H. Garvey, *Freedom of Choice in Constitutional Law*, 94 HARV. L. REV. 1756, 1770–71 (1981); Shelley Ross Saxer, *Shelley v. Kraemer's Fiftieth Anniversary: "A Time for Keeping; A Time for Throwing Away?"*, 47 U. KAN. L. REV. 61, 101 (1998).

123. *See* Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 COLUM. L. REV. 1527, 1580 (2002); William J. Rich, *Taking "Privileges or Immunities" Seriously: A Call to Expand the Constitutional Canon*, 87 MINN. L. REV. 153, 211, 211 n.361 (2002). According to the Supreme Court, "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." Schmerber v. California, 384 U.S. 757, 767 (1966).

124. *See* REGAN, *supra* note 7, at 35.

125. The U.S. Supreme Court, for example, has recognized privacy interests such as associational privacy, *NAACP v. Alabama*, 357 U.S. 449, 462 (1958), political privacy, *Watkins v. United States*, 354 U.S. 178, 198–99 (1957), and the right to anonymity in public expression, *Talley v. California*, 362 U.S. 60, 64 (1960) (distribution of handbills in public place). *See also* Couch v. United States, 409 U.S. 322, 327 (1973) (the privilege against self-incrimination "respects a private inner sanctum of individual feeling and thought").

126. *See, e.g.*, Dow Chemical Co. v. United States, 476 U.S. 227, 231 (1986) (no violation of Fourth Amendment when EPA engaged in warrantless aerial photography of manufacturing facility); California v. Greenwood, 486 U.S. 35, 40–41 (1988) (no reasonable expectation of privacy in trash bags left at curb for pick-up because bags are "readily accessible to . . . scavengers, snoops, and other members of the public").

127. *See infra* note 132.

application). The Court has held, for example, that there is no expectation of privacy in the telephone numbers we dial because we have released the information to the phone company.[128] There is no privacy right in the information contained in personal checks because they are not "confidential communications" once they are sent through the check collection process.[129]

However, courts have upheld a constitutional right to information privacy in a narrow set of circumstances. In 1977, the Supreme Court recognized a right to information privacy, noting a constitutionally protected "individual interest in avoiding disclosure of personal matters."[130] Most of the decisions in this line involve a breach of confidentiality, or the risk of unwanted publication of very private facts. In particular, courts have occasionally found a constitutionally protected right to information privacy when the records involve highly personal issues such as sexual practices or medical conditions.[131] Thus, while medical records might be protected from disclosure,[132] arrest and conviction records are unprotected because they already appear in a public record.[133] Outside the realm of health and sex information, courts have not found much protection within the United States Constitution against information collection and disclosure.

---

128. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979). *See also* United States v. Miller, 425 U.S. 435, 442 (1976) (holding there is no expectation of privacy in a person's financial records held by a third party).

129. *Miller*, 425 U.S. at 442. In response to the decision in *Miller*, Congress enacted the Financial Privacy Act in 1978, 12 U.S.C. § 3401 et seq. (2000), which provides some privacy protection for a customer's banking records.

130. Whalen v. Roe, 429 U.S. 589, 599 (1977). Although the Court recognized the privacy right, it upheld a New York law that required the state to maintain computerized records for certain drugs. *Id.*

131. *See* Solove, *supra* note 53, at 1204–05.

132. *See* Doe v. Borough of Barrington, 729 F. Supp. 376, 382 (D.N.J. 1990) (police disclosure that a person had AIDS); Woods v. White, 689 F. Supp. 874, 875 (W.D. Wis. 1988) (prisoner has privacy right in medical records). The Supreme Court in *Nixon v. Administrator of General Services*, 433 U.S. 425, 465 (1977) held that President Nixon had a privacy interest in his communications with family members, his physician and his minister, but not in communications within the scope of his official duties. Even with respect to Nixon's personal communications, however, the Court held that the privacy interest was outweighed by the public interest in obtaining full access to the documents. *Id.*

133. *See* Russell v. Gregoire, 124 F.3d 1079, 1094 (9th Cir. 1997) (holding law requiring community notification of sex offenders did not violate privacy rights because the arrest and conviction records were "already fully available to the public"); Cline v. Rogers, 87 F.3d 176 (6th Cir. 1996) (holding that there is no protection for information already in public record).

Without a radical expansion of tort and constitutional law doctrine, these areas are not likely to provide effective privacy protection for most database problems. What people want when they demand privacy with regard to their personal data is confidence that information about them—even if it is not confidential or embarrassing per se—will be used only for the purposes they desire.[134] There is a considerable loss of privacy when someone extracts even ordinary information buried in government or business records and uses it for purposes other than the purpose for which it was originally intended.

More importantly, as more and more information about us is maintained in databases, less and less information will be considered secret. The limited federal constitutional and common law protections that currently exist will become even less relevant. If privacy law is only concerned with protecting against the release of certain highly personal, non-public, confidential information, it protects very little information at all. And if we rely on individual enforcement of common law and constitutional norms through private litigation as the principal policing mechanism, we have hardly any legal safeguard whatsoever.

B. The Development of Legislative Solutions—the Public Sector and the Privacy Act of 1974

Concerns about information privacy as a political and social issue surfaced in the 1960s. Two factors combined to bring the issue to the public agenda. One was the rapid development in record-keeping systems in both government and the private sector. The other was the computerization of information storage, retrieval, and data processing.

During the period after World War II, government agencies expanded social welfare programs, consumers and businesses became more credit dependent, and the insurance industry grew rapidly. As a by-product of these and other developments, more records containing personal information were being collected and maintained by an increasing number of institutions, both public and private. At the same time, governments, financial institutions, insurance companies, and other entities that held personal information on large numbers of individuals began to see the benefits of converting their paper files and forms to

134. "Between data warehousing, profiling, and bankruptcy asset liquidations, American consumers perceive that they have lost control over their personal information. For e-commerce, this belief becomes an obstacle to the growth of online transactions." Joel R. Reidenberg, *E-Commerce and Transatlantic Privacy*, 38 HOUSTON L. REV. 717, 722 (2001).

computer databases.[135] Few legal norms constrained data collection practices during this era.[136]

The first major catalyst for the privacy debate in Congress occurred in 1965. A report of the Social Science Research Council proposed the creation of a "Federal Data Center" that would coordinate the storage and use of government statistical information among several agencies that, until then, had been operating independently.[137] The proposal was intended to increase the efficiency of government operations by aggregating data from various government sources and combining it into a single, more versatile system. However, the proposal raised concerns that too much information would be held and maintained by one centralized source, and more generally, about the impersonality of treating citizens as data entries rather than human beings.[138] This led to a series of hearings that focused on invasion of privacy in the computerized world. Congress ultimately rejected the national data center idea, but government agencies continued to computerize information systems hoping to increase the efficiency of government operations.[139]

Also influential in the development of early privacy legislation was a 1973 report by the Department of Health, Education and Welfare (HEW Report) entitled "Records, Computers, and the Rights of Citizens."[140] The report viewed information privacy as an important and growing societal

135. *See* REGAN, *supra* note 7, at 69.

136. *Id.* at 70.

137. The proposal prompted extensive hearings in both the House and Senate. *See* UNITED STATES HOUSE COMMITTEE ON GOVERNMENT OPERATIONS, SPECIAL SUBCOMMITTEE ON INVASION OF PRIVACY, *The Computer and Invasion of Privacy: Hearings*, 89th Cong., 2d sess. (1966) [hereinafter U.S. HOUSE PRIVACY HEARING]; UNITED STATES SENATE COMMITTEE ON THE JUDICIARY, SUBCOMMITTEE ON ADMINISTRATIVE PRACTICES AND PROCEDURE, *Invasion of Privacy (Government Agencies): Hearings*, 89th Cong., 2d sess., part 5 (1966).

138. Rep. Cornelius Gallagher (D-NJ), chair of the House Special Subcommittee on Invasion of Privacy, expressed this concern about creating a Federal Data Center: "[I]f safeguards are not built into such a facility, it could lead to the creation of what I call 'The Computerized Man.' The Computerized Man, as I see him, would be stripped of his individuality and privacy. Through the standardization ushered in by technological advance, his status in society would be measured by the computer, and he would lose his personal identity. His life, his talent, and his earning capacity would be reduced to a tape with very few alternatives available." U.S. HOUSE PRIVACY HEARING, *supra* note 137, at 2.

139. REGAN, *supra* note 7, at 73.

140. UNITED STATES DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers, and the Rights of Citizens* (Washington D.C., Government Printing Office, 1973) [hereinafter HEW REPORT].

problem, and concluded that the "natural evolution of existing law will not protect personal privacy from the risks of computerized personal data systems."[141] Its final recommendations included the adoption of a Code of Fair Information Practices to govern recordkeeping throughout the federal government.[142] The report was influential in creating a framework for subsequent policy formulation in both the public and private sectors for years to come.

Early legislative initiatives followed the recommendations of the HEW Report and viewed information privacy as a societal value and called for a comprehensive regulatory response in the public interest. In 1974, Senators Sam Ervin (D-NC), Charles Percy (R-Ill.), and Edward Muskie (D-Maine), introduced a bill that was broad in scope, covering all information storage systems in federal, state, and local government, as well as the private sector.[143] Its regulatory approach included the creation

---

141. HEW REPORT, *supra* note 140, at 37. The report also called for "[t]he development of legal principles comprehensive enough to accommodate a range of issues arising out of pervasive social operations, applications of complex technology, and conflicting interests of individuals, record-keeping organizations and society, will have to be the work of legislative and administrative rule-making bodies." *Id.*

142. The proposed Code of Fair Information Practices set out certain fundamental principles of privacy protection:

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

HEW REPORT, *supra* note 140, at 40–41. A similar set of guidelines was developed in England and Germany at about the same time, and the Organisation for Economic Cooperation and Development (OECD) issued eight similar principles in 1980. *See* OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [hereinafter *Guidelines*], *available at* http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-1-no-no-10255-0,00.html (1980); *see also* BENNETT, *supra* note 49, at 98–100. As the OECD was developing its *Guidelines*, a similar effort by the Council of Europe resulted in the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data. The *Convention* had similar aims, but one difference is that the *Guidelines* are not legally binding on OECD member states, whereas the *Convention* is binding on all ratifying states. However, only 21 of the Council's 41 member states ratified the *Convention*. *See* Council of Europe, *Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*, E.T.S. 108, *available at*

of a national Privacy Board with authority to police breaches of the privacy rules and standards established by the law. It also proposed a set of fair information practices similar to those in the HEW Report, and granted individuals the rights to see and amend their personal files, and to be informed about the release or sharing of their information.[144]

These comprehensive privacy bills did not fare well in the legislative process. The private sector was eventually removed from the most seriously considered privacy bills. Influencing this decision was the lack of evidence that the private sector was misusing large amounts of personal information at the time.[145] The burden was placed on privacy advocates to show that a serious problem existed in private sector databases, and the evidence was unconvincing.[146] Although anecdotal accounts of improper information disclosure were offered, and some evidence of systematic problems with the integrity of private database was presented, the evidence was not persuasive enough to justify a heavy handed regulatory approach that included privately held data records.[147]

There were practical considerations as well. The private sector was considered too complex for a centralized regulatory system and it

---

http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm> and http://conventions.coe.int/ (Jan. 28, 1981).

143. *See* Privacy Act of 1974, 88 Stat. 1896 (1974), *reprinted in* SENATE COMM. ON GOV'T OPERATIONS AND HOUSE COMM. ON GOV'T OPERATIONS, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974, S. 3418 (Pub. L. No. 93-579), Source Book on Privacy, at 9–28 (Joint Comm. Print 1976); Steven W. Becker, *Maintaining Secret Government Dossiers on the First Amendment Actitivies of American Citizens: The Law Enforcement Activity Exception to the Privacy Act*, 50 DEPAUL L. REV. 675, 688 (2000).

144. REGAN, *supra* note 7, at 77. At the time, several important participants in the debate considered the establishment of a federal agency to oversee information privacy practices to be an integral part of an effective plan. Among them was Arthur Miller, who called for the appointment of an "information ombudsman." *See* UNITED STATES. SENATE COMMITTEE ON THE JUDICIARY, SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS, *Federal Data Banks, Computers, and the Bill of Rights*, Testimony of Arthur Miller, 92d Cong., 1st sess., at 19 (1971). Others recommend a "regulatory commission with full powers over the collection, use and dissemination of personal information." *See* Becker, *supra* note 143, at 713.

145. *See Before the Ad Hoc Subcomittee on Privacy and Information Systemes of the Senate Committee on Government Operations and the Subcomittee on Constutational Rights of The Seante Committee on the Judiciary, Privacy—The Collection, Use and Computerization of Personal Data: Joint Hearings*, 93d Cong., 2d sess., 515, 450–51 (statements of the American Life Insurance Association and Department of Commerce).

146. *See* REGAN, *supra* note 7, at 78.

147. *Id. See also* Patricia Mell, *A Hitchhiker's Guide to Data Exchanges Between EU Member States and the U.S. Under the European Union Directive on the Protection of Personal Information*, 9 PACE INT'L L. REV. 147, 158 (1977).

involved too many competing interests.[148] Countless factors would have to be balanced if a regulatory regime was going to protect information privacy yet not impose high costs on businesses. Even Alan Westin, a strong privacy advocate during this period, concluded that this was not the right time for comprehensive regulation of the private sector.[149]

With the private sector effectively removed from the legislation, support also weakened for the creation of a national Privacy Board, or a similar independent agency with supervisory authority over information privacy in the government sector.[150] A new oversight agency would be costly and, agencies argued, unnecessary because they also regarded privacy as a high priority and could monitor their own compliance with legal mandates. A separate entity would only pit one agency against another, an inefficient course when all agencies shared the same privacy protection goals.[151] At this pivotal point in the debates, the focus thus shifted to privacy as an individual concern, with emphasis on agency independence and legislative solutions that gave legal rights and remedies to individuals who would be left to police their rights under the law.[152]

The ultimate legislative result came after more than ten years of debate,[153] when Congress enacted the Privacy Act of 1974 (Privacy

148. *See* REGAN, *supra* note 7, at 79.

149. *See* HEW Report, *supra* note 140, at 43; REGAN, *supra* note 7, at 78–79. This political dynamic in the development of privacy law has continued to this day. Industry lobbyists argue that information practices have not resulted in significant economic loss to individuals and that greater protection of privacy would cost the rest of society more than any harm done to the individuals affected. *See* Reidenberg, *supra* note 134, at 724; William S. Challis and Ann Cavoukian, *The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective,* 19 JOHN MARSHALL J. COMPUTER AND INFO. L. 1, 4 (2000); Joel R. Reidenberg, *Governing Networks and Rulemaking in Cyberspace,* 45 EMORY L. J. 911, 922 (1996).

150. REGAN, *supra* note 7, at 79.

151. *Id.*

152. Influential in the debates was this statement by President Ford:

> I do not favor the establishment of a separate Commission or Board bureaucracy empowered to define privacy in its own terms and to second guess citizens and agencies. I vastly prefer an approach which makes Federal agencies fully and publicly accountable for legally mandated privacy protections and which gives the individual adequate legal remedies to enforce what he deems to be his own best privacy interests.

123 CONG. REC. 162, H10962 (1974). *See* REGAN, *supra* note 7, at 79–80.

153. Debates over privacy policy did not end in 1974. Congressional committees held more than 150 days of hearings dealing with privacy policy between 1965 and 1988, excluding those on the privacy aspects of the FCRA. During the same period, congressional staff released more than a dozen reports on the subject. *See* REGAN, *supra* note 7, at 7.

Act).[154] In its final form, the law provided the lowest level of protection that policy makers were considering at the time.[155] The statute covered only federal agencies and did not establish a separate entity to oversee government information processing practices. With regard to digital databases, the policy resolution was more procedural than substantive. From the beginning of the debates, database technology had been a primary concern. A stated objective of the Privacy Act was to restrict the government's use of technology to invade privacy interests, and the Privacy Act even included a statement that digital technology "greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information."[156] The solution to this growing problem, however, was not to impose substantive limits on the use of technology in collecting and sharing information, but to create a handful of procedural safeguards to give individuals a right of access to their files, an opportunity to correct errors, and a right to demand disclosure about records under certain circumstances.[157] The only notable substantive limit in the Privacy Act was the imposition of standards of fair information handling on federal agencies to reduce the likelihood of mistakes or inadvertent disclosure to unauthorized sources, and even here the standards were vague and riddled with loopholes.[158]

The Privacy Act is generally considered weak and ineffectual by today's standards.[159] Although the privacy interest was properly defined throughout the years of legislative debates as the right to control information about oneself, the most seriously debated solutions merely quibbled over how individuals could effectively guard this right.[160] On paper, the Privacy Act guaranteed access to one's own records and the right to correct inaccurate or irrelevant information. But these rights were not easily exercised because the costs, in time and money, were high both for the individuals involved and the agencies covered by the law.

---

154. 5 U.S.C. § 552(a) (2000).

155. Regan, *supra* note 7, at 82.

156. 5 U.S.C. § 552(a), Pub. L. 93-579, § 2(a)(2) (congressional findings and statement of purpose). *See* Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LEGAL LANDSCAPE 193, 195 (Philip E. Agre & Marc Rotenberg eds., 1997).

157. REGAN, *supra* note 7, at 81–82.

158. *See* Gellman, *supra* note 156, at 195–96.

159. *See id.* at 196–98. Gellman deftly illustrates the shortcomings of the Privacy Act as a means of satisfying the list of six Fair Information Practices developed a year earlier in the HEW Report. *See* HEW REPORT, *supra* note 140.

160. *See* REGAN, *supra* note 7, at 100.

For example, individuals were given the right not to have their information shared among agencies without their consent, but obtaining consent from massive numbers of people was impracticable.[161] It was suggested that individuals be notified prior to sharing their information, but privacy advocates questioned whether this would give individuals a bona fide choice, and agencies complained that the expense of mass paper notification would outweigh any efficiencies gained from database technologies.[162]

The Privacy Act had other deficiencies. It had no specific enforcement or oversight structure for ensuring compliance with the statute's limitations on information collection.[163] It limited the internal use of personal information to those agency employees who had a need to know the information in the performance of their official duties, but this proved to be a vague standard incapable of systematic enforcement.[164] There was no requirement that information be used only for purposes related to the original reason for gathering it.[165] No administrative process provided a safeguard or review process for internal agency use. Individuals have occasionally objected to specific uses as unauthorized by law, but in most litigated cases the agency has prevailed.[166]

Perhaps the most glaring failure of the Privacy Act is the manner in which it addresses the disclosure of information to external sources. Agencies have been permitted to disclose records for virtually any purpose if the agency can establish that disclosure is for "routine use," or it can satisfy the statute's procedural requirements for notice by advance

---

161. *See* REGAN, *supra* note 7, at 86–87.

162. *See* REGAN, *supra* note 7, at 96–99. Ultimately "Data Integrity Boards" (the Boards) were created in the late 1980s as intermediaries between individuals and agencies that wanted to share information or run matching programs with databases maintained by other agencies. The Boards, which every federal agency doing computer matching was required to create, had authority to reject database matching programs before they were implemented. The idea was borrowed from the Defense Department, which had implemented a similar privacy board to comply with its obligations under the Privacy Act of 1974. *See* REGAN, *supra* note 7, at 95–100. Gellman, *supra* note 156 at 200.

163. In contrast, the Paperwork Reduction Act, 44 U.S.C. § 3507, calls for a specific administrative approval process before a federal agency collects information covered by the Act. The Office of Management and Budget (OMB) oversees both the Paperwork Reduction Act and the Privacy Act, but it devotes far more resources to the Paperwork law. *See* Gellman, *supra* note 156, at 197.

164. *See Solove, supra* note 32, at 1166.

165. *See* Gellman, *supra* note 156, at 198–99; *See Solove, supra* note 32, at 1167.

166. *See* DEPARTMENT OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE AND PRIVACY ACT OVERVIEW 478–80 (1994); Gellman, *supra* note 156, at 198.

publication in the Federal Register.[167] Neither has been an effective limit on information collection and sharing.[168] Consequently, the Privacy Act became more of a procedural impediment for federal agencies and a symbolic, but ineffectual law for citizens, far less protective of individuals' privacy interests than other alternatives would have ensured.[169]

Congress has not materially revised the Privacy Act since 1974 because efforts to strengthen the law have met strong resistance. Three years after the Privacy Act was enacted, a report of the Privacy Protection Study Commission (PPSC)[170] resurrected the idea of creating a federal Privacy Board that would monitor and implement privacy legislation and advise on the privacy implications of proposed legislation.[171] Advocates of the idea saw the Board serving as an "influential prodding structure,"[172] which would have supplemented self-policing legislation such as the FCRA that calls upon individuals to monitor their own privacy interests. The recommendations of the PPSC were never enacted, however, due in part to strong opposition from government agencies, trade associations, and other organizations that were enjoying the benefits of more relaxed controls on information sharing.[173] In addition, although President Carter supported efforts to protect privacy in principle, establishing a federal Privacy Board conflicted with his view of limited federal involvement in this and other policy issues at the time.[174]

---

167. Limited oversight by the OMB and Congress also has some controlling effect on the external sharing of personal information. *See* HOUSE COMMITTEE ON GOVERNMENT OPERATIONS, WHO CARES ABOUT PRIVACY? OVERSIGHT OF THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS, H.R. No. 98-455, 98th Cong., 1st Sess. (1983).

168. *See* Gellman, *supra* note 156, at 198.

169. *See id.*

170. The Privacy Protection Study Commission (PPSC) was established by the Privacy Act of 1974 to examine the need for privacy legislation governing the private sector and to review the need for a general oversight body to ensure compliance with privacy rules by the federal government. *See* REGAN, *supra* note 7, at 81–82.

171. THE REPORT OF THE PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 36 (Washington, D.C.: Government Printing Office, 1977) [hereinafter PPSC REPORT].

172. *Id. See* REGAN, *supra* note 7, at 84–85.

173. *See* REGAN, *supra* note 7, at 85.

174. *See id.* at 86. The decision to reject a federal Privacy Board was critical. Public policy analysts have long recognized that the institutions chosen to pursue a public policy goal will profoundly affect the ultimate public policy resolution. *See* J. Brooke Overby, *An Institutional Analysis of Consumer Law*, 34 VAND. J. TRANSNAT'L L. 1219, 1232 (2001) ("Under an institutional

As it turned out, an important role for a national oversight body became apparent two years after the PPSC report was issued. In an effort to reduce welfare fraud, HEW created Project Match, which compared the digital records of federal employees to the records of individuals who received benefits under the entitlement program Aid to Families with Dependent Children.[175] In March 1979, the Office of Management and Budget (OMB) issued guidelines for Project Match and allowed it to proceed over the objections of a few federal agencies and numerous privacy advocates.[176] Critics observed that the Privacy Act prohibited the use of information for purposes other than those for which it was initially collected, unless the individual gave affirmative consent to the different use.[177] The OMB guidelines permitted the matching so long as the agency complied with certain procedural requirements, including advance notice in the Federal Register, and established that the matching would have "demonstrable financial benefit" exceeding its costs.[178] Agencies did not follow the procedural guidelines in many cases, however, and the public did not respond to the Federal Register notices. Because there was little congressional opposition to the matching program, the practice grew over time. The only group with a vested interest in protesting the program was the class of individuals under investigation, but they were not aware that their records were being matched until the results of the matching detected a conflict.[179]

---

framework, the social policy aims of consumer law must be balanced with the question of institutional and organizational choice—for example, by considering whether a goal is better accomplished through a particular type of rule and through a particular mechanism, such as markets, state legislatures, federal legislatures, and so forth.").

175. *See* Kenneth Langan, *Computer Matching Programs: A Threat to Privacy?*, 15 COL. J.L. & SOC. PROBS. 143, 144–45 (1979); John Shattuck, *Computer Matching Is a Serious Threat to Individual Rights*, COMMUNICATIONS OF THE ACM 27, no. 36 (June 1984) at 538; Laura Weiss, *Government Steps Up Use of Computer Matching to Find Fraud in Programs*, CONGRESSIONAL QUARTERLY WEEKLY REPORT, Feb. 26, 1983, at 432; Jake Kirchner, *Privacy—A History of Computer Matching in the Federal Government*, COMPUTERWORLD, Dec. 14, 1981, at 1.

176. *See* REGAN, *supra* note 7, at 86–87.

177. *See id.*

178. *Privacy Act of 1974: Supplemental Guidance for Matching Programs*, 44 Fed. Reg. 23,138 (Apr. 18, 1979). This cost/benefit analysis was frequently ignored by agencies, and the requirement was dropped from the guidelines in 1982. REGAN, *supra* note 7, at 95–96.

179. *See* REGAN, *supra* note 7, at 86–87. The cost savings from the matching program were debatable. *See* Jeffrey Rothfeder, *Is Nothing Private?*, BUSINESS WEEK, Sept. 4, 1989, at 74 (discussing conclusions of a 1986 study by the General Accounting Office). Matching has been used to detect fraud and mistakes in other federal benefit programs. *See, e.g.*, Jaffess v. Secretary of HEW, 393 F. Supp. 626 (S.D.N.Y. 1975) (upholding match of recipients receiving veterans' disability benefits with recipients of social security benefits as a "proper" administrative purpose).

For the next several years, privacy did not disappear from the congressional agenda, but the importance of other governmental interests—particularly operational efficiency and improved law enforcement—took on greater importance. Catching "welfare cheats" through information sharing was more important than limiting governmental intrusions on privacy interests.[180] Nevertheless, the increased use of computer matching during the late 1970s and early 1980s reawakened privacy advocates and reopened the debate.[181] The number of computer matches performed by federal agencies had almost tripled by 1984,[182] the Orwellian year of reckoning that once again brought Big Brother to the front pages and privacy concerns to the public policy stage. Also during this period, the capabilities of computerized databases were expanding rapidly, making it possible for governments and private organizations to monitor the activities of individuals to an unprecedented degree.[183]

By 1986, increased concern about information privacy prompted the Office of Technology Assessment (OTA) to survey the practices of federal agencies on database sharing and privacy protection.[184] The OTA's analysis revealed that new applications of information technology were undermining the principal goal of the Privacy Act—to give individuals more control over their personal information. The study concluded that widespread information collection, sharing, and computer networking was leading to the creation of a "de facto national database" containing information about most every person residing in the United States.[185] This was the same concern that had ignited the privacy debate more than twenty years earlier.[186]

---

180. *See* REGAN, *supra* note 7, at 92.

181. *See id.*

182. *See id.* at 94 and n.83.

183. *See* Gary T. Marx & Nancy Reichman, *Routinizing the Discovery of Secrets: Computers and Informants*, 27 AM. BEHAVIORAL SCIENTIST 425, 425 (1984); John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching and Privacy in the United States*, 35 HASTINGS L.J. 991, 991–95 (1984).

184. UNITED STATES CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, OTA-CIT-296 (Washington, D.C.: Government Printing Office, June, 1986) (survey of 142 agency components covering various aspects of Privacy Act compliance).

185. *See* REGAN, *supra* note 7, at 95.

186. *See supra* note 138 and accompanying text.

In response to the concern about data matching, Congress enacted the Computer Matching and Privacy Protection Act (CMPPA) in 1988.[187] The legislation required agency review and cost-benefit analysis before computer matching could be performed, and it instituted other procedural requirements in an effort to curb abuses.[188] But the ultimate effect of the CMPAA was not to limit, but to legitimize, computer database sharing in the federal government. Rather than address privacy and surveillance concerns, the law took the same approach as the Privacy Act by emphasizing procedural and administrative goals rather than imposing limits on what kind of data could be collected and how it could be used.[189]

With respect to privacy protection in the federal government, not much has changed since the late 1980s. The PPSC report in 1977 observed that "neither law nor technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him."[190] Twenty-five years later, this statement rings truer than ever.

C. Protecting Privacy in the Private Sector

On the subject of information privacy outside of government,[191] the Privacy Act charged the PPSC with studying the issue and making recommendations to Congress.[192] As the PPSC considered the relevant public policy interests in regulating information practices, it took the position that privacy was both a "societal value" and an "individual interest."[193] Because record-keeping relationships were "inherently

187. 5 U.S.C. § 552(a) (2000). For a discussion of the legislative history of the CMPAA, see REGAN, *supra* note 7, at 95–99.

188. *See* REGAN, *supra* note 7, at 96–97.

189. *See* DAVID A. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 357 (1989).

190. PPSC Report, *supra* note 171, at 8. *See* Reidenberg, *supra* note 134, at 722.

191. Although privacy protection laws in the United States usually apply to either the public or private sector, the line between the two in information sharing is often blurred. The FBI, for example, routinely purchases information from privately assembled databases in its crime investigations. *See* Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask Choicepoint*, WALL ST. J., Apr. 13, 2001, at A1; Reidenberg, *supra* note 134, at 721.

192. *See* PPSC Report, *supra* note 171, at 621–38 (schedule of hearings from credit, banking, insurance and other economic sectors); REGAN, *supra* note 7, at 83.

193. PPSC Report, *supra* note 171, at 21.

social" the societal interest could not be ignored.[194] The PPSC developed a list of "significant societal values and interests" against which privacy should be balanced, including First Amendment concerns, freedom of information policies, law enforcement priorities, cost implications, and federal-state governmental relations.[195] But in deciding how these interests should be balanced, the PPSC ultimately lost sight of the "societal value" of maintaining privacy and treated privacy protection as largely a problem of individual concern.

As the PPSC viewed the policy problem, the goal was to strike the right balance between an individual's interest in keeping his or her personal information private and the need for governments and businesses to gain access to that information for various societal purposes.[196] Consistent with the philosophical literature on privacy that had been circulating during this period, the PPSC recognized in principle that privacy has a societal value apart from each individual's own privacy interests, but the group did not develop that value further.[197] Only the societal benefits to governments and businesses were taken into account.

Consistent with the view of privacy as a matter of individual concern, the PPSC Report ultimately concluded that privacy policy in the private sector should begin with a voluntary, market-oriented approach.[198] As is the case with most market mechanisms, the conclusion was premised on the principle of individual choice and the idea that individuals could asses their own risks of harm. If individuals were given the right to assert their own privacy interests, they would take measures to protect themselves, and organizations that collect and maintain information would have incentives to honor privacy concerns voluntarily. Only if voluntary compliance proved ineffective would mandatory enforcement mechanisms be imposed. Moreover, existing federal agencies, such as the FTC and state insurance regulators, were seen as appropriate control mechanisms to the extent that some government oversight was needed. A

194. *Id.*

195. *Id.*

196. *Id.* at 29 ("A major interest that must be weighed in the balance of organizations' needs for information against the individual's interest in having his personal property protected is society's interest in maintaining the integrity of the Federal system.").

197. *See* REGAN, *supra* note 7, at 84.

198. PPSC REPORT, *supra* note 171, at 32.

federal Privacy Board or similar agency that would act as guardian of the societal value in privacy protection was deemed unnecessary.[199]

This legislative evolution was not surprising given the political and economic conditions. Protecting information privacy threatened defined and influential stakeholders—government agencies, employers, marketing firms, law enforcement—all of whom were just beginning to see the advantages of information technologies. All had an interest in collecting and sharing as much information as possible. Each of these stakeholders thus had incentives to redefine the issue from the ideal of privacy as a foundational societal value to some lesser ideal that required the balancing of other societal concerns—efficiency, productivity, crime control, etc.—against the individual harms that might be caused by data collection and sharing.

The result was a legislative process that quickly involved the balancing of competing interests, and the focus of debates centered on whose particular interests would be jeopardized by limiting information collection and sharing, and whether jeopardizing those interests was worthwhile. Privacy advocates were again put on the defensive to carry the burden of showing how a particular data collection or sharing activity invaded privacy and, even if it did, showing that protecting the privacy interest was not outweighed by the interests of others in gaining access to the information in question.[200] This was another burden privacy advocates could not carry. This political dynamic, which has since been repeated numerous times, has led to a set of privacy laws that are sectoral in their scope and largely consist of narrowly applicable privacy provisions that do not cover the vast array of today's data collection and sharing activities.[201] Even in the sectors covered by legislative enactments, there is a heavy reliance on market-based solutions and laws that require individuals to police their own data protection interests.

1. The Fair Credit Reporting Act and the Rise of Market-Based Solutions

As it turns out, the emphasis on market solutions to the privacy problem in the 1970s foreshadowed a general shift in the perception of

199. *Id. See* REGAN, *supra* note 7, at 84.

200. *See* REGAN, *supra* note 7, at 174–75.

201. *See* Bradley Slutskey & Allison Brantley, *Privacy on the Internet: A Summary of Government and Legal Responses*, 637 PLI/Pat 85 (2001); Reidenberg, *supra* note 134, at 726. For a list of federal privacy laws, see Gellman, *supra* note 156, at 202.

privacy invasion in the following decades.[202] The anti-regulatory position was reinforced in 1997 when the Clinton White House released a report entitled "A Framework for Global Electronic Commerce."[203] The first principle stated in the Framework is that "the private sector should lead" the development of electronic commerce.[204] The section on privacy calls on private industry to work with consumer groups to develop a self-regulatory environment.[205]

With market-based solutions as the presumed control mechanism, stakeholders in the formulation of privacy policy, whether proponents of data collection, consumer groups, or privacy advocates, became partners with largely similar objectives, differing only over the details. Resulting regulatory schemes now involve a voluntary component that has the effect of neutralizing public concern but with few enforceable restrictions on the use and misuse of data.[206] Privacy rights have been treated primarily as commercial policy problems, rather than fundamental civil rights. Debates are often framed as if privacy were a consumer issue (e.g., caller identification blocking). Resulting laws do little to prevent or limit the collection of information in the first instance, and their success depends on individuals to seek remedies when legal norms are broken, much as they do with other consumer laws.

This self-policing approach had an early precedent in the FCRA,[207] the first major federal privacy legislation in the United States and arguably the most detailed to date.[208] The FCRA limits the uses for which credit

---

202. *See* Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity and a Practical Guide to Protecting Your Client, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 144 (Philip E. Agre & Marc Rotenberg eds., 1997).

203. W.J. Clinton & A. Gore, *A Framework for Global Electronic Commerce, available at* http://www.nyls.edu/cmc/papers/whgiifra.htm (July 1, 1997).

204. *Id.*

205. *Id.* at II, Legal Issues, § 5, par. 17.

206. David Flaherty aptly observed in 1979 that the "public is being lulled into a false sense of security about the protection of their privacy by their official protectors, who often lack the will and energy to resist successfully the diverse initiatives of . . . the 'information athletes' in our respective societies." *See* Davies, *supra* note 202, at 156–57.

207. 15 U.S.C. §§ 1681–1681(u) (2000).

208. *See* Gellman, *supra* note 156, at 202. Privacy legislation at the state level has been sporadic, in part because some courts have held that state laws regulating information trafficking can violate the Commerce Clause. *See* ACLU v. Johnson, 194 F.3d 1149, 1160–63 (10th Cir. 1999); American Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997). For information on state privacy laws generally, see ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1997); Electronic Privacy Information Center, Privacy Laws by State, *available at* http://www.epic.org/privacy/consumer/states.html (last visited Jan. 20, 2003).

reporting companies can release the information in a consumer's file. It provides that consumers may see their files and correct mistakes, and relies heavily on consumers to ensure the accuracy of their own records.[209] Yet only in recent times, more than twenty years after the enactment of the FCRA, have a significant number of consumers learned how to locate their credit reports and take steps to ensure their accuracy and completeness.[210] This improvement is due in part to the increased access to information about credit reports on the Internet.[211] Even so, most consumers have no idea how to police their rights under the FCRA.[212]

Even with its deficiencies,[213] the self-policing scheme of the credit reporting system is at least feasible for many consumers because most

---

209. *See* James P. Nehf, *A Legislative Framework for Reducing Fraud in the Credit Repair Industry*, 70 N.C. L. REV. 781, 786–87 (1992).

210. United States Public Interest Research Group, *Mistakes Do Happen: Credit Report Errors Mean Consumers Lose* [hereinafter PIRG], *at* http://www.pirg.org/reports/consumer/mistakes/index.htm (March 1998); (concluding that it is still difficult for many consumers to obtain their own credit report; participants in a survey had to make several calls, deal with busy signals, and remain on hold numerous times to obtain their credit reports). *See Information Resources, A Summary of Your Rights Under the Fair Credit Reporting Act*, *available at* http://www.informationresources.com/faircredit.htm (2002) (explaining a consumer's right to view the contents of a credit report, and the conditions under which the report must be provided free of charge).

211. R. Ken Pippin, *Consumer Privacy on the Internet: It's Surfer Beware*, 47 A.F. L. REV. 125, 146 (1999) ("Credit report information is becoming more accessible on the Internet as credit reporting agencies take advantage of this growing business medium. Although a credit report is only supposed to be available to authorized customers, over-disclosure and unauthorized disclosure are certainly possible, if not more likely, on the Internet.").

212. PIRG, *supra* note 210, at Executive Summary (warning that "until policymakers and credit bureaus do what it takes to allow consumers to have free and easy access to their credit reports and set tougher standards to prevent and clean-up mistakes, too many credit reports will remain a ticking time bomb of dangerously inaccurate information," recommending that each national credit bureau annually and automatically mail a copy of each consumer's report, and urging that increased duties to ensure accuracy and avoid errors be imposed on banks, department stores and other firms that furnish information to credit bureaus); *Consumers Union, Credit Bureau Nightmares: Victims Speak Out*, *available at* http://www.consumersunion.org/finance/vict.htm (Sept. 29, 1997) (discussing and illustrating the difficulty of having mistakes removed from a credit report); Dagen McDowell, *How to Fix Credit Errors: Be Ready to Dog the Process Every Step of the Way*, ABCNEWS.COM, *available at* http://abcnews.go.com/sections/business/TheStreet/dagen000714.html (July 14, 2002).

213. Among its weaknesses, 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 information, and birthdate) to various commercial entities. The FCRA does little to equalize the unbalanced power relationship between individuals and credit reporting companies, and the vast amount of information in credit reports can be obtained for many commercial purposes. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO. L. REV. 1153, 1206 (1997).

injuries caused by inaccurate information in a credit report will be made known to a consumer shortly after the harm occurs. The statute requires a user of a credit report, such as a creditor, employer, or insurance company to whom the consumer has applied, to inform the consumer if adverse action was taken in reliance on information in that report.[214] This disclosure must identify the source of the credit report and tell the consumer that she has a right to see her report and correct any inaccuracies.[215] Thus, in the ordinary course of events, a consumer will learn that a wrong has occurred and will be able to identify the problem by tracing it to the reporting agency that issued the mistaken credit history. Outside of the scope of the FCRA, this kind of feedback information is much less accessible, if at all.

2. *Other Privacy Statutes that Rely on Individual Self-Policing*

Unfortunately, privacy statutes subsequently enacted follow the FCRA model in this respect and rely largely on individual self-policing as the primary control mechanism, but they do not create a similar framework for ensuring that an individual will learn about a problem when it occurs. In a few instances, these laws have been reasonably successful. For example, the Family Educational Rights and Privacy Act of 1974 (FERPA),[216] regulates the disclosure of student records. The statute imposes controls on the release of student transcripts, disciplinary files, and other records without the student's (or parent's) consent.[217] One of the principle reasons why the law protects student privacy interests is that there are few lawful reasons for disclosure. Accordingly, there are few opportunities for even honest mistakes to be made. In addition, information in student records is controlled by a well defined, relatively small set of information keepers, the educational institutions, who have few incentives to disclose information about their students anyway. Information in student records has long been considered personal,

214. 15 U.S.C. § 1681(m) (2000). For example, if a consumer applies for a store credit card and is denied, the store must inform the consumer that a credit report was relied upon in making the decision, and it must give contact information so the consumer can find out what information is in the report.

215. *Id.*

216. 20 U.S.C. § 1232(g) (2000). FERPA is also known as the "Buckley Amendment."

217. *See* 20 U.S.C. § 1232(g)(b).

possibly embarrassing, and sometimes hurtful if disclosed.[218] Consequently, schools usually prefer not to disclose student records, and they have resisted market incentives to do so.[219] Indeed, the law gives schools legal cover to refuse information requests that they would prefer to decline.

Other privacy laws that rely on individual self-policing have proved less successful. The Cable Communications Policy Act of 1984 (CCPA)[220] prohibits cable operators from disclosing information about the viewing habits of subscribers. It also requires cable companies to have privacy policies that inform subscribers about the nature of information collected and how it will be used.[221] The law contains a broad exception, however, that permits the disclosure of personal information for a "legitimate business activity."[222] Moreover, the recently enacted USA Patriot Act[223] reduces the privacy protections afforded to cable Internet users. Before the terrorist attacks of September 11, 2001, the CCPA required cable companies to notify and grant a hearing to cable subscribers when their confidential information was subject to disclosure to the government.[224] The USA Patriot Act took those rights away from cable broadband subscribers.

In 1986, Congress updated wiretapping and clandestine surveillance limitations with the Electronic Communications Privacy Act of 1986 (ECPA).[225] The ECPA extends the protections of the Federal Wiretap Act of 1968 to the government's unauthorized interception of modern forms of communications, including cellular phones, e-mail, and computer transmissions.[226] The focus of the law, which draws heavily on the Big Brother metaphor, is on eavesdropping and monitoring communications

---

218. *See, e.g., Porten v. Univ. of San Francisco,* 64 Cal. App. 3d 825, 832, 134 Cal. Rptr. 839, 843 (1976) (recognizing cause of action for privacy invasion when university released student transcript to scholarship commission without authorization).

219. Market incentives in some instances might favor nondisclosure. To the extent an educational institution relies upon good alumni relations to finance its operations, disclosing student information to outside entities could damage the school's ability to raise funds from its alumni base.

220. 47 U.S.C. § 551 (2000).

221. *Id.* § 551 (a)(1).

222. *Id.* § 551(c)(2)(A).

223. Pub. L. No. 107-56, 209-212, 224, 115 Stat. 272, 283–85, 295 (2001).

224. 47 U.S.C. § 551(c), *amended by* USA Patriot Act, Pub. L. No. 107-56, §211, 1115 Stat. 272, 28384(2001).

225. 18 U.S.C. §§ 2511–20, 2701–07 (2000).

226. *See* Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?,* 3 COMM. L. CONSPECTUS 63, 66–67 (1995).

between one person or computer and another.[227] The ECPA does not otherwise limit the collection and use of personal data, and its usefulness as a limitation on cookie technology, web bugs, clickstream data recovery, and other surreptitious Internet data mining is uncertain.[228] Moreover, the law governs only the disclosure of records to government entities, so in the absence of a state law, service agreement or privacy policy to the contrary, Internet service providers are free to share the e-mail of their subscribers with non-governmental entities.[229] Even the limited protection of the ECPA is in some jeopardy in the aftermath of September 11, 2001 because law enforcement agencies perceive a need to monitor e-mail and other electronic communications more rigorously and share information more freely among each other.[230]

A related federal statute is the Computer Fraud and Abuse Act of 1986 (CFAA),[231] also known as the "anti-hacking" statute, prohibits persons from obtaining access to a computer without authorization. The applicability of the CFAA was at issue in *In Re DoubleClick, Inc. Privacy Litigation*.[232] In that case, the federal district court held that the CFAA did not bar the use of cookies and other data mining activities online, and that the statutory minimum of $5,000 in damages under the CFAA was not satisfied.[233] Although litigation on the scope of this statue continues, the $5,000 minimum damage threshold significantly limits the

227. *See* Peter Murphy, *An Examination of the United States Department of Justice's Attempt to Conduct Warrantless Monitoring of Computer Networks Through the Consent Exception to the Wiretap Act*, 34 CONN. L. REV. 1317, 1321 (2002) (explaining purpose of the ECPA).

228. The ECPA contains two distinct causes of action relevant to data collection. The first prohibits the unauthorized interception of electronic communications in transit. 18 U.S.C. § 2511. The second prohibits unauthorized access to stored electronic communications. *Id.* § 2701. Plaintiffs have argued both sections in recent litigation. The majority of decisions have held that the ECPA is not violated by the use of cookies, web bugs and similar data mining tools. *See* In re Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. LEXIS 16947, at *28 (N.D. Cal. Oct. 9, 2001); In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001). *Cf.* In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1278 (C.D. Cal. 2001) (district court refused to dismiss a claim based on one aspect of the ECPA—unauthorized access to stored information—although the court agreed with the *DoubleClick* decision on other claims).

229. 18 U.S.C. § 2703. *See* Vanessa Hwang, *Cable Modems and Privacy in the New Millennium*, 32 COLUM. HUMAN RIGHTS L. REV. 727, 745 (2001).

230. *See supra* note 12; Abraham McLaughlin, *CIA Expands Its Watchful Eye to the U.S.*, CHRISTIAN SCIENCE MONITOR, Dec. 17, 2001 (describing how USA Patriot Act expands the authority of law enforcement agencies to share information).

231. 18 U.S.C. § 1030 (2000).

232. 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001).

233. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (holding CFAA required proof of loss of at least $5,000).

usefulness of the CFAA. Some courts have held that damages under the CFAA may be aggregated in a class action, but they can only be aggregated with respect to a single act of wrongful conduct.[234] Other courts have denied aggregation of claims altogether.[235] Moreover, the CFAA has a mens rea requirement that is difficult to establish.[236]

Congress enacted the Video Privacy Protection Act of 1988 (VPPA)[237] in response to the disclosure of Robert Bork's video rental information to reporters during his contested U.S. Supreme Court confirmation hearing in the Senate.[238] The VPPA prohibits video stores from disclosing information about the titles of video cassettes rented or purchased unless the customer has given prior written consent.[239] The VPPA relies primarily on customer self-policing for enforcement, and creates a private cause of action only against stores that knowingly make prohibited disclosures.[240] The statute expressly permits disclosure of the subject matter of video sales and rentals to marketing firms, and to any person if the disclosure takes place in the "ordinary course of business."[241]

The Telephone Consumer Protection Act of 1991 (TCPA)[242] addresses information privacy only at the margin. The TCPA permits individuals to sue a telemarketer for certain automated dialing calls and unauthorized faxes.[243] The TCPA is concerned primarily with the aggravation of disruptive phone calls. It does not limit the collection, use, or transfer of

234. *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 15 (D. Mass. 2002); Ingenix, Inc. v. Lagalante, 2002 U.S. Dist. LEXIS 5795, at *17 (E.D. La. Mar. 28, 2002).

235. In *Thurmond v. Compaq Computer Corp.*, 171 F. Supp. 2d 667, 680 (E.D. Tex. 2001), the court held that the $5,000 aggregated loss must be to no more than one computer. *See also In re DoubleClick*, 154 F. Supp. 2d at 523. The *Thurmond* court stated that damages could not be aggregated among individual plaintiffs, relying in part on Attorney General Janet Reno's statement that "we may need to strengthen the Computer Fraud and Abuse Act by closing a loophole . . . [which would] escape [from] punishment if no individual computer sustained over $5,000 worth of damage." 171 F. Supp. 2d at 680–81.

236. *See In re Pharmatrak, Inc. Privacy Litig.*, 2002 U.S. Dist. LEXIS 15293, at n.93.

237. 18 U.S.C. § 2710–11 (2000).

238. *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L. J. 1085, n.430 (2002); Francoise Gilbert and Brad Laybourne, *Privacy Issues for the Global Company*, 724 PLI/PAT 291, n.4 (2002).

239. 18 U.S.C. § 2710(a)(4) (definition of "video service provider" covered by the law).

240. *Id.* §§ 2710(b)(1), 2710(c) (the aggrieved person may recover actual damages, statutory damages in the amount of $2,500, punitive damages and attorney's fees).

241. *Id.* §§ 2710 (b)(2)(D)(ii), 2710(b)(2)(E).

242. 47 U.S.C. § 227 (2000).

243. *Id.* § 227(b) (actual damages or a statutory award of $500; treble damages for willful violations).

personal data.[244] In the same vein, many states have recently passed "no call" legislation to supplement the federal law.[245] These laws represent important consumer rights legislation because by registering on a state-administered list, an individual can keep her name and phone number off of most telemarketing calling lists, but they do little to protect the privacy of information in digital databases.

An important step in the protection of individual records was the Driver's Privacy Protection Act of 1994 (DPPA),[246] which forces states to obtain a driver's consent before disclosing personal information. Although the DPPA is an important development in controlling government disclosures of "public records" to the private sector, it applies only to motor vehicle records, and it authorizes the sharing of information in many circumstances. The legislation exempts law enforcement authorities, the automotive industry, government agencies, the insurance industry, debt collectors, businesses that want to verify certain identifying information, researchers, private investigators, and several other categories of inquirers.[247]

In 1996, Congress addressed the critically important issue of health information privacy in the Health Insurance Portability and Accountability Act (HIPAA).[248] HIPAA did not contain detailed substantive restrictions on information sharing in the health sector, but it required the Department of Health and Human Services (HHS) to promulgate regulations dealing with the privacy of medical records. HHS published its regulations under HIPAA in December 2000.[249] The privacy

244. *See Solove*, supra note 31, at 1442.

245. *See, e.g.*, IND. CODE § 24-4.7-1 (2002). The law exempts several categories of callers, including a call made "primarily in connection with an existing debt or contract for which payment or performance has not been completed." This would include calls from creditors with whom the consumer already carries outstanding balances. Since many telemarketing calls are solicitations from current creditors of the consumer (e.g., the creditor trying to sell credit insurance), this is a significant exception. It also exempts calls made by a charitable organization, a licensed real estate broker, a licensed insurance agent, and a newspaper of general circulation. *Id.* § 24-4.7-1(a).

246. 18 U.S.C. § 2721 (2000).

247. *Id.* § 2721(b). *See* REGAN, *supra* note 7, at 103.

248. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at 42 U.S.C. § 1320d-2 (2000)).

249. 45 C.F.R. § 164.500 (2002). For an account of the legislative history of the HIPAA statute, see REGAN, *supra* note 7, at 105–07. As stated in the Federal Register, "The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the

rules, which take effect in April 2003, will govern the use and dissemination of health information and will apply to health plans, health care clearinghouses, and certain health care providers.[250] HIPAA requires that a covered institution obtain consent or authorization prior to using or disclosing protected health information to carry out treatment, payment, or health care operations, and contains many other requirements to safeguard patient medical information.[251] Even without written consent or authorization, there are provisions within HIPAA which permit dissemination of patient information when identifying information has been removed.[252] Both civil and criminal penalties are provided for non-compliance with the mandates of the privacy regulations.[253]

---

privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors." 65 Fed. Reg. 82461 (Dec. 28, 2000).

250. 45 C.F.R. § 164.104.

251. 45 C.F.R. §§ 164.506(a), 164.508(a)(1) (2001), and Subpart E of the regulation generally. Beyond HIPAA's requirement for consent or authorization, and the necessary review of medical records for identifying information, the HHS rules require additional steps to safeguard patient medical information, including: the right to adequate notice to patients of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information, *Id.* §164.520; the need to ensure that patients may receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, with certain exceptions, *Id.* § 64.528; the need to maintain documentation (including policy and procedure documents, communications, and other specified documents) for a period of six years, *Id.* §164.530; and the need to provide training to all members of a covered entity's workforce on policies and procedures with respect to protected health information required by HIPAA. *Id.* §164.530(b).

252. Regulations concerning these "de-identification" procedures specify numerous identification elements, including (a) names; (b) all geographic subdivisions smaller than a State, including street address, city, county, precinct, and zip code; (c) all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89; (d) telephone numbers; (e) fax numbers; (f) electronic mail addresses; (g) social security numbers; (h) medical record numbers; (i) health plan beneficiary numbers; (j) account numbers; (k) certificate or license numbers; (l) vehicle identifiers and serial numbers, including license plate numbers; (m) device identifiers and serial numbers; (n) web Universal Resource Locators (URLs); (o) Internet Protocol (IP) address numbers; (p) biometric identifiers, including finger and voice prints; (q) full face photographic images and any comparable images; and (r) any other unique identifying number, characteristic, or code. *See id.* §164.514(b)(2)(i)-(ii).

253. Affected entities may be subject to civil monetary penalties of up to $25,000 per person, per year, per standard. 42 U.S.C. § 1320d-5 (2002). In addition, federal criminal penalties may be imposed for the knowing, improper disclosure of information or the obtaining of information under false pretenses, with higher penalties prescribed for offenses involving actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and ten years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm. *Id.* § 1320d-6.

The Children's Online Privacy Protection Act of 1998 (COPPA)[254] was the first federal law to specifically address Internet privacy concerns. The Act, which was prompted by an FTC study that found widespread abuses of privacy interests on web sites directed at children,[255] seeks to limit the collection of personal information about children under age thirteen. If a website or web page is aimed at an audience predominantly comprised of children, it must post a privacy policy and obtain parental consent for the collection, use, or disclosure of personal information.[256] COPPA applies only to sites that are "directed to children" or sites where the operator has "actual knowledge" that it is collecting information from children under thirteen.[257] Moreover, it is primarily a disclosure law that imposes a strict privacy policy on Internet sites within its reach, and it relies primarily on individual enforcement for its success. It also contains a number of important exceptions.[258]

The Gramm-Leach-Bliley Act of 1999[259] presented Congress with an opportunity to enact meaningful privacy legislation in the financial services industry, but the law serves primarily as an enabling statute that imposes few limits on the collection and sharing of information. The Gramm-Leach-Bliley Act expressly authorizes banks, insurers, investment companies, and other financial services organizations that are "affiliated" with each other, through common ownership or otherwise, to

254. 15 U.S.C. § 6501 (2000). *See generally* Laurel Jamtgaard, *Big Bird Meets Big Brother*, 16 COMPUTER & HIGH TECH. L.J. 385 (2000).

255. In its 1998 report to Congress, the FTC concluded that self-regulation was not working to protect the privacy of children online. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS, *at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (June 1998). In a review of 212 American commercial web sites aimed primarily at children aged 15 and under, the FTC found that 186 of them (88%) collected personal identifying information and 188 (89%) collected personal information. Only 109 of the 188 contained a notice of even one of the commonly accepted fair information principles, and no site practiced the full range of those principles. *Id.* at 20, 31, 36.

256. The law requires "verifiable parental consent" before information is collected from children 12 and younger that would allow them to be contacted online or off-line. "Verifiable parental consent" is defined as:

> [A]ny reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

15 U.S.C. § 6501(9).

257. *Id.* § 6502(a).

258. *Id.* §§ 6502(b)(2)(A)–(E).

259. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–09 (2000)).

share "nonpublic personal information."[260] Although affiliates have to tell customers that they are sharing this information, individuals cannot block the sharing of this "nonpublic" information collected by the affiliated institutions. Because the financial services industry is dominated by large conglomerates of affiliated entities, sharing of information is routine.[261]

Under Gramm-Leach-Bliley, customers can opt-out of the disclosure of certain "non-experience" data among affiliates and certain data that the conglomerate wishes to share with non-affiliated third parties.[262] To do so, however, individuals must read through the often lengthy privacy policies mailed by the financial institution and learn now to exercise their opt-out rights.[263] Bank customers who have tried to navigate through the numerous "opt out" forms mailed in recent months know that this is not as simple as it sounds.[264] Financial institutions have no incentive to make opting out easier.

---

260. 15 U.S.C. § 6802(a) (prohibiting disclosure to nonaffiliated third parties). *See also* 12 C.F.R. § 216.4(a) (2000), 12 C.F.R. § 216.7(a) (2001).

261. *See generally* Gregory T. Nojeim, *Financial Privacy*, 17 N.Y.L. SCH. J. HUM. RTS. 81 (2000) (explaining inadequacies of Gramm-Leach-Bliley Act).

262. 15 U.S.C. § 6802(b) (creating obligation to give consumers the opportunity to opt out, and providing exceptions to the general opt out rule).

263. Acting Comptroller of the Currency Julie Williams commented, "Most bank customers can't ever recall seeing something like this . . . . [I]t has been known to happen that the affiliate-sharing 'opt out' disclosure is buried in the middle or near the end of a multi-page account agreement. For existing accounts, some institutions have gotten into the habit of reducing the required 'opt out' disclosures to the fine print along with a long list of other required disclosures. Few consumers are likely to have the fortitude to wade through this mass of legal verbiage, and fewer still will take the time to write the required 'opt out' letter. I have even heard of people getting two separate notifications covering different types of information, requiring two separate letters to opt out." Office of the Comptroller of the Currency, U.S. Treasury Dep't, Remarks by Julie L. Williams, Acting Comptroller of the Currency, Before the Banking Roundtable Lawyers Council, *at* http://www.occ.treas.gov/ftp/release/98%2D50a.txt (May 8, 1998); *see* Sovern, *supra* note 2, at 1087, 1088; David J. Klein, *Keeping Business out of the Bedroom: Protecting Personal Privacy Interests from the Retail World*, 15 J. MARSHALL J. COMPUTER & INFO. L. 391, 398 (1997) ("List creators generally place [opt-out provisions] in the fine print with other boilerplate terms of the contracts; thus the clause is not readily apparent to most consumers.").

264. In the financial services industry, opting out usually requires the account holder to read through the privacy policy of the financial institution and call a toll-free number. In the privacy policy of Bank One and First USA, the opt-out information appears on the third and fourth pages. The policy warns the customer, "Choosing to opt out of this information sharing may limit opportunities for you to receive product and service information that may interest you." It also states that if only one customer on a joint account opts out, the bank can continue to share information about the other joint account holders. *See* "Important Privacy Notice," M51388 STI40485, Letter from Carter Warren, Chief Marketing Officer, Bank One, to James P. Nehf (on file with author).

Note the holes in this patchwork of sector-specific privacy laws. For adults, there is virtually no regulation of the collection and disclosure of information on the Internet. Many Internet sites have voluntarily published privacy policies, but even those policies can offer little privacy protection, and if a privacy policy is breached the individual has little recourse under current law. It is difficult to show economic injury from the breach, and while violation may be an unfair or deceptive practice under the Federal Trade Comission Act (FTCA),[265] in most circumstances the FTCA will only obtain injunctive remedies. In addition, no federal law and few state laws make it illegal for an employer to gather and compile personal information about employees, even if the information is unrelated to the job they do. Employers can monitor our family lives, check on organizations in which we belong, ask about our medical histories, listen to our phone calls, read e-mail, listen to voicemail, monitor our computer screens, install software that tracks and counts our keystrokes, require urine tests for drugs, and check our credit reports.[266] Other classes of unprotected records include those maintained by online and offline merchants, records held by bookstores, department stores, restaurants and clubs, and personal information profiles assembled by database companies.[267]

D. The Failure of Self-Policing and Market-Based Solutions

One of the problems with privacy laws and regulations is that they are usually written by policy makers who lack thorough knowledge about the operation of computers and information systems. Even when lawmakers have the requisite technical background, they must try to anticipate largely unknown technological developments. Resulting laws and regulations have therefore contained broad guidelines with sufficient

265. 15 U.S.C. § 45(a) (2000). For a general discussion of the FTC Act, see Peter C. Ward, *Restitution for Consumers Under the Federal Trade Commission Act: Good Intentions or Congressional Intentions?*, 41 AM. U. L. REV. 1139, 1156 (1992).

266. *See* Benjamin F. Sidbury, *You've Got Mail . . . and Your Boss Knows It: Rethinking the Scope of the Employer E-mail Monitoring Exceptions to the Electronic Communications Privacy Act*, 2001 U.C.L.A. J. L. & TECH. 5; Amanda Richman, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337, 1346–47 (2000) ("[R]estrictions on preemptive screening create incentives for employers to monitor employees post-hire in order to minimize the employer's potential liability and protect others from personal harm. . . . More than 67% of employers monitor employees, a 3.9% increase since 1997, and e-mail monitoring nearly doubled between 1997 and 1999."); S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 826 (1998).

267. *See* Solove, *supra* note 32, at 1148.

latitude to embrace later developments, but few details or specific directions to the information processing industry concerning permissible or prohibited activity.[268] Almost by default, the laws have placed an enormous amount of trust in individuals and the marketplace to ensure that privacy interests are protected.

This choice of policing mechanism was not irrational. Representatives of free information flow have long said that the market will achieve a socially acceptable proportion of information privacy and disclosure.[269] In theory, both individuals and businesses will balance the value of personal information, such as its commercial value in the marketplace, against the value of keeping the information within the individual's control.[270] There are market incentives for companies to keep their collected data secret and to be honest about their data collection policies. Conversely, there are incentives for individuals to limit the release of their personal information to others and to monitor the use of information that has already been released. In some instances, market mechanisms have worked. In 1996, for example, the online news and legal search engine, Lexis-Nexis, announced a new service called the P-TRAK Personal Locator, which would have given subscribers access to the addresses, maiden names, and Social Security numbers of millions of individuals. After considerable adverse publicity, the company changed its plans.[271]

A related argument in support of marketplace solutions is that the technology industry itself will provide an acceptable degree of privacy protection. For example, more widespread use of cryptography has been suggested as a technique to protect some types of privacy invasion, particularly in the telecommunications and Internet data transfer

---

268. *See* Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99, 104 (Philip E. Agre & Marc Rotenberg eds., 1998).

269. One of the strongest and most powerful proponents of market-based resolutions and self-regulation is the Direct Marketing Association. *See* SCHWARTZ & REIDENBERG, *supra* note 122. The Online Privacy Alliance, a group of large, global corporations and trade associations also promotes industry self-regulation and issues privacy guidelines. *See* Online Privacy Alliance: Privacy Policy Guidelines, *available at* http://www.privacyalliance.org/resources/ppguidelines.html (Nov. 15, 1999).

270. *See* Solove, *supra* note 31, at 1446–47.

271. Along similar lines, Lotus Development Corporation and Equifax Credit Corporation had planned to market a CD-ROM in 1990 containing information on 120 million consumers. The parties cancelled the plans after concerned individuals posted complaints on the Internet. Kim Bartel Sheehan & Mariea Grubbs Hoy, *Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns*, 28 J. ADVERTISING 37 (Fall 1999). *See* Solove, *supra* note 31, at 1447.

industries.[272] Savvy consumers can install and employ a wide range of products that allow for anonymous web surfing and defense against surreptitious data mining.[273] Computer software can be crafted to act like an "electronic lawyer," negotiating our privacy concerns with Internet sites.[274] Products such as Anonymizer[275] allow users to retain anonymity while surfing the Internet.[276] P3P technology, which provides a standard language for web sites to encode privacy policies, allows web browsers to display privacy warnings to users and block cookies.[277] To date, such systems have yet to be widely used. If they are to become the standard control mechanism against privacy invasion on line, a massive educational effort would be needed[278] and a universal system would need to be developed that would be compatible with most Internet sites, relatively easy for consumers to use, and difficult for data seekers to evade.[279]

---

272. *See* BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS 4 (1997) (arguing that the FBI and other law enforcement organizations are impeding the development of new technologies that would enhance privacy but might impede crime investigations and communication monitoring).

273. Kennedy & Meade, *supra* note 74, at 344.

274. Lawrence Lessig more quaintly calls this service an "electronic butler." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999). An individual sets his or her privacy preferences once—specifying how to negotiate privacy and what information the user is willing to give up—and from that moment on, when the user enters a site, the site and the user's machine negotiate. Only if the machines can agree will the site be able to obtain the user's personal data. Microsoft, AOL, and IBM worked to develop the "Platform for Privacy Preferences" software (P3P) along these lines several years ago. *See* Jeri Clausing, *New Technology Is Aimed at Web Privacy*, NYTIMES.COM, June 22, 2000, *available at* http://www.nytimes.com/library/tech/00/06/cyber/articles/22privacy.html.

275. For a more detailed product description, see http://www.anonymizer.com/ (last visited Jan. 20, 2003).

276. *See* Eric Shih, *Putting Internet Privacy Laws Aside, What Technology Might Guard Your Privacy?*, 5 ELEC. BANKING L. & COM. REP. 12 (March 2001).

277. *See* World Wide Web Consortium, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C Recommendation, http://www.w3.org/TR/P3P/ (Apr. 16, 2002).

278. *See Exposure in Cyberspace*, WALL ST. J., Mar. 21, 2001, at B1 (survey showing that almost 30% of computer users did not know about "cookies" and almost 40% had no idea how to de-activate them).

279. The P3P program, for instance, was criticized by privacy advocates for failing to comply with basic standards for privacy protection, and for employing a protocol that was too complex and confusing. *See* Electronic Privacy Information Center & Junkbusters, Pretty Poor Privacy: An Assessment of P3P and Internet Privacy, *at* http://www.epic.org/reports/prettypoorprivacy.html (June 2000). *See also* Bennett, *supra* note 268, at 117; Reidenberg, *supra* note 134, at 729 (stating for technology to provide effective privacy protection, three conditions must be met: technology respecting fair information practices must exist, the technology must be deployed universally, and the technology must have a "privacy protecting default configuration" to ensure its widespread use).

While technology might hold the key to privacy protection in the future, it would require government intervention to require privacy technology as a standard installation or default preference in most computers.[280] A year 2000 survey showed that less than half of Internet users—forty-three percent—even knew what a cookie was; only ten percent said that they had set their browser to block cookies.[281] For now, economic incentives more often produce technologies that enhance data collection and sharing rather than restrict it. For example, a version of the Microsoft Internet Explorer came equipped with default settings that enabled hidden surveillance of users, and a version of Netscape Communicator reported back to Netscape every time a user read e-mail.[282] Because personal information has become so valuable, technologies have developed that increase data collection and decrease our ability to monitor the data collection process. This makes privacy protection even more difficult for computer users who might be interested in curbing surreptitious information collection practices.[283]

1. Reasons Why Market Solutions Fail to Protect Privacy Interests

The non-regulatory solutions to the privacy problem were promoted with good intentions, but the conditions of market failure are simply too

---

280. Time Magazine ran a feature story on information privacy in July 2001 that recommended to readers ten steps to protect privacy. *See* David Jackson, et al., *Internet Security*, TIME MAGAZINE, July 2, 2001, at 50. Except for the advice not to "download anything unless you trust the sender" and "be careful what you give out," the recommendations were not likely to be known or deployed by many computer users for years to come unless required by law as a default preference in home and business computers. *Id.* The list includes: installing a home firewall, changing browser preferences to delete a user's e-mail address and replace it with a "false name and dummy e-mail account," opting out of information sharing policies when given the choice (although the writer acknowledges that this "can be a chore"), resetting your browser to reject cookies or install software like "Cookie Crusher," checking to make sure a website uses encrypted transfer software before giving sensitive information online, hiding your identity with an "anonymizer" program, and clearing your memory cache each time you surf the Internet. Even with all of this advice, Time gives its readers the "Bottom line: If it has to stay secret, don't put it on a computer hooked up to the Internet." *Id.*

281. Fox, *supra* note 2.

282. *See Oversight Hearing on Privacy and Electronic Commerce*, Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, United States House of Representatives (testimony of Joel R. Reidenberg), *available at* http://www.house.gov/judiciary/reid0518.htm (May 18, 2000).

283. Reidenberg, *supra* note 134, at 723. *See* John Hanchette, *New Microsoft Software Raises Privacy Protection Concerns*, INDIANAPOLIS STAR, Aug. 26, 2001, at D1 (describing Microsoft plans to combine personal identification information with a powerful information distribution network).

strong.[284] Although market-based solutions can be effective in some areas of consumer law, they are not likely to limit the use and misuse of personal information. There are several reasons why.

First, the operations of the data collection and sharing industry are not transparent. The vast majority of data collection and sharing practices occur outside public view. How do we know what information about us is being collected and when our data is being used in a way we did not expect or authorize? If the collection and sharing of information is not transparent, and it is becoming less so as data mining technologies become more sophisticated, then unfair information practices—practices most of us would object to—will likely go unnoticed. If we are not aware of malfeasance, we cannot seek redress or stop it from recurring. Moreover, requiring a public protest each time a privacy invasion occurs is not an effective privacy policy. People should not have to start a public relations campaign whenever a dangerous privacy plan is exposed.

Second, individuals cannot effectively value their personal information. To be effective, market-based solutions presume that we can value our privacy rights in some meaningful way. Only then can we make intelligent choices about whether and how to share information. Since it is impossible to know where our information will end up and how it will be used, it is difficult to assess the risks associated with giving out the information or failing to monitor its use once we have released it. We might read a privacy policy on a web site, for example, and conclude that even though the site reserves the right to share our data, we consent to the policy because we are only providing "innocent" facts and details. We may perceive the risk as small compared to the benefits provided by the web site, not knowing how or when the seemingly innocent information might be shared or aggregated with other information in a combination that will cause harm. According to one commentator, it is possible to identify eighty-seven percent of the American population knowing only a person's birth date, gender, and postal ZIP code.[285]

---

284. *See generally* Reidenberg, *supra* note 134, at 726.

285. Erik Sherman, *It Doesn't Take Much to Make You Stand Out*, NEWSWEEK, Oct.16, 2000, at 74N. (quoting Latanya Sweeney, an assistant professor of computer science and public policy at Carnegie Mellon University). According to the FTC, 99% of the "Most Popular" websites collect personal information, including e-mail address and other personal identification, from and about consumers. The FTC concluded that most of the sites "are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior or surfing behavior information they collect to personal identifying information." *See* UNITED STATES, FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE

To create an appearance that individuals are knowingly revealing personal information, data collection businesses often post privacy policies voluntarily.[286] These policies are hardly "arms length agreements" between users and the data collectors, so the user's consent is illusory in most instances.[287] Moreover, privacy policies tend to make vague promises that commit to very little.[288] The privacy "commitment" of the GAP credit card, for example, promises virtually no privacy protection. The policy simply informs the card holder that GAP will "collect personally identifiable information about you . . . from a number of sources," and "may use and share all of the information" for any reason not prohibited by law.[289] In addition, businesses can and do change their privacy policies frequently. Unless a person rereads the policy at each interaction with the business, it will never know the current practice.[290] And if a business violates its own policy, how does one discover this fact and the extent of any injury?[291] These problems exacerbate the difficulty of valuing information privacy.

---

at 9–10 [hereinafter FTC REPORT], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (May 2000).

286. *See Transcript: Colloquium on Privacy and Security,* 50 BUFFALO L. REV. 703, 723 (2002) (comments of Ann Bartow regarding voluntary privacy policies).

287. Most Web privacy policies are little more than confusing boilerplate for the typical Internet user. Reidenberg, *supra* note 134, at 727–28. *See also* MacDonnell, *supra* note 83 (TRUSTe, BBBOnline, WebTrust and other seal programs do not require compliance with OECD privacy guidelines, which are discussed *supra* note 142).

288. *See* Will Rodger, *Privacy Isn't Public Knowledge: Online Privacy Policies Spread Confusion With Legal Jargon*, USA TODAY, May 1, 2000, at 3D.

289. *See* GAP Credit Card, *supra* note 74. *Cf.* NAT'L TELLECOM. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, ELEMENTS OF EFFECTIVE SELF-REGULATION FOR PROTECTION OF PRIVACY (Jan. 1998) (stating that for self-regulation to be meaningful, laws must impose substantive rules on businesses concerning notices and consumer choice, rather than setting forth broad guidelines and allowing businesses to implement them as they choose), *available at* http://www.ntia.doc.gov/reports/privacydraft/198DFTPRIN.htm (Jan. 1998).

290. The privacy policy of the GAP Credit Card, *supra* note 74, states, "We may amend this Privacy Policy at any time, and we will inform you of changes as required by law." In December 2000, the online travel service Expedia changed its privacy policy to include the following: "Expedia.com reserves the right to modify or amend this Privacy Statement at any time and for any reason. If there are material changes to this statement or in how Expedia.com will use your [personal information], Expedia.com will prominently post such changes prior to implementing the change." Expedia.com's Privacy Pledge, *available at* http://www.expedia.com/daily/service/privacy.asp?rfrr=-480&CCheck=1 (last visited Jan. 27, 2003). Despite the assurance that changed privacy rules will only apply to data acquired after the change, practical difficulties may make it impossible for Expedia to fulfill this promise, and for users to monitor Expedia's compliance. *See* Kennedy & Meade, *supra* note 71, at 321, 337.

291. A poll of 580 Canadian Internet users found that 40% of the respondents did not believe that online companies would honor their posted privacy policies. D. Akin, *Canadians Still Not Sold On Net Privacy Policies*, THE NATIONAL POST, Jan. 17, 2001, at C6.

Another aspect of the valuation problem is the difficulty in pricing specific pieces of personal information out of context. How do I value my monthly grocery store shopping list? One might say that its value is the amount of store discounts I receive each month because I voluntarily trade that information for these cost savings when I use my store "convenience" card. Yet to value this information with even remote accuracy, I need to know how the information will be used. The store might sell it to a marketing firm in the aggregate (along with data from all customers) without any name identification, in which case I might value its release nominally. If the store sells it to insurance companies and financial institutions with name identification, I would likely value it much higher. Most personal information may never come back to haunt us, but a few items of information could be used to wreak havoc if identity fraud occurs.[292] Once the information is stored and capable of being accessed, we lose control over our fate. We often do not have enough information to evaluate this risk.

Voluntary "trustmarks" or "web seals" are not a suitable substitute for legal mandates. Seal programs[293] can help web users gain confidence in the privacy practices of the sites they visit, but the most popular programs do not require that damage remedies be readily available to the victims of information misuse, and the scope of the web seal "guarantee" of privacy can be narrower than individuals might expect. For example, TRUSTe certifies sites that promise not to share information "used to identify, contact, or locate a person."[294] Yet reports show that most Internet users do not want Web sites tracking their movements even if

---

292. *See* Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1424 (2001); Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL L.J. & PUB. POL'Y 661, 662–67 (1999). *See also supra* note 4.

293. A trustmark or seal program requires a website licencee to abide by a code of information practices and to submit to various types of compliance monitoring in order to display a program's privacy seal. *See Pippin, supra* note 211, at 132; Web Seals: A Review of Online Privacy Programs, *available at* http://www.privacy.gov.au/publications/seals.html#2 (Sept. 2002); *Privacy Standards for Web Sites: Web Seals*, *available at* http://www.tilj.com/content/ecomarticle02050103.htm (Feb. 5, 2001).

294. *See* TRUSTe Program Principles, *available at* http://www.truste.org/programs/pub_principles.html (last visited Jan. 20, 2003). TRUSTe is an independent, non-profit organization founded in 1997 by the CommerceNet Consortium and the Electronic Frontier Foundation. TRUSTe developed a license agreement that governs a licensee's collection and use of information and requires licensees to adhere to standards for notice, choice, access, and security. The program includes third party monitoring and periodic review of licensee information practices. *See* Pippin, *supra* note 211, at 132.

the site does not associate the data with a particular user's identity.[295] In addition, the most popular seal programs do not perform regular and rigorous audits on their client's web sites to ensure that the web seal standards are being satisfied.[296]

Third, there are accountability problems with data collection and sharing practices. Tracing an injury to a particular cause, source, or leak will often be impossible. In the context of identity theft, a typical complaint is, "How did the thief get this information about me?"[297] With information about us residing in so many databases, if a problem does surface, there may be no way to locate the original source of the leak. Without accountability, market forces cannot effectively curb harmful behavior.

Fourth, if we want to participate in modern society, we have little choice but to reveal information about ourselves. If we want the job, the loan, or the medical care, we have to disclose information about ourselves and our lives.[298] Market solutions presuppose choice, and where the choice to reveal information is limited, the market will fail to protect our interests.

Perhaps most fundamentally, however, one may ask why the burden should be on the individual to figure out how to keep others from getting, selling, and using information. Self-regulation assumes that information about us is a property right or commodity that can be bought and sold. Viewing privacy in this way produces an ineffective system of sporadic notice and illusory choice. This approach ignores other universally recognized principles of fair information practice such as minimizing the amount and type of data that can be stored, and restricting access to the

---

295. Reidenberg, *supra* note 134, at 727–28. *See also* MacDonnell, *supra* note 83, at 348–49 (explaining that TRUSTe, BBBOnline, WebTrust and other seal programs do not require compliance with OECD and Canadian privacy guidelines).

296. *See* MacDonnell, *supra* note 83, at 392. Auditing compliance with web seal mandates is a burdensome task and can be costly if the audit is rigorous. One solution to this problem was advanced by Colin Bennett in a slightly different context. Bennett's scheme would involve three tiers of compliance with privacy standards: 1) a conformity of "policy"; 2) a conformity of "procedure"; and 3) a conformity of "practice." Only an organization seeking certification in the third tier would undergo a complete privacy audit to ensure that it honor its representations in practice. *See* Colin Bennett, *Prospects for an International Standard for the Protection of Personal Information, available at* http://www.e-com.ic.gc.ca/english/privacy/632d29.html (August 1997).

297. Studies have shown that nearly 80% of identity theft victims do not know how or where the thief obtained their personal information. Lucas, *supra* note 4.

298. The FCRA, for example, mandates that individuals consent before an employer can obtain their credit report. 15 U.S.C. § 1681(b)(2) (2000). This consent is virtually meaningless if the person wants the job.

data that can legally be stored, organized, and sorted.[299] Only by deemphasizing the commodity aspects of information privacy, and focusing on the societal value of keeping information private, can we create a different and more effective regulatory model. More "notice and consent" requirements are not likely to provide greater privacy protection.[300]

Evidence showing the failure of market-based regulation has been gathered by the FTC. After years of promoting market based privacy measures and waiting for acceptable industry-regulated fair information practices, the FTC in its May 2000 report concluded that broad-based legislation is necessary to ensure fair information practices online.[301] The agency noted private sector initiatives to develop self-regulatory regimes, but concluded that industry measures were far from adequate.[302] The FTC report recommended that technology neutral legislation be enacted, and called for an implementing agency with regulatory and supervisory authority.[303] New leadership at the FTC, however, has recently backed off of this recommendation, calling for increased enforcement of existing laws instead.[304] The retreat is unfortunate because, for a short period at least, it looked as if we might be moving toward a privacy policy that is more compatible with the idea of privacy as a societal value. Without prompting from the FTC or another influential voice in the privacy debate, the status quo is likely to remain for some time.

---

299. Self-regulation also enables data collectors to change the rules after the data has been collected from individuals. Reidenberg, *supra* note 134, at 727.

300. A number of bills have been introduced that would impose various types of notice and consent requirements, including S. 1055, 107th Cong. (2001); H.R. 89, 107th Cong. (2000); H.R. 237, 107th Cong. (2000); and H.R. 2135, 107th Cong. (2001).

301. FTC REPORT, *supra* note 285.

302. In a random sample of 335 American commercial web sites that collected personal identifying information, only 20% applied fair information practices. The figure was higher, 42%, for 91 of the 100 busiest commercial sites. FTC REPORT, *supra* note 285, at 20.

303. *Id.* at iii, 36.

304. *See* FTC Chairman Timothy J. Muris, *Protecting Consumer's Privacy: 2002 and Beyond*, Address Before The Privacy 2001 Conference, *at* http://www.ftc.gov/speeches/muris/privisp1002.htm (Oct. 4, 2001); Timothy J. Muris, *Challenges Facing the Federal Trade Commission*, Address Before the Committee on Energy and Commerce, *at* http://energycommerce.house.gov/107/hearings/11072001Hearing403/Muris678print.htm (Nov. 7, 2001).

III. PRIVACY AS A SOCIETAL VALUE

A. Defining Information Privacy as a Societal Value

It has been four years since Sun Microsystems CEO Scott McNealy issued his now famous warning, "You have zero privacy anyway. Get over it."[305] So much information about us is already in government and private sector databases that it may be too late to rethink our approach to information privacy protection.[306] Yet, if we begin to think about information privacy as an important societal value rather than a typical consumer law problem calling for a balance between business and consumer interests, we may be able to achieve several important goals. However, we must initially agree on a set of privacy objectives. I suggest three baseline goals for a national privacy policy.

1. Fundamentals of Effective Privacy Policy

First, while we have begun to recognize that certain uses of even non-confidential information can threaten privacy, it is not sufficient to impose limits on the use of information once it has been collected. Procedural safeguards alone cannot protect the confidentiality of information adequately. Thought must be given to the types of information that can be collected in the first instance—by public authorities and private sector enterprises—because once information is in a database, controlling its subsequent use is extremely difficult. For instance, why should we allow employers to collect virtually any information on applicants and current workers and store the information in a database? We should reevaluate our presumption that virtually any piece of personal information can be stored electronically.

Second, we should acknowledge that the current self-regulatory approach, which requires individuals to police the market to ensure that their data is not collected or disseminated, is ineffectual. A more complete range of enforcement schemes should be developed to control how information will be collected, used, and shared. To the extent market mechanisms are used, regulation mandating that consumers opt-in rather than opt-out, for example, can in some circumstances achieve a

---

305. *See generally Sun on Privacy: Get over It*, WIRED NEWS, *at* http://www.wired.com/news/politics/0,1283,17538,00.html (Jan. 26, 1999).

306. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 131 (1999) (observing that the genie is already out of the bottle).

more balanced approach to the disclosure of information.[307] Opt-in systems place the incentive on entities that want to acquire personal information, in both the government and private sector, to make it as easy as possible for individuals to give meaningful consent to the collection and use of their information.[308]

Third, a national Privacy Board, or an institutional network of privacy agencies, is necessary to ensure that government and private sector data collectors maintain fair information practices. Stiff penalties should be imposed upon those who breach privacy agreements with their customers (not just a finding under the FTCA that an unfair trade practice has been committed). Watchdog organizations and individual lawsuits cannot be relied upon to assume this responsibility. Organizations like the Electronic Privacy Information Center (EPIC) bring legal actions to accomplish privacy protection goals, but they work piecemeal, vary in their targets depending on the priorities of the organization bringing the suit, and succeed only when state or federal laws have been broken. Individual lawsuits are even rarer. More importantly, however, litigation should not be the primary enforcement mechanism for citizens who can rarely afford to sue the government or a large commercial enterprise.[309]

These three changes would mark a fundamental shift from a presumption favoring the collection and sharing of personal information

---

307. A survey conducted in 2000 showed that 86% of respondents favored privacy policies requiring organizations to seek explicit permission before gathering any personal information. *See* Fox, *supra* note 5. Several states require affirmative consent from individuals before their personal information can be shared with others. *See* William M. Fay, Jr., *Lost in Oz: There Is No Yellow Brick Road for State Lawmakers to Follow in Drafting Privacy Legislation for Insurers*, 7 CONN. INS. L.J. 585, 604–18 (2000).

308. To the extent websites give users a choice, most use an "opt-out" system, i.e., unless a user affirmatively indicates that he or she does not want information sold or shared to another party, the site is free to circulate the information. An August 2000 survey indicated, however, that 86% of users favored "opt-in" policies that require affirmative consent from the user before information can be shared. *See* Dylan Tweney, *The Rules for Writing a Privacy Policy*, ECOMPANY NOW, *available at* http://www.ecompany.com/articles/web/0,1653,8297,00.html (Sept. 7, 2000).

The Federal Communications Commission recently adopted an opt-in rule to protect sensitive personal information of customers of telecommunications carriers. The Order provides for express-consent customer approval for carriers' release of customer information to third parties, but permits opt-out consent for release of information to affiliated parties. *See Federal Communications Comission Adopts Rules Resolving How Phone Companies Share and Market Customer Information*, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-224366A1.pdf (last visited Jan. 20, 2003).

309. *See* David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 167, 174 (Philip E. Agre & Marc Rotenberg eds., 1998).

and toward a neutral position or a presumption against it. How can we get there from here? We should begin by convincing policy makers to look at information privacy in a different way. How an issue is defined on the public agenda is important to the politics of the law-making process and ultimately the policy resolution.[310] When information privacy is defined as a matter of individual concern, it is difficult to see a broader purpose in controlling the problem. There is no polluted atmosphere or outbreak of disease that identifies the issue as one of general public concern demanding a societal, rather than individual, resolution.

2. *Moving Toward a Societal View of Privacy*

Priscilla Regan and others have argued that privacy serves not just individual interests, but also common, public, and collective purposes. Privacy is a common value because we all recognize its importance in our lives, a public value because it is necessary to the proper functioning of a democratic political system, and a collective value because technology and market forces make it increasingly difficult for any of us to have privacy unless we all have privacy at a similar level.[311] If privacy is regarded as being of societal importance, different policy discourse and interest alignments are likely to follow, and this opens the way to serious consideration of different policy resolutions.

Theoretical underpinnings for a societal view of information privacy began in the 1960s and early 1970s. Privacy literature was abundant during this period, and several writers acknowledged that privacy was important to society at large, not just to individuals.[312] Yet there was little development of the idea that privacy policy should be created with this perspective in mind. Alan Westin, quoting from Robert Merton's *Social Theory and Social Structure,* wrote: "Privacy is not merely a personal predilection; it is an important functional requirement for the effective operation of social structure."[313] Abstract declarations of this sort failed

---

310. *See* REGAN, *supra* note 7, at xiii, 220–31.

311. *Id.* at xv–xvi. *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1653 (1999) (stating that database privacy is necessary for democratic deliberation).

312. *See, e.g.*, WESTIN, *supra* note 85, at 58; James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFFAIRS 323 (1975) (observing a "close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships").

313. WESTIN, *supra* note 85, at 58 (quoting ROBERT MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 375 (1957)). *See* REGAN, *supra* note 7, at 32.

to influence the formulation of public policy. Even in the philosophical literature during this period, the "effective operation of social structure" quickly evolved into advocacy for privacy as a component of individual freedom and liberty.[314] The result was an approach to privacy policy that focused on the individual and the legal protection of his or her rights versus the rights of others to use personal information for their own purposes.[315] More recent writing has similarly emphasized privacy's importance to the individual, and the policy debate has sought to balance the individual right to privacy against broader societal interests in information collection and sharing.[316]

An effort to redefine the societal value of privacy was begun, however, by Regan and privacy proponents such as Colin Bennett. Bennett writes about the humanistic and political aspects of privacy.[317] The humanistic value recognizes the loss of dignity, autonomy, or respect for the individual that results when we lose control over personal information.[318] For some privacy advocates, the humanistic dimension is the only justification needed for protective public policy.[319] The very collection of personal information, regardless of how it is used, contributes to the sense of alienation in post-industrial society. Information technology adds a new layer to the already impersonal

314. *See* REGAN, *supra* note 7, at 32–33.

315. Political theorists identify two types of "rights"—civil liberties and civil rights. Privacy has often been characterized as a civil liberty, the right to be free from interference from other individuals, governments or organizations. *See* ISAIAH BERLIN, *Two Concepts of Liberty*, *in* FOUR ESSAYS ON LIBERTY 118 (1969) (privacy as a negative liberty); VINCENT J. SAMAR, THE RIGHT TO PRIVACY: GAYS, LESBIANS, AND THE CONSTITUTION 53 (1991) (privacy as a "negative freedom"). As such, it loses some of the legitimacy that civil rights have in American politics. Defining a problem as a civil right can be a successful political strategy (e.g., women's rights, minority rights, rights of the disabled). Civil rights movements in the United States have usually assigned some benefit or status to a group rather than to an atomistic individual. As privacy began to be viewed as a policy matter of individual liberty, its claim to status as a civil right diminished. *See* REGAN, *supra* note 7, at 4.

316. *See, e.g.*, JULIE INNESS, PRIVACY, INTIMACY, AND ISOLATION 140 (1992) (privacy important because it gives individuals more control over the making of intimate decisions); Post, *supra* note 93, at 2091 (privacy as "important to individuals to resist misjudgments based upon private information," and loss of privacy as "particularly hurtful to individuals").

317. BENNETT, *supra* note 49, at 29–33.

318. *See* Lawrence E. Rothstein, *Privacy or Dignity? Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 383 (2000) (describing privacy as "dignity" in a European sense, looking at European approaches to workplace monitoring).

319. *See, e.g.*, JAMES RULE, ET AL., THE POLITICS OF PRIVACY 22 (1980) (recognizing "the restriction of personal information as an end in itself"); DUNCAN CAMPBELL & STEVE CONNER, ON THE RECORD: SURVEILLANCE, COMPUTERS AND PRIVACY 12 (1986) (privacy as "fundamental to human integrity").

character of government bureaucracy and commercial relations with individuals.[320] It contributes to an uneasy sense that "someone out there knows something about me,"[321] a sentiment which alone should get the attention of policy makers.

A political aspect of privacy policy is at work as well. Privacy is rooted in the classical liberal belief in limited government and a general distrust of powerful institutions, whether they are public or privately owned. Information technology enhances the power of the government and commercial enterprises to obtain and manipulate information about us. As power shifts further away from the individual to large institutions that can affect the individual's life and liberty, we have a collective cause for concern and a need for a political resolution.[322]

This revival of a societal view of privacy coincided with the emergence of the "politics of ideas" movement, which became an important model for explaining policy making in the 1990s. The model received considerable attention and some popular appeal during the Clinton administration, though its application in practice has been uneven at best. On the theoretical side, the model has both normative and descriptive aspects. The notion that public policy should promote the general public good, rather than accommodate competing claims of influential stakeholders, has long been part of our political culture, if not our political reality.[323] More recent scholarship, however, has emphasized the descriptive aspect. Ideas about what is good for society, rather than what emerges from a battle of individual self interests, can explain more policy making activity than interest group models would predict.[324] Ideas associated with the public interest, commonly shared

---

320. *See* Martin Heidegger, *The Question Concerning Technology*, *in* THE QUESTION CONCERNING TECHNOLOGY AND OTHER ESSAYS 25–28, 37–41, 48–49 (William Lovitt trans., 1977) (warning that technology threatens the "Enframing" of "Being"); Krotoszynski, Jr., *supra* note 56, at 234.

321. BENNETT, *supra* note 49, at 28. On the humanistic and ethical dimensions of data collection and computer technology generally, see JOSEPH WEIZENBAUM, COMPUTER POWER AND HUMAN REASON (1976) and HUBERT DREYFUS, WHAT COMPUTERS CAN'T DO: A CRITIQUE OF ARTIFICIAL REASON (1972).

322. BENNETT, *supra* note 49, at 30 (quoting DAVID BURNHAM, THE RISE OF THE COMPUTER STATE (1983)) ("The 'rise of the computer state' is regarded as a threat to the liberal values that have such a central place in the American Heritage."). Viewed in this way, information privacy is "rooted in Lockean liberalism: inalienable human rights, limited government, the rule of law, and a separation between the realms of state and civil society." *Id.* at 31.

323. *See generally* THE POWER OF PUBLIC IDEAS (Robert B. Reich ed., 1990).

324. On interest group politics in general, see THEODORE J. LOWI, THE END OF LIBERALISM: IDEOLOGY, POLICY, AND THE CRISIS OF PUBLIC AUTHORITY (1969); GRANT MCCONNELL, PRIVATE

principles of morality, justice, and the collective welfare occasionally do overcome narrower interests as lawmakers evaluate policy alternatives. Some of the work in this area has focused on deregulation, particularly in the trucking, airline, and telecommunications industries, where deregulation occurred despite initial opposition by powerful interest groups such as the targeted industry, labor unions, and regulatory oversight agencies.[325]

In the instances where fundamental policy change results despite the influence of well-organized special interests, three conditions seem to be present. First, an outside force or public event brings the problem to the front of the political agenda. Second, popular symbols or slogans emerge to give the idea political strength. Third, a forceful yet latent public interest pushes the idea through to ultimate enactment.[326] Interestingly, all three seemed to be present in the information privacy debate of the 1960s and early 1970s. Rapid changes in information technology and the proliferation of large computer databases brought renewed interest to the problem and continued throughout the period of debates. The idea of privacy protection evoked powerful symbols in American culture. Big Brother, *1984*, and *A Clockwork Orange* created fearful images that helped get the issue on the public agenda. Finally, as numerous public interest surveys revealed, there was and continues to be a strong public interest in protecting information and controlling the technologies that could compromise it.[327]

Despite this strong public interest in protecting privacy, strong, countervailing forces ensured that privacy as a political ideal and as an accepted social value would not have a powerful influence on policy making. By framing the debate in terms of individual rights—the right of an individual to control access to information about himself or herself—policy makers elicited two responses that narrowed the range of possible resolutions. First, privacy was viewed as a matter of "individual utility."[328] Each of us considers how valuable our own information is to

---

POWER AND AMERICAN DEMOCRACY (1966) and DAVID B. TRUMAN, THE GOVERNMENTAL PROCESS: POLITICAL INTEREST AND PUBLIC OPINION (1958).

325. *See generally* MARTHA DERTHICK & PAUL J. QUIRK, THE POLITICS OF DEREGULATION (1985) (arguing that the idea of deregulation was powerful enough to prevail over stakeholders in business and government); TIMOTHY J. CONLAN, ET AL., TAXING CHOICES: THE POLITICS OF TAX REFORM (1990); Priscilla M. Regan, *Ideas or Interests: Privacy in Electronic Communications*, 21 POL'Y STUD. J. 450 (1993).

326. *See* REAGAN, *supra* note 7, at 18.

327. *See id.* at 176–77.

328. *See id.* at 178.

us, and how we might be hurt if the information is shared. If individuals have not personally been affected in a negative way, then the problem is not as important and the person may disengage from the debate. Second, because rights are not absolute, privacy had to compete with other rights and social interests, such as the right of commercial speech and societal interests in efficient government or business activity. As a result, the influence of interest group politics could not be overcome.[329]

Another circumstance that affected privacy policy resolutions during this period was the existence of information technology at the periphery of public awareness and consequently at the sidelines of political discourse. Despite the appeal of popular symbols like *1984*, the costs, benefits, and broader implications of computer systems were largely indirect, if perceived at all. Without the consciousness-raising equivalent of a nuclear accident, most Americans did not view privacy as a political priority.[330]

In addition, policy makers were not writing on a clean slate. Previous court rulings had discussed privacy and frequently balanced privacy "rights" against other societal interests. In 1976, the Supreme Court decided *United States v. Miller*,[331] holding that records in possession of a third party (a bank) are considered property of that party. Under these circumstances, the individual does not have a Fourth Amendment privacy interest in the records.[332] Thus, the idea of privacy as an individual right or individual liberty had already been curtailed.

One lesson from the earlier privacy debates is that privacy, when framed as a matter of an individual interest, does not easily tap into the idea that there is a broader public purpose being pursued. In fact, those seeking to weaken proposals to protect individual privacy have successfully framed their position as a commitment to the common good (i.e., better government service, stronger law enforcement capabilities, and a less encumbered business environment). To date, arguments for

329. *See id.*

330. BENNETT, *supra* note 49, at 22–23; JAMES N. DANZIGER, ET AL., COMPUTERS AND POLITICS: HIGH TECHNOLOGY IN AMERICAN LOCAL GOVERNMENTS 1 (1982) ("the costs and benefits and the broader impacts of computer systems are largely perceived as indirect and subtle, if they are indeed perceived at all").

331. 425 U.S. 435 (1976).

332. *See* REAGAN, *supra* note 7, at 179.

privacy protection have not successfully transcended this political dynamic.[333]

3. *Defining Characteristics of Societal vs. Individual Concerns*

In an effort to move the debate forward, the theoretical foundations for a societal view of privacy must be buttressed by more policy-oriented arguments. What are the basic characteristics of issues that we generally view as societal concerns, justifying a resolution in the broader public interest? Why do we not say, for example, that individuals should police their own environmental problems and seek redress if an industry breaks the law or violates its own clean-up program? Why is environmental protection viewed as a general societal problem calling for a regulatory response in the public interest?

There are sound reasons why a societal problem like environmental pollution calls for a societal resolution. Societal problems have the following six defining characteristics:

Involuntary and unavoidable risk. We are all more or less equally and involuntarily at risk simply by living in and sharing the same environment. We have no real choice in this regard, and we are all equally susceptible to injury if legal norms are breached. We do not know which of us will become ill if toxins are released, so we all have an equal interest in controlling the risk.[334] While a person might take some steps to minimize individual exposure (e.g., eating healthy foods or moving to a city with cleaner air), we realize that such measures help, if at all, at the margin.[335] Most risks are uncontrollable by individual action.

---

333. Legislation in the United States must survive many "veto points" in the legislative process. A bill can lose momentum as a result of committee procedures, bicameral approval difficulties, floor amendments in either chamber, failure of presidential signing, and possibly another set of hurdles in agency implementation. Even in the best of political climates, any attempt to pass a comprehensive data protection law would be challenged by an influential army of industry lobbyists. *See* Bennett, *supra* note 268, at 114.

334. *See* ROBERT V. PERCIVAL, ET AL., ENVIRONMENTAL REGULATION: LAW, SCIENCE, AND POLICY 4, 5 (3d ed. 2000) (listing the basic characteristics of environmental concerns as follows: collective risks, uncertainty of mechanism and effect, potentially harmful effects, irreversibility, and uncontrollability).

335. *See, e.g.*, Daniel Machalaba, *Local Ties: Decades of Mishandling Hazardous Cargo Leave Railroads a Toxic Legacy: Areas Near Rail Yards Face Possible Health Problems; Lawsuits Are on the Rise*, WALL. ST. J., at A1, Feb. 3, 1999 (reporting that a resident who lived across from a rail yard for forty-six years used to eat watermelons and cantaloupes grown in her garden but now restricts her plantings to flowers, fearing contamination in home-grown produce; another resident says he will not allow his four children to play outside anymore for fear the ground is contaminated, explaining that he feel like they are "prisoners" in their own house).

Difficulty in identifying individual harm. When injuries occur, they are often not known or even knowable. A harm resulting from environmental contamination can be latent or, in a great number of cases, undiscoverable.[336] Yet even if an injury is undetectable, we are nonetheless concerned about potential injuries or damage that is occurring without our knowledge. Indeed, unseen harms frighten us just as much as known ones.[337]

Obstacles to tracing injury to its cause. If a person does discover an injury and suspects an environmental cause, tracing the harm to a particular source is often impossible. The source may be unknown, unknowable, or there may be many possible contributors so it is impossible to identify the perpetrator. We may identify toxins in ground water as the cause of a person's cancer, but we will have difficulty proving causation against a particular farm, industry or other contaminating source. Waste secretly dumped often avoids detection.[338]

---

336. *See* Thornton v. Roosevelt Hosp., 391 N.E.2d 1002, 1003 (N.Y. 1979) (plaintiff was exposed to a carcinogenic substance in 1954, but did not develop cancer until 1972); Le Vine v. Isoserve, Inc., 334 N.Y.S.2d 796 (N.Y. Sup. Ct. 1972) (plaintiff developed cancer nine years after exposure to radioactive isotope); Carl B. Meyer, *The Environmental Fate of Toxic Wastes, the Certainty of Harm, Toxic Torts, and Toxic Regulation*, 19 ENVTL. L. 321, 330 (1988) (reporting that the impact of toxic exposure is often intensified because many toxic substances are neither visible nor malodorous; frequently, victims neither suspect nor avoid exposure to toxic waste until its effects, enhanced by cumulative exposure, manifest themselves in acute or chronic discomfort or harm); Christopher W. Krueger, *Legislative Relief from Toxic Exposure: The Lifeguard Presumption Act*, 3 S. CAL. INTERDISC. L.J. 867, 872 (1994) (noting that the gestation period for cancer is indeterminable, appearing anywhere from six months to fifty years after the initial toxic exposure); CONGRESSIONAL RESEARCH SERVICE OF THE LIBRARY OF CONGRESS, COMM. ON ENVIRONMENTAL PUBLIC WORKS, U.S. SENATE, 96th Cong., 2d Sess., Six Case Studies of Compensation for Toxic Substance Pollution 43 (June 1980) (noting that harms at Love Canal (an abandoned hydroelectric canal in New York, where the Hooker Chemical Company placed harmful substances from 1942–53) arose over twenty-five years after the last dumping of hazardous waste).

337. *See* Bill Charles Wells, *The Grin Without the Cat: Claims for Damages from Toxic Exposure Without Present Injury*, 18 WM. & MARY J. ENVTL. L. 285, 310 (1994) (commenting that the development of an action or element of damages to compensate the plaintiff for fear of injuries that he has not yet suffered is a more recent development); Terry Morehead Dworkin, *Fear of Disease and Delayed Manifestation of Injuries: A Solution or a Pandora's Box?*, 53 FORDHAM L. REV. 527, 567 (1984) (recognizing that although precedent exists for allowing toxic tort plaintiffs who sue for fear of disease to recover, many courts have opted to focus on requirements such as physical injury or other economic harm).

338. Christopher H. Schroeder, *Lost in the Translation: What Environmental Regulation Does That Tort Cannot Duplicate*, 41 WASHBURN L.J. 583, 601 (2002) (explaining the difficulty of tracing the harm to its cause); Allan Kanner, *Environmental and Toxic Tort Issues, ALI-ABA Continuing Legal Education, Environmental Litigation*, June 26, 1995 (explaining that causation refers to two distinct issues: (1) defendant must be causally related for the liability-creating actions, and (2) there must be a medical connection between the liability-creating act and the complained of injuries).

Inadequacy of money damages. Once someone is injured, and assuming we can identify the cause, money is a rough compensation for the harm, and it will not make the person whole, even if damages can be recovered. Money damages are well suited for economic injury, but they are at best a crude substitute if the harm is not easily translated into economic terms.[339] In such cases, we are better off preventing the harm from occurring in the first place. Money cannot replace the loss.

Externalities. With societal problems such as environmental contamination, it is not possible to charge the full cost of the harm against the entity that caused it.[340] Pollution imposes costs on others that are not easily recoverable. Unclean air can increase health care costs, raise expenses for cleaning buildings, and decrease work productivity for those who take ill. Without government intervention of some kind (such as a tax on toxic emissions), the costs are not borne by the entity causing them.

Non-economic value in preventing the harm. Many aspects of life are difficult to quantify in economic terms. Most of us would agree that there are important intangible benefits to having certain legal norms in place, whether or not we can identify an economic benefit from their existence. We gain pleasure from having a clean environment (fresh air, good fishing waters, etc.) even if we do not suffer any obvious or tangible adverse effects when they are gone. While some quality of life benefits might be discussed in economic terms (e.g., we might estimate the value of clean drinking water by looking at the revenues of the bottled water industry), such an analysis seems counterintuitive and unnecessary in

339. *See* Meyer, *supra* note 336, at 370 (stating that environmental and personal injury damages are complex and difficult to measure); Schroeder, *supra* note 338, at 589 (arguing that the goal of modern environmental regulation is to prevent harm to the environment before it occurs, with an implementation structure that includes prior approvals, permits that embody standards to be met, and the monitoring of compliance).

340. *See* EBAN S. GOODSTEIN, ECONOMICS AND THE ENVIRONMENT 33–39 (1995) (discussing why it is not possible for victims of negative externalities to simply band together on their own to prevent pollution); Kenneth S. Abraham, *The Relation Between Civil Liability and Environmental Regulation: An Analytical Overview*, 41 WASHBURN L.J. 379, 379 n.2 (2002) (externalities resulting from barriers to the imposition of liability on those who create environmental risk were the principal justifications for the development of environmental law, and especially for the enactment of the major federal regulatory statutes of the 1970s); Henry N. Butler & Jonathan R. Macey, *Externalities and the Matching Principle: The Case for Reallocating Environmental Regulatory Authority*, 14 YALE L. & POL'Y REV. 23, 29 (1996) (arguing that the economic goal of government regulation of pollution is to force polluters to bear the full costs of their activities).

many circumstances.[341] We enjoy certain things because we are human, and our lives would be less fulfilled if they were gone.

In contrast to a problem of societal concern, a problem of individual concern such as a consumer warranty complaint or deceptive advertising program typically has a very different set of characteristics:

Voluntarily assumed risk. The risk of injury is usually created individually and assumed voluntarily. By purchasing a car, we create expectations of quality from a specific product or manufacturer; by signing a lease, we establish a landlord/tenant relationship with a management company we chose; by dropping off shirts at the cleaners, we entrust the local merchant with our property. We make choices and voluntarily assume certain risks when we do so, and in this way we distinguish ourselves from the rest of society.[342]

Discoverable injury. The car does not work properly, or the landlord breaches the lease. Although we might not know exactly what went wrong until further investigation reveals the actual cause, we usually know that an injury of some kind has occurred. We can then try to trace its cause and seek appropriate redress.

Fewer tracing obstacles. With most consumer problems of individual concern, tracing the injury to a particular source is typically not the problem. We know who caused the injury because we know who the other party in the relationship was. Even if the source of the problem is not readily identifiable, the list of possibilities is usually small and finite. For example, in an unlawful debt collection practice the wrongdoer will

---

341. *See* Dworkin, *supra* note 337, at 566 (discussing emotional illness and stress associated with the threat of cancer and other diseases). Even some economic injuries are non-compensable. *See* Adkins v. Thomas Solvent Co., 487 N.W.2d 715, 730 (Mich. 1992) (twenty-two property owners who lived near a contaminated site could not recover for the diminution of their property values because no contaminants actually had migrated to their property). *See generally* Richard L. Manning, *Changing Rules in Tort Law and the Market for Childhood Vaccines*, 37 J.L. & ECON. 247 (1994) (discussing ways of valuing pain and suffering).

342. Many consumer relationships are based in contract, and the relationship is voluntarily undertaken. *See* Stephen J. Ware, *Employment Arbitration and Voluntary Consent*, 25 HOFSTRA L. REV. 83, n.134 (1996) (citing ALAN WERTHEIMER, COERCION 4 (1987) (noting that "the general assumption is that promises are binding . . . if, but only if, the relevant actions are voluntary")); Robert E. Scott & William J. Stuntz, *Plea Bargaining as Contract*, 101 YALE L.J. 1909, 1919 (1992) (the central normative justification for contractual enforcement is facilitating the exercise of voluntary choice). *But see* Michael Philips, *Are Coerced Agreements Involuntary?*, 3 LAW & PHIL. 133, 133 (1984) (observing that the term "voluntary" could be used to describe all willful acts, i.e., as a synonym for "volitional"; Michael D. Bayles, *A Concept of Coercion*, *in* XIV NOMOS: COERCION 16, 18 (J. Roland Pennock & John W. Chapman eds., 1972) ("[A] man who is physically forced to squeeze the trigger of a gun does not do it voluntarily in any sense. But a man who fires a gun due to a threat does in one sense act voluntarily although he does not in another.").

likely be either the creditor itself, a financial institution as the creditor's assignee, or a collection agency to whom the creditor transferred the debt.

Economic injury predominates. Transactions usually involve payment for goods or services. If we are compensated for the economic losses, we have some confidence that justice was done. Although full compensation may be difficult to obtain given that we may have to pay attorney's fees or we have difficulty proving consequential harm, injury is usually economic and money damages can compensate for it.

Fewer external costs. In most consumer transactions, externalities are usually nonexistent or a small part of the harm done. The injury caused by breaking the legal norm usually affects only a single individual or class of individuals. Ripple effects to society at large are usually not significant.

When viewed in this light, information privacy fits the "public interest" model better than the "individual concern" model:

- We are all equally at risk of injury from misuse of our data, and we cannot avoid the problem if we are to participate in modern society. Information about us is seemingly everywhere, and we can do little to minimize its collection and use.[343]

- Except in the most egregious situations, harms resulting from information misuse may never be known to us. So much of our data is being shared every day, yet we have no idea what the ramifications may be (good or bad) or what decisions are being made in reliance on it.[344]

---

343. *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 108, 108-09 (2001) (discussing how ineffective efforts to keep personal information secret will be since "one's personal information is available from so many sources").

344. *See* Adam S. Marlin, *Online Identity Theft a Growing Concern*, CNN.COM, *at* www.cnn.com/2000/TECH/computing/08/16/id.theft.offline.idg/index.html (Aug. 16, 2000) (describing how an identity thief obtained a doctor's personal information from the Medical Board of California and another web site (medical license and Social Security number) and used them to buy medical supplies on his credit; by the time the doctor convinced the medical supply company that he had not made the purchases and learned that someone had stolen his identity, the identity thief had spent $185,000); PRIVACY RIGHTS CLEARINGHOUSE, IDENTITY THEFT VICTIMS' STORIES, LEGISLATIVE TESTIMONY OF JOHN AND JANE DOE (testifying before the Maryland legislature that he was shocked to find out that he and his wife had no credit: "We were being accused of defaulting on loans, not making car payments, and overdue on credit card payments. We were suddenly being called by stores that we never heard of, banks demanding payment on cars or loans that we didn't have, collection agencies demanding that we pay immediately on some account we never heard of, or face legal action against us.") *at* http//:www.privacyrights.org/victim5.htm (1999); Identity Theft

- Even if we discover an injury from data sharing, tracing its cause to a particular information source or leak will likely be difficult, if not impossible.[345] Obtaining effective redress will therefore be rare.[346]

- Injury, while economic in some cases, can be very hard to undo. This is particularly true with identity theft, the loss of an employment opportunity, or harm to reputation caused by embarrassing information being revealed.

- Information misuse imposes significant external costs beyond the direct injury to the individuals involved. Financial institutions, for example, incur costs investigating claims of

---

Resource Center, Amy Jo Sutterluety, *The Silent Encroachment on Our Privacy: One Woman's Search for Her Stolen Identity, at* http://www.idtheftcenter.org/html/silent.htm (2000) (revealing that one victim's search to find the ring of thieves who were impersonating her started with a call to a home-furnishings store that had sent her a letter asking her to confirm a credit application and ended 180 phone hours and 580 miles later).

345. With identity theft, the only solvent entity against whom a lawsuit might be brought will often be the financial institution that opened a credit account or otherwise dealt with the thief. Liability will not likely be found, however, unless the victim can show that the institution was negligent. *See* Stephen L. Wood & Bradley I. Schecter, *Identity Theft: Developments in Third Party Liability*, 8 (No. 3) CONS. & PERSONAL RIGHTS LITIG. 3, 5 (Summer 2002).

346. *See* UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT TO CONGRESSIONAL REQUESTERS, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363, (Mar. 1, 2002) [hereinafter GAO REPORT] (reporting that identity theft can cause potentially severe emotional or other nonmonetary harm in addition to economic harm; the leading types of non-monetary harm cited by consumers were "denied credit or other financial services (mentioned in over 7,000 complaints), "time lost to resolve problems" (mentioned in about 3,500 complaints), and "subjected to criminal investigation, arrest, or conviction" (mentioned in almost 1,300 complaints)); *See generally* Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756 (1995) (assessing common-law and federal legislative remedies for commercial disclosures of information that violate personal privacy); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) (arguing that privacy law has fixed itself too firmly to certain conceptions of privacy, and as a result, has lost flexibility in dealing with emerging privacy problems). *Cf.* Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1A (last visited Jan. 27, 2003) (explaining that the key market failures with respect to privacy are due to information and bargaining costs: "[A] company that acquires personal information gains the full benefit of using the information but does not suffer the full losses caused by disclosure. Because of imperfect monitoring, customers often will not learn of the disclosure and will not be able to discipline the company in the marketplace for its less-than-optimal privacy practices. Because the company internalizes the gains from using the information, but can externalize a significant share of the losses, it will have a systematic incentive to over-use private information.").

credit card fraud and re-crediting customer accounts.[347] Some of these costs are passed though to customers in the form of higher interest rates and incidental fees, so we all pick up a share of the expenses when privacy breaches cause harm.[348]

- Most of us would say that we benefit in intangible ways just knowing that our data is reasonably secure, and is not being bought and sold without our permission. We would feel less vulnerable if we knew that our data was either not being collected or, at least, was protected from misuse. Such sentiments are worth respecting in their own right, but they can translate into economic benefits as well. If we felt more secure in our relationships with data collectors, we might use their services more. One of the impediments to the development of Internet commerce is the fear many people have that the information they transmit could be shared, misused, or stolen.[349]

Even though information privacy has many of the defining characteristics of other societal values, this does not mean that a heavy-handed regulatory approach should be used to protect our privacy interests. One important difference between information privacy and

347. *See* Wood & Schecter, *supra* note 345, at 4 ("law enforcement consider banks and financial institutions to be the 'victims' in identity theft cases [because] they are frequently forced to absorb the costs of the thefts").

348. *See* LoPucki, *supra* note 343, at 91 (stating that in dealing with the problem of identity theft, defrauded creditors are likely to employ legal and practical means that are cost effective, and pass the remaining costs on to their consumers); Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 663 (1999) (estimating that identity theft imposes a cost on consumers approaching $100 million annually); GAO REPORT, *supra* note 346 (stating that the American Bankers Association reported total check fraud-related losses reached $2.2 billion in 1999; Mastercard's and Visa's aggregated identity theft-related losses from U.S. operations rose to $114.3 million in 2000; total cost of one national consumer reporting agency's Fraud Victim Assistance Department was $4.3 million for 2000).

Apart from cost-benefit analysis, economic arguments misconstrue the harm to society from the loss of confidence in information practices. Many view privacy as central to the democratic fabric of society. The misuse of personal information harms an individual and deserves protection regardless of how the misuse might benefit others. *See* Reidenberg, *supra* note 134, at 725.

349. FEDERAL TRADE COMMISSION, *supra* note 285, at 2 (reporting that 92% of consumers are "concerned," including 67% who are "very concerned," about the misuse of personal information online, and explaining that this apprehension likely translates into lost online sales due to lack of confidence in how online personal data will be handled; also cites a study that estimates potential losses in online retail sales due to privacy concerns will reach $18 billion by 2002).

societal problems like environmental pollution or unsafe food and drugs is that privacy is seldom a matter of life and death. The effects of even a widespread disclosure of personal information will not be as catastrophic as global warming or a mass outbreak of contagious disease. Still, the case for viewing information privacy as a societal value should not be discounted. If the stakes do not seem quite as high, the appropriate policy resolutions may differ but the regulatory function of government need not be minimized and the policing of privacy interests need not be left to market forces and individual enforcement initiatives. A less intrusive, but nonetheless vital, governmental role may be in order.

Throughout our history, we have created administrative bodies to implement national legal norms and regulate important societal values. Not all have concerned basic health and safety issues. The Securities Exchange Commission oversees the operation of our capital markets, the Equal Employment Opportunity Commission ensures fair employment practices, and the Comptroller of Currency watches over our national banks. In all of these areas and many others, oversight became necessary when policy makers realized that market forces could no longer effectively protect important societal interests. As we witness the vast expansion of digital databases and nearly complete loss of control over the collection and dissemination of our personal information, we see that the same conditions presently exist with our interest in information privacy.

B. Looking to Europe for a Model

There is reason to believe that our approach to the database problem would take a different form, and policy resolutions would be recognizably different, if the issue were viewed in a different way. In Europe, for example, privacy is treated as a political imperative, anchored in fundamental human rights, and considered a matter of basic "social protection."[350] National and regional governments are viewed as key players in ensuring data protection, and the problem is considered an

350. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1347 (2000). This difference in political philosophy was likely influenced by fairly recent experiences in Europe with information abuse. A 1984 conference on data protection concluded that "one of the prime motives for the creation of data protection laws in continental Europe is the prevention of the recurrence of experiences in the 1930s and 1940s with Nazi and fascist regimes." *See* David H. Flaherty, *Nineteen Eighty-Four and After: Final Report of the Bellagio Conference on Current and Future Problems of Data Protection*, GOV'T INFO. Q. 5 (1984); BENNETT, *supra* note 49, at 30.

important element of public law. Market forces and individual enforcement are important in the regulatory scheme, but they are not the primary policing mechanisms. Law and government are considered fundamental in ensuring shared norms of social and citizen protection.[351]

The most important act of legislation dealing with information privacy was the 1996 European Community Directive on Data Protection (EU Directive), which outlines the basic principles for European Union member countries.[352] The EU Directive took effect in 1998, and although the Directive has its share of critics,[353] it recognizes some key dimensions of the problem that are missing in United States privacy law.[354] The Directive mandates that all fifteen EU Member States ensure that citizens have the right to access their data, the right to fix erroneous data, the right to a recourse for violations, and the right to keep the information from being used for any marketing purpose without their permission.[355]

More importantly, however, unlike most American privacy laws, the EU Directive applies essentially the same standards to private sector and

---

351. *See* Reidenberg, *supra* note 350, at 1347.

352. *See generally* Directive 95/46/EC of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data, 1995 O.J. (L 281) 31 (Oct. 24, 1995) (EU Directive). The EU Directive was first proposed by the European Commission five years earlier. *See* EUROPEAN COMMISSION, PROPOSAL FOR A COUNCIL DIRECTIVE CONCERNING THE PROTECTION OF INDIVIDUALS IN RELATION TO THE PROCESSING OF PERSONAL INFORMATION, COM (90) 314 Final-SYN 287 (1990). *See generally*, Paul Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995). The Directive is one of several European Union acts designed to ensure that the free movement of capital and labor will be supported by the free movement of information. Bennett, *supra* note 268, at 105. The Directive must be implemented in each Member State, usually through legislative action in the Member State. *See, e.g.*, Swedish Personal Data Act (1998:204); Data Protection Act 1998 (1998 ch. 29) (United Kingdom); Protection of Individuals and Legal Persons Regarding the Processing of Personal Data Act (Jan. 1997) (Italy).

353. *See, e.g.*, Cate, *supra* note 122 (arguing that the EU approach is not compatible with longstanding constitutional and political traditions in the U.S.); PETER SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 14, 50–53, 191 (1998) (EU Directive may have limited usefulness outside the world of mainframe computers).

354. The progression from the 1975 Council Resolution to the Treaty of Amsterdam evidences an increasing centralization of consumer policymaking at the Community level, if only in theory. Overby, *supra* note 174, at 1241 (discussing the progression).

355. Article 2(a) of the EU Directive broadly defines protected information as "any information relating to an identified or identifiable natural person." Article 2(b) defines data "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available . . . ." EU Directive, *supra* note 352, art. 2(a), (b).

government data bases.[356] Cross-sectoral legislation in each Member State guarantees a set of fundamental privacy rights that ensure the fair treatment of personal information. Data protection laws define each citizen's basic legal right to control personal information. Instead of beginning with a presumption of legitimacy for government and commercial enterprises that wish to collect and share information, the European approach seeks to strike a balance that provides for a high level of data protection for all EU citizens.[357]

Information policies in Europe tend to have broad applicability and cut across economic sectors.[358] There is an underlying presumption that the collection and sharing of personal information, particularly in the private sector, is not a standard practice that citizens must simply learn to accept. Information can be collected only for specified purposes, used in ways that are compatible with those purposes, and stored no longer than is necessary.[359] Individuals must be told that information is being collected, the purposes of the data collection, and the person responsible for collecting and controlling the information after it has been stored.[360] Affirmative consent is required in more situations when data is to be collected or shared, with less responsibility on the individual to opt-out of data sharing.[361] Independent, national supervisory authorities oversee, investigate, and enforce legal norms.[362] National "ombuds" serve as

356. Indeed, earlier drafts of the Directive placed stronger restrictions on the private sector than on governments. The final version treats them essentially the same. Moreover, the scope of protection in the Directive does not depend on the technique used to store information. Manual filing systems are covered as well as computerized systems. BENNETT, *supra* note 49, at 105–07.

357. *See* Reidenberg, *supra* note 134, at 731; Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 469 (2000).

358. *See generally* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995) (discussing events leading to the adoption of the EU Directive).

359. *See* SCHWARTZ & REIDENBERG, *supra* note 122, at 13–14.

360. *See id.* at 15.

361. The EU Directive mandates that the national law of all Member States protect information about each identifiable individual even if the data is publicly available. Laws must also require an individual's consent before processing personal information, except for the purposes contemplated by the original data collection. Member States can further restrict the processing of data deemed "sensitive" (e.g., medical information), and certain "black list" data is not collectable at all without the affirmative consent of the individual. This includes data revealing racial/ethnic origin, political views, religious beliefs, and membership in a trade union. EU Directive, Art. 8(1). *See* Reidenberg, *supra* note 134, at 732.

362. *See* Cate, *supra* note 122, at 186.

advocates for individuals who feel that a breach has occurred.[363] Persons who process individual information in both the public and private sectors must comply with notice and reporting mandates so their activities can be monitored.[364] Civil liability and "dissuasive penalties" must be available for noncompliance with legal norms.[365]

C. *Moving Toward a Global Information Policy in the United States*

Circumstances already exist that may move the United States toward the European approach to information privacy. The EU Directive is far from perfect, particularly with regard to enforcement of its mandates,[366] but it is clearly becoming the international model for data protection.[367] We are seeing a convergence of information policy worldwide, and the United States is under increasing international pressure to conform.

Article 25 of the Directive states that transfers of information about EU citizens to a country outside the EU may take place only if the receiving country ensures an "adequate level of protection."[368] EU Member States are instructed "to take the measures necessary to prevent [the] transfer of data of the same type to the third country in question."[369]

---

363. In the 1970s, four Nordic countries (Denmark, Finland, Norway, and Sweden) established the office of consumer ombudsman, a supervisory body for overseeing the marketing of consumer goods and services. *See generally* Kjersti Graver, *A Study of the Consumer Ombudsman Institution in Norway with Some References to the Other Nordic Countries I*: Background and Description, 6 J. CONS. POL'Y 1 (1986). Similar offices have been created in other nations. *See* Ewa Letowska, *The East Block's First Government Ombudsman*, INT'L HERALD TRIB., Jan. 8, 1988, at 5.

364. *See, e.g.*, Italian Data Protection Act (1996), *in* MARC ROTTENBERG, THE PRIVACY LAW SOURCEBOOK 2000, *available at* http://www.privacy.it/legge675encoord.html (2000). The Forward to the Italian law proclaims that data should be processed "by respecting the rights, fundamental freedoms and dignity of natural persons, in particular with regard to privacy and personal identity." Privacy is considered a "fundamental component of the 'electronic citizenship.'" *Id.* Member States must also require any person processing personal information to notify the national supervisory authority, which is required to keep a public register of data processors. Reidenberg, *supra* note 98, at 733. States must delegate responsibility to one or more public authorities for monitoring the compliance with the law. EU Directive, Art. 28. These authorities must act with "complete independence" and must be given investigative authority and the power to bring legal proceedings. *See* Bennett, *supra* note 268, at 108.

365. EU Directive, arts. 23, 25.

366. *See* Lynn Chuang Kramer, *Private Eyes Are Watching You: Consumer Online Privacy Protection—Lessons from Home and Abroad*, 37 TEX. INT'L L. J. 387, 409–10 (2002) (noting lack of compliance with the EU Directive in a survey of European websites).

367. *See* Graham Greenleaf, *The 1995 EU Directive on Data Protection—An Overview*, 3 INT'L PRIVACY BULLETIN, no. 2, at 1 (1995); Joel Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 303 (1993).

368. EU Directive, Art. 25(1).

369. EU Directive, Art. 25(4).

This means that national authorities in each Member State can prevent U.S. businesses from processing data of EU citizens if U.S. privacy protections are not up to EU standards.[370] The consequences of this provision are severe for credit-granting and financial institutions, hotel and airline reservations systems, direct-marketing firms, insurance companies, and any commercial enterprise that relies on the flow of personal information from European sources. Europe has made it clear that it will not tolerate "data havens" that would compromise the personal information of its citizens.[371]

The EU Directive now constitutes the "rules of the road" for the increasingly global nature of information processing. The Directive represents a multi-national consensus on the content of data protection rights, and has proved to be a valuable model for countries looking to enact their own data protection laws.[372] Pressures for "policy convergence" worldwide have prompted other nations to adopt similar principles that give their citizens more control over personal information.[373] Significant movement toward an EU-style data protection has already occurred in Canada, South America, and Eastern Europe, and the movement is spreading to other regions.[374] The international

370. *See* Reidenberg, *supra* note 134, at 736. In the U.K., the Data Protection Registrar blocked a proposed sale of a British mailing list to a U.S. direct mail company. *See* OFFICE OF THE DATA PROTECTION REGISTRAR, SEVENTH ANNUAL REPORT 33–34 (1990).

371. Bennett, *supra* note 268, at 109–10.

372. *Id.* at 111–12.

373. Convergence in this context means more than similarity at a given point in time. It points to a pattern of similar regulatory regimes developing over time, rather than a static condition. *See* BENNETT, *supra* note 49, at 111. Bennett identifies five principle causes for this policy convergence: (1) technological determinism, (2) the influence of pioneers in the field, (3) the interaction of a small group of international experts, (4) harmonization projects of international organizations, and (5) the accelerating pace of global commerce that forces states to make policy changes that conform to international norms. *Id.* at 116–17. Supporting evidence of policy convergence also comes from David Flaherty, who examined the workings of national and state data protection agencies in Germany, Sweden, France, Canada and the United States. FLAHERTY, *supra* note 84. For statements of privacy principles in an international context generally, see BENNETT, *supra* 49, at 96–115 (discussing convergent themes of openness (disclosure of the type of information collected and from what categories of individuals), individual access and correction, limits on what information can be collected (e.g., relevant and necessary to accomplish the limited purposes of the collecting entity), limits on how data can be used, limits on disclosing information to external sources, and security safeguards. *See also* OECD Guidelines, *supra* note 142.

374. By the end of the 1980s, most European countries applied the same data protection standards to both the public and private sector. The U.S., Canada, Australia and Japan rejected this approach, regulating the public sector with one set of laws (e.g., the Privacy Act in the United States) and the private sector with sector-specific laws and voluntary codes of practice. *See* Bennett, *supra* note 268, at 100. Not much had changed by the end of 1996. Of the 24 OECD countries, only six had failed to

harmonization of data protection laws can be attributed partly to pressure from Europe and the effects of Article 25, but it is fueled by the conceptual appeal of a comprehensive set of standards that were carefully crafted by the EU after years of study and debate. Those rules are becoming the standard for multi-national transactions in the increasingly global environment of offline and online data sharing.[375] In this regard, United States information policy lags behind.[376]

However, we may not be behind for long. Many U.S. businesses are already affected by the European standards. Companies that handle information about European citizens must now certify compliance with European data protection principles.[377] A Safe Harbor agreement between the Department of Commerce and the European Commission

---

enact a comprehensive privacy law to all data processing entities: U.S., Canada, Australia, Japan, Greece and Turkey. As a Member State in the EU, Greece must now conform to the standards of the EU Directive. *Id.* at 113. In the U.S., the private sector continues to be regulated through an expanding but still incomplete patchwork of federal and state laws, with no general oversight agency for privacy compliance in the U.S., and few effective remedies. *Id.*

More recently, the EU Directive has had its influence worldwide. In October 2000, the Argentinean Congress approved a data protection act (Law 25.326) based on the EU Directive. *See* Kennedy & Meade, *supra* note 74, at 347. Canada recently passed its Protection of Personal Information and Electronic Documents Act (Bill C-6), effective January 1, 2001. 48–49 Elizabeth II, ch. 5, *available at* http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052bE.html (Apr. 13, 2003).

375. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 45–51 (2000).

376. Mechanisms outside the law, such as "contractual" agreements between American businesses and data protection authorities in specific countries, can minimize privacy conflicts for e-commerce transactions, but an international treaty may ultimately be necessary to ensure the growth of trans-border information exchange. The U.S. could, for example, promote a "General Agreement on Information Privacy" within the WTO framework. *See* Reidenberg, *supra* note 134, at 747.

Of course, inferences about the actual level of data protection in any country cannot be drawn merely by reading the statutes. In this regard, data protection is different from other societal problems like environmental protection, where states might agree on a desirable level of a particular contaminant in the atmosphere and have a clear understanding of how to monitor and assess performance. *See* Bennett, *supra* note 268, at 119. Assessing the level of data protection in practice is a difficult problem of measurement and is not addressed in this article.

377. The EU Directive bars the dissemination of information about EU citizens to entities outside of Europe where looser protections are in place. Sweden, for instance, insisted that American Airlines delete all health and medical information (including dietary requests) they had gathered on Swedish passengers unless the airline obtained the consent of each passenger to allow them to keep the info in the database. *See* American Airlines v. Sabre Kammarratan i Stockholm (Admin. Ct of Appeal, Stockholm), Apr. 1997; Paul R. Prabhaker, *Who Owns the Online Consumer?*, 17 J. CONS. MARKETING 158, 161 (2000). European nations can thus use the Directive to exert significant pressure on U.S. companies.

assists businesses who want to comply,[378] and nearly 200 American corporations have signed up.[379] If companies find that the EU norms are not unduly burdensome, then resistance to a similar regime in the United States may weaken. Moreover, as American policy makers see that U.S. companies are giving EU citizens greater data protection than U.S. citizens, then pressure to change our laws may increase.

The Safe Harbor agreement was a response to the real possibility that Europe would prevent data flows to the U.S. and to pressure from online industries that did not wish to take that risk.[380] The U.S. Department of Commerce negotiated with the European Commission for an agreement that would assure Europe that U.S. businesses could comply with Article 25 even if the U.S. did not change its privacy laws.[381] In the agreement, the European Commission endorsed what amounts to a voluntary code of conduct that, the parties agreed, would meet the Article 25 standard.[382] The Department of Commerce then established the Safe Harbor mechanism allowing American businesses publicly to commit to this code for the treatment of European data. If businesses make and adhere to the commitment, they can be assured of continuing data transmissions from Europe.

There are several reasons why a U.S. based business with European operations might want to certify compliance with the Safe Harbor agreement. It reduces the likelihood that European privacy authorities would target a company on the compliance list, thereby avoiding the interruption of data flows and any associated negative publicity. In addition, claims brought by EU citizens would be brought in U.S. courts. Drawbacks include the difficulty of complying with the Safe Harbor, especially for a large corporation that uses personal data in various ways that may not be allowed. Risk of prosecution under the Safe Harbor,

---

378. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45, 665–686 (Dept. Commerce, July 24, 2000) (Safe Harbor). The decision to enter into the Safe Harbor is voluntary, but once made the company must (1) publicly declare its participation, (2) annually certify to the Department of Commerce that it is complying, and (3) provide notice to its customers that it adheres to the Safe Harbor. *See* U.S. Dep't of Commerce, Safe Harbor Overview, *available at* http://www.export.gov/safeharbor/sh_overview.html (last visited January 30, 2003).

379. The Safe Harbor procedure and a list of companies that have agreed to adhere to the Safe Harbor Principles can be found at www.export.gov/safeharbor/ (last visited January 30, 2003).

380. Reidenberg, *supra* note 134, at 738.

381. *See* Letter from David L. Aaron, U.S. Dep't of Commerce, to Industry Representatives (Nov. 4, 1998), *available at* http://www.ita.doc.gov/td/ecom/aaron114.html.

382. *Id.*

either by consumers or the FTC, may be higher than the risk of prosecution by EU authorities.[383]

There are legal and practical problems with the Safe Harbor agreement, however, that may limit its effectiveness as a standard for data collection and widespread use in the United States. First, some European Member States have expressed concerns about the adequacy of the agreement.[384] To the extent national privacy authorities find its data protection provisions inadequate, they can influence the way American businesses deal with information of European origin through threatened prosecution of American businesses.[385] Second, the Safe Harbor agreement relies largely on the authority of the FTC to ensure compliance, but the jurisdiction of the FTC and it ability, as practical matter, to fill this role are questionable. Amendments to section 5 of the FTC Act in 1975 extended the jurisdiction of the FTC to unfair or deceptive acts and practices "in or affecting commerce,"[386] but there is no evidence that Congress contemplated protecting foreign consumers or American businesses from foreign prosecution. Its purpose was to extend the jurisdiction of the FTC to protect American consumers from a broader range of unfair or deceptive practices by businesses. The claim that Safe Harbor comes within section 5 of the FTC Act is a departure from the purposes of the statute and could be subject to legal challenge.[387]

---

383. *See* Lillian Blageff, *Review and Update on Data Protection and E-Commerce Issues*, CORP. COUNSEL INT'L ADVISOR 192–97 (May 1, 2001).

384. Reidenberg, *supra* note 134, at 744. For many Member States, Safe Harbor weakens their data protection standards. It exempts public record information and any information processing called for by "conflicting obligations" or "explicit authorizations" in U.S. law. These vague authorizations could turn into large loopholes for U.S. businesses who claim they cannot comply with European standards because of some other agreement or U.S. law that imposes different demands. The Safe Harbor agreement also weakens European standards for redress. Under the EU Directive, victims must be afforded legal recourse and a remedy in damages. The Department of Commerce assured the European Commission that Safe Harbor and the U.S. legal system provided for remedies for individual European victims of Safe Harbor violations. In support of its claim that U.S. law provided adequate remedies for information privacy violations, the Department of Commerce made some misleading statements about the remedies available to aggrieved individuals. In fact, few effective remedies for privacy violations exist. *See id.* at 744–45.

385. The directive states that national "supervisory authorities" have investigative powers and the right to institute legal proceedings against violators of the privacy laws mandated in the directive. EU Directive, art. 28(3).

386. *See* Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 201, 88 Stat. 2183, 2193 (1975).

387. *See* Reidenberg, *supra* note 134, at 741.

In addition, the Safe Harbor agreement vastly overstates the extent of privacy protection offered by U.S. law, and in any event, it may not be broad enough in scope to have a significant effect on U.S. information policy.[388] By its terms, it applies only to the activities of organizations that fall within the regulatory jurisdiction of the FTC and the Department of Transportation.[389] As a result, many economic sectors will not be able to insulate themselves from EU challenges by committing to the voluntary code. Among these sectors are the financial services and telecommunications industries, which are excluded from FTC jurisdiction.

IV. CONCLUSION

If information privacy were viewed more as a societal problem than one of individual concern, privacy policy in the United States would not necessarily change. The stakes might simply be too small. Data privacy, while important to most people, is not generally regarded as an absolutely critical societal value. Even the most ardent privacy advocates would not put it in the same class as basic health and safety concerns. If the risks are viewed as real but not particularly important, then the need for a fundamental shift in policy or a strong regulatory response may be lacking even if we view the problem as one of general societal concern.

Moreover, even in the regulation of societal problems like environmental pollution, we often do not use a singular, comprehensive approach. We have sectoral laws, such as water, air, noise, and laws governing specific industries such as coal burning utilities, and policies that reflect compromises reached in part by looking at the costs and benefits of various alternatives. We do not expect absolutely clean air and water. We should not expect to keep information about us absolutely private. Tradeoffs are inevitable. Most of us do not want or expect to keep our information completely private. We benefit from the collection and sharing of information in many ways.

The question remains whether we will see a fundamental shift in the way information privacy is controlled in the United States, or whether our interests will continue to be bought, sold, and given away as freely as they have been in recent years. I have argued in this article that privacy

388. *See* Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2806–09 (2002).

389. Reidenberg, *supra* note 134, at 743.

should be viewed as a societal value, and if it were understood in this way, a more comprehensive regulatory approach like the one in place in Europe and a growing number of other regions could emerge in the United States. No legal impediments to a European-style regulatory regime exist.[390] Commercial speech and speech on matters of purely private concern enjoy less First Amendment protection than speech related to political discourse.[391] Congress has enacted privacy legislation many times before with few constitutional conflicts, and it could rationally conclude that personal information about its citizens warrants more protective legislation than currently exists.

The obstacles to a more comprehensive approach to information privacy are rooted not in our laws but in our view of the appropriate function of government and the role of the private sector in ordering societal relationships. Legalities aside, our long history of general distrust in government solutions, coupled with our preference for open information flows and reliance upon market forces, make a comprehensive regulatory approach less likely as a practical and political reality.[392]

Given the political history of the privacy debate in this country, no significant shift in U.S. policy seems likely to occur until some crisis or highly publicized event forces us to look at the issue from a new perspective. Indeed, in the current political climate, efforts to press a fundamental shift in policy appear to be losing momentum. With the Chairman of the FTC coming out strongly against new privacy legislation, the prospect for instrumental change seems even more

390. *See* Volokh, *supra* note 122, at 1055 (opposing information privacy rules on free speech grounds, but conceding that First Amendment limitations on nongovernmental gathering of information are unclear); Krotoszinski, *supra* note 56, at 242 ("[T]he states or Congress could enact privacy-protection laws that limit the legal means of obtaining information about non-public figures involving matters that are not of public concern."). *But see* Cate, *supra* note 122 (the U.S. Constitution does impose restrictions on privacy legislation addressed to the private sector). Some courts have struck down state privacy laws under the Commerce Clause. *See* authorities cited *supra* note 208.

391. *See* Florida Bar v. Went for It, Inc., 515 U.S. 618, 623 (1995); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985).

392. *See* Cate, *supra* note 122, at 219–25 (observing "four features of American society" that work against an EU style of privacy protection); BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD (March 1997) at 2 ("it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society . . . ").

remote.[393] Without a sense of urgency, special interest politics and a general anti-regulatory sentiment will likely dominate political discourse in the United States on this issue for the foreseeable future.[394]

A change in perception can occur over time, however. If people start thinking about privacy as a general societal concern, the rhetoric of public debate can shift and the range of politically acceptable policy resolutions can expand. If no change occurs, we can expect to see more laws enacted periodically that purport to address privacy concerns in particular sectors, but individuals will still be expected to shoulder the burden of monitoring their own information, and market-based solutions will predominate.[395] So long as information privacy is viewed largely as a matter of individual concern, individuals will be asked to carry the lion's share of the burden. In time, we may get better at the task, especially as younger generations become more comfortable with the technologies that control the flow of our data. For now, we have little choice but to hope, wait and trust that the data collectors who are holding our personal information are guarding it securely and using it only for purposes we would prefer.

393. *See supra* notes 301–04 and accompanying text; Remarks of FTC Chairman Timothy J. Muris, *supra* note 304 (calling for increased enforcement of current laws rather than new legislation).

394. *See* Schriver, *supra* note 388, at n.189 (observing that most privacy legislation has been enacted in response to public scandals, thus explaining its patchwork quality).

395. In the past two years, dozens of privacy bills have been introduced in Congress. *See supra* note 300 and the website for the Electronic Privacy Information Center, *available at* http://www.epic.org/privacy/bill_track.htm (last visited, Jan. 20, 2003).