UNIVERSITY OF
COLORADO LAW REVIEW
*Volume 76, Number 1* *2005*

# INCOMPARABILITY AND THE PASSIVE VIRTUES OF AD HOC PRIVACY POLICY

JAMES P. NEHF*

In *The Least Dangerous Branch*,[1] Alexander Bickel advocated the use of "passive virtues" in Supreme Court decision making as a way to deepen confidence in the judiciary and safeguard the esteem in which the Court is held. Bickel argued that the Court should selectively use procedural doctrines such as standing, ripeness, and political question to ensure that it does not rule on the merits of a case when doing so might erode the Court's effectiveness.[2] By withholding precedent on an important substantive issue for a period of years, the Court gives lower courts, litigants, and the general public more time to experience the issue in various contexts and to debate the merits of competing ideas. When the Court decides the issue at a later time, it is better equipped to develop an enduring legal standard.

As Bickel was advocating passive virtues for the Court forty years ago, Congress was considering bold national legislation to set privacy rules for the collection and sharing of personal information in federal government agencies and the private sector of the U.S. economy.[3] After years of debate, Congress addressed information policy in the federal

* Professor and Cleon H. Foust Fellow, Indiana University School of Law—Indianapolis; Visiting Professor, University of Georgia School of Law. I would like to thank Sally Molloy, Elizabeth Harris, and Jeffrey Lell, my research assistants at the University of Georgia. Special thanks to the International Association for Consumer Law and participants in the Ninth Annual International Consumer Law Conference in Athens, Greece, whose comments on an early draft of this paper were invaluable.

1. ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH: THE SUPREME COURT AT THE BAR OF POLITICS 111 (1962).

2. *Id.* at 174.

3. With the rapid development of computerized record keeping in the early 1960s, concerns about information privacy first surfaced as a political and social issue, prompting hearings on the subject in Congress. *See The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the H.R. Comm. on Gov. Operations*, 89th Cong. (1966), *reprinted in* JOINT COMM. ON GOV. OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 9-28 (1976).

government with the Privacy Act of 1974, but in the non-governmental sector it chose a more passive approach.[4] By doing little to regulate information privacy outside government agencies, Congress defaulted to a voluntary, market-oriented model that relied on individual self-policing as the dominant means of information control, supplemented in later years by state laws and federal sector-specific legislation. Proposals for a federal "privacy board" that would oversee a national policy, for example, were rejected.[5]

The passive approach prevailed into the 1990s. Congress, state legislatures, and oversight agencies such as the Federal Trade Commission were reluctant to enact broad-based privacy rules, perceiving a lack of consensus on generally accepted privacy principles and fearing the erosion of societal benefits brought about by new technologies and the free flow of information. To this day, information privacy in the United States relies heavily on individuals guarding the integrity of their data records and protecting personal information from unintended use.[6] While Congress and state legislatures have periodically addressed privacy concerns in particular sectors, individuals are still expected to shoulder the heavy burden of protecting and monitoring others' use of their personal information.[7]

One of many reasons for the passive approach is the basic incomparability of the competing norms. Policymakers are continually asked to compare apples to oranges. On the anti-regulation side, supporters of free information flow press utilitarian claims and apply cost-benefit analysis to evaluate the merits of alternative privacy proposals. They judge proposed regulatory solutions by comparing the costs of protecting personal data—such as added security, Web site restructuring, and lost efficiency from restrictions on information trading—to the purported

4. Congressional debates in the 1960s led to the passage of the Privacy Act, which governs the collection and sharing of information by federal government agencies. *See* 5 U.S.C. § 552(a) (2001). Congress expressly rejected calls for a parallel regime in the private sector at that time. *See* THE REPORT OF THE PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 32 (1977).

5. *See* U.S. COMM. ON GOV. OPERATIONS, PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE, AND DISCLOSURE OF INFORMATION, S. REP. NO. 93-1183, at 25 (1974).

6. James P. Nehf, *Recognizing the Societal Value in Information Privacy,* 78 WASH. L. REV. 1, 48-58 (2003).

7. *See, e.g.,* Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681(a)-1681(u); Cable Communications Policy Act of 1984 (CCPA), 47 U.S.C. § 551; Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2511-20; 2701-07; Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. § 1030; Video Privacy Protection Act of 1988 (VPAA), 18 U.S.C. § 2710(a)(4); Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d-2; Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506 (2001); The Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809.

benefits individuals would derive from protecting the data. This decision method generally works against robust privacy protection. Business interests have little trouble identifying and quantifying the costs of restricting data collection and sharing,[8] while privacy advocates can seldom identify and quantify the costs of data proliferation or the benefits of data protection. When policymakers use utilitarian decision-making models, privacy laws tend to be weak and, in the view of privacy advocates, ineffective.

Privacy advocates generally shun utilitarianism in favor of categorical or ontological arguments that invoke the rhetoric of fundamental rights, or at least rights that are universally recognized as important and worth protecting in civil society despite the high cost.[9] Loss of privacy is seen as loss of personal autonomy,[10] an affront to human dignity,[11] or an intrusion on one's "core self."[12] The arguments focus on the dehumanizing of an individual by the pervasive collection of personal information and seemingly uncontrolled access to that information. Protecting privacy is an important way of ensuring that individuals receive the respect they deserve, whether or not there is any quantifiable economic benefit that can be set off against efficiency losses or increased regulatory costs.[13]

When competing arguments do not address the same type of concern, even the best-intentioned policymakers will have difficulty comparing the relative strengths and weaknesses of competing proposals. The diversity of arguments also exposes the lack of consensus on whether and why privacy policy is being pursued and what outcomes constitute success. When no consensus emerges, policymakers do little or nothing and, for better or worse, market forces emerge as the de facto privacy regime.

---

8. Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 157, 169-71 (2002) (tabulating the costs of various privacy proposals but recognizing that valuing the benefits of privacy protection is extremely difficult).

9. "Kantian" is another label sometimes used to describe rights-based normative reasoning. *See* Timothy P. Terrell & Anne R. Jacobs, *Privacy Technology, and Terrorism:* Bartnicki, Kyllo, *and the Normative Struggle Behind Competing Claims to Solitude and Security*, 51 EMORY L.J. 1469, 1487 (2002).

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

11. *See generally* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2088, 2092-98 (2001) (connecting privacy to three distinct concepts: dignity, autonomy, and the creation of knowledge).

12. ALAN F. WESTIN, PRIVACY AND FREEDOM 32 (1967).

13. *See* Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 223 (Shoeman ed., 1982); Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2121 (2001).

In this Article, I examine the reasons for the passive approach to information privacy and discuss its virtues and vices. I contend that utilitarian arguments (those based on cost-benefit analysis in particular) should have a limited role in privacy debates and that policymakers should recognize the point at which such arguments have reached their useful limits. Rather than proposing an alternative normative theory supporting information privacy protection, I advocate an inductive approach that takes stock of lessons learned from the passive approach. Forty years of self-regulation supplemented by incremental, ad hoc privacy regulation have prepared fertile ground for exploration. Norms, preferences, and shared values are emerging. As more laws, standards, and policies about information privacy evolve, we will in time arrive at a consensus about our collective privacy preferences.

The Article has four parts. In the first part, I review several of the federal privacy laws in the United States that can materially affect information collection and sharing in the private sector. I conclude that these laws are driven largely by the idea that individuals can effectively value their privacy and then take steps to ensure that they receive a net benefit from the collection and sharing of their data. In the second part, I discuss several conditions of market failure that undermine the usefulness of this self-regulatory framework. In the third part, I argue that a cost-benefit approach to privacy policy fails to account for important aspects of the problem, primarily because we have difficulty determining the value of privacy rights and comparing them to competing values. As policymakers fail to recognize the basic incomparability of competing norms, suboptimal public policy resolutions will likely result. In the final part, I maintain that when policymakers reach the limits of a cost-benefit (or any other utilitarian) model, they need a different framework for deciding how to regulate information privacy in our society. I conclude that such a framework may be emerging in at least two areas of information policy: personal identity protection and the maintenance of personal health or medical records. The best course for policymakers as they address this relatively new problem may be to proceed inductively, recognize these and other emerging norms, and take appropriate measures to ensure their evolution in the future.

## I. FEDERAL PRIVACY LAWS AND INDIVIDUAL SELF-POLICING

In the United States today, the protection of information privacy in the non-governmental sector depends largely on businesses either to take voluntary measures or, in some sectors, to comply with legal mandates that include few enforceable restrictions on the use and misuse of data. This situation exists because privacy in the non-governmental sector has

been treated primarily as a commercial policy problem rather than one of ensuring fundamental individual rights or civil liberties. As a result, debates have often been framed as if privacy were a typical consumer protection issue, similar to product safety and price gouging, that pits business interests against consumer concerns. Emerging laws have done little to prevent or limit the collection of information in the first instance and the sharing of information thereafter. Their success has depended primarily on voluntary compliance by the business community. Individuals are expected to police their own interests and seek judicial remedies when legal norms are breached, much as they do when they bring suit for relief from the purchase of a defective automobile or a usurious loan.

This consumer-oriented approach had an early precedent in the Fair Credit Reporting Act ("FCRA"),[14] one of several federal consumer protection laws enacted in the late 1960s and early 1970s.[15] The FCRA regulates the collection and sharing of information in the credit reporting industry. The first national law regulating information privacy in the private sector, the FCRA established a model for future legislation. It placed no limits on the types of information that credit reporting agencies could collect and store in their databases, leaving private industry to decide what information is relevant and worth collecting.[16] While the FCRA did limit the reasons for which reporting companies could release information to persons who request it, the permitted uses were many,[17] decisions were left to the discretion of the reporting agencies, and consumers seldom knew when an unauthorized release had occurred.

---

14. 15 U.S.C. §§ 1681a–1681u (2002).

15. Notably, the FCRA was not enacted as a civil rights law but as a consumer protection statute amending the Consumer Credit Protection Act of 1968. The FCRA came into effect on April 24, 1971. *See* Statement of General Policy or Interpretation, 55 Fed. Reg. 18,804, 18,828 (Fed. Trade Comm'n May 4, 1990) (commentary on Fair Credit Reporting Act).

16. While there are no limits on the types of information that a consumer reporting agency can collect and store, there are limits on what it may *release* to a third-party inquirer. Those limits are minimal, however. The law bars the release of certain "stale" information (such as credit accounts more than seven years old and bankruptcies more than ten years old), but this older information can be released for credit or insurance transactions of $150,000 or more and employment positions paying $75,000 or more (figures that have not been adjusted recently). *See* 15 U.S.C. § 1681c(a) and (b).

17. See *id.* § 1681b(a)(3) (allowing release of a report to a person that the reporting agency has "reason to believe—(A) intends to use the information in connection with a credit transaction involving the consumer . . . (B) . . . for employment purposes . . . (C) . . . the underwriting of insurance . . . (D) eligibility for a license or other [governmental] benefit . . . (E) [evaluation of] an existing credit obligation; or (F) otherwise has a legitimate business need for the information (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an [existing] account . . . ."). In addition, medical information can only be disclosed under limited circumstances. *See id.* § 1681b(g) and *infra* text accompanying notes 226–29.

Although the FCRA has been amended several times,[18] to this day the law relies heavily on individuals to correct mistakes in their credit reports, ensure the continuing accuracy of their own records, and monitor the system in order to see that no unauthorized access has occurred.[19] Only in recent years—due in large part to increased access to credit reports on the Internet—have a significant number of consumers learned how to locate their credit reports, understand their contents, and take steps to ensure their accuracy and completeness.[20] Thirty years after the law's enactment, even with widespread Internet availability, most consumers know little about their rights under the FCRA and how they can protect those rights.[21]

Despite its deficiencies,[22] the self-policing scheme of the credit reporting system was not an irrational policy choice. The system is structured in a way that allows reasonably diligent individuals to discover inaccuracies in their credit reports. The statute requires a commercial user of a credit report (typically a lender, employer, or insurance company to whom the consumer has applied) to inform the consumer if the business took any "adverse action" (denial of credit or insurance, for example) in reliance on information in a consumer report.[23] The disclosure must identify the source of the credit report and tell the consumer that she has

---

18. The most recent FCRA amendment is the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159.

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

20. Commercial Web sites such as freecreditreport.com promote the dissemination of credit reports without charge, and for a fee they will also provide credit monitoring and other services. *See* http://www.freecreditreport.com (last visited Oct. 24, 2004). The major reporting companies also provide online access to consumer reports. *See, e.g.*, the Equifax Web site, at http://www.equifax.com (last visited Oct. 24, 2004).

21. NATIONAL CONSUMER LAW CENTER, FAIR CREDIT REPORTING ACT 74 (4th ed. 1998); Consumers Union, *Credit Bureau Nightmares: Victims Speak Out*, Sept. 29, 1997, *available at* http://www.consumersunion.org/finance/vict.htm (discussing and illustrating the difficulty of having mistakes removed from a credit report). Widespread ignorance about credit reporting rights fueled growth in the credit repair industry, which purports to help consumers fix errors in credit reports. Deceptive practices in the industry led Congress in 1996 to enact the Credit Repair Organizations Act, Pub. L. No. 104-208, 110 Stat. 3009-455 (1996) (codified at 15 U.S.C. § 1679 (2001)). Among other things, the act requires credit repair organizations to explain to consumers how they can assert their credit report rights by themselves. *See* 15 U.S.C. § 1679d (mandatory disclosure language).

22. Because of the burdens the FCRA places on consumers, the law has its share of critics. *See generally* the Electronic Privacy Information Center's Web site, *at* http://www.epic.org/privacy/fcra (last visited Oct. 24, 2004); Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1206-09 (1997).

23. 15 U.S.C. § 1681m. For example, if a consumer applies for a department store credit card and is denied, the store must inform the consumer that a credit report was used in making the decision, and it must give the reporting agency's contact information. By contacting the agency, the consumer can then find out what information is in the report.

a right to see her report at no charge and to correct any inaccuracies.[24] Thus, by following the law, an individual user of credit reports should learn when a report contains material mistakes. She can then trace the problem to the reporting agency that issued the report and request a copy. If she can convince the reporting agency that the report is inaccurate, the agency must correct it.[25]

In addition, consumers can periodically contact the reporting agency themselves and view their credit reports even if no adverse action has triggered their curiosity.[26] Upon reading the report, consumers can discover who has requested a copy within the past year and thereby have an opportunity to see if the reporting agency released the report to someone for unlawful purposes.[27] Although the FCRA has its weaknesses,[28] it is at least structured in a way that gives individuals a reasonable opportunity to learn about mistakes and unlawful disclosure so that they can then take steps to protect their rights. Privacy and accuracy are not entirely entrusted to the goodwill of the information keeper.

The structure of privacy laws enacted after the FCRA seldom gives individuals the opportunity to ensure compliance with legal mandates.

---

24. *Id.*

25. 15 U.S.C. § 1681i. As a practical matter, to ensure accuracy the individual must do a bit more. She must request copies of her reports from the other major reporting companies and, if those reports also contain errors, insist that corrections be made. (For years, there were three major reporting companies—Equifax, Experian, and TransUnion—but Innovis has emerged as a fourth popular database.) *See* Michelle Singletary, *The Color of Money*, WASH. POST, Feb. 29, 2004, at F01. After correcting the information in each database, the consumer must monitor the situation for several months to make sure that the erroneous information does not reappear in any of the four reports. Recent amendments to the FCRA may help consumers with this task. Consumers can now dispute the accuracy of information directly with the entity that furnished it. If the information is indeed wrong, the furnisher must report the correction to any reporting agency to whom it had given the erroneous information, and it is prohibited from reinserting the erroneous information thereafter. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 312.

26. Until recently, credit reporting agencies could charge consumers a fee for their report unless they requested it following some adverse action by a user of the report. *See* 15 U.S.C. § 1681j(a). In 2003 Congress changed this rule and required agencies to issue one free report each year. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 212 (2003). A few states had already required credit reporting companies to provide free reports twice a year. *See, e.g.*, GA. CODE ANN. § 10-1-393(b)(29)(C) (2000).

27. 15 U.S.C. § 1681g(a)(3). The report must identify persons who procured a report within the past two years for employment inquiries and one year for all other inquiries. *See also supra* note 20.

28. Critics contend that the law seldom works in practice, as consumers have difficulty getting consumer reporting agencies to undertake meaningful investigations of alleged inaccuracies, and users of consumer reports have few incentives to ensure that completely accurate information gets into the system. *See, e.g., The Fair and Accurate Credit Transactions Act of 2003: Hearing on H.R. 2622 Before the House Comm. on Fin. Serv.*, 108th Cong. (2003) (Statement of Chris Hoofnagle, Deputy Counsel, Electronic Privacy Information Center), *available at* http://www.epic.org/privacy/fcra/2622testimony.html.

Nevertheless, the statutes enacted after 1970—the Cable Communications Policy Act, the Video Privacy Protection Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act—relied largely on a combination of disclosure and consumer self-policing as the primary control mechanisms.[29]

### *A. Cable Communications Policy Act*

The Cable Communications Policy Act of 1984 ("CCPA")[30] allows cable operators to collect personal information about subscribers, including viewing habits, provided that they obtain the subscribers' written or electronic consent in advance.[31] Consent can be accomplished in any number of ways, even in the standard cable agreement or by a click-through on the cable operator's Web site.[32] As cable services expand and more consumers use interactive technologies to order programming through cable and other delivery devices, vast amounts of sensitive and personally identifiable information can be stored.[33] Like the FCRA, the CCPA does not restrict the types of information that can be collected or require that the information be relevant to the customer-operator relationship. Unlike the FCRA, however, so long as the cable operator receives the subscriber's initial consent to collect information, the CCPA allows the operator to disclose that information to virtually anyone.[34]

Under the CCPA, customer consent is not even necessary for disclosures that fit within a broad exception for a "legitimate business activity."[35] The operator may collect and maintain personally identifiable information such as a customer's name, service address, billing address, telephone numbers, Social Security and driver's license numbers, premium service subscription information, demographic information, and customer complaints. The operator may then use this information for fi-

29. Ironically, the FCRA, which served as the model for self-regulation in subsequent privacy laws, was amended in 2003 to give federal agencies greater oversight authority to ensure the accuracy and integrity of credit reports. Federal banking regulators and the Federal Trade Commission will, for the first time, establish and maintain guidelines regarding the accuracy and integrity of information provided by data furnishers to credit reporting agencies. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 114.

30. 47 U.S.C. § 551.

31. *Id.* § 551(b).

32. *Id.* §§ 551(b), (c)(1) (both sections requiring "written or electronic consent" but not defining how consent may be obtained).

33. *See* U.S. Dept. of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (Oct. 1995), *available at* http://www.ntia.doc.gov/policy/privwhitepaper.txt.

34. 47 U.S.C § 551(c)(1).

35. *Id.* § 551(c)(2)(A).

nancial, tax, and accounting purposes, for rendering services such as billing and marketing, and for monitoring unauthorized reception of the cable signal. It may also disclose the information to third parties, including program guide distributors, Internet and other service providers, collection agencies, construction and installation contractors, and marketing companies.[36]

Another problem with the CCPA is that subscribers have no practical way of learning about a violation of the disclosure rules. Unlike the FCRA, where a reasonably savvy consumer might catch a privacy violation or detect a breach of law before much harm has occurred,[37] cable subscribers are unlikely to discover a privacy leak until the disclosure has caused an irreparable injury. There is no disclosure mechanism to bring subscribers into the system and invite them to monitor their data periodically. Subscribers must trust their cable operators to treat them fairly.[38]

### *B. Video Privacy Protection Act*

Congress enacted the Video Privacy Protection Act of 1988 ("VPPA")[39] after public release of Judge Robert Bork's video rental information during the controversial Senate confirmation hearings upon his nomination to the United States Supreme Court.[40] The VPPA prohibits video stores from disclosing information about the titles of videocassettes, DVDs, and similar devices rented or purchased unless the cus-

---

36. *See, e.g.*, CHARTER COMMUNICATIONS, INC., CHARTER CABLE TELEVISION AND INTERNET SERVICE PRIVACY STATEMENT, *available at* http://www.charter.com/site/rules.asp#privacy (last visited Oct. 24, 2004). Moreover, the USA PATRIOT Act, Pub. L. No. 107-56, §§ 209-212, 224, 115 Stat. 272, 283–85, 295 (2001), further reduced the privacy protections afforded to cable 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 personal information was disclosed to the government. 47 U.S.C. § 551(c)(2)(D), as amended by the USA PATRIOT Act, at § 211. The USA PATRIOT Act took those rights away from many cable subscribers.

37. Under the FCRA, consumers should receive an "adverse action" letter if a report contributed to a denial of credit, employment, or insurance, and can monitor their reports online. *See supra* notes 23-37 and accompanying text.

38. The CCPA does authorize strong civil penalties, which should dissuade cable operators from intentionally violating the law. *See* 47 U.S.C. § 551(f) (providing for actual, statutory—the greater of $100 a day or $1,000—and punitive damages).

39. 18 U.S.C. §§ 2710–11.

40. See Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1148 n.430 (2002); Francoise Gilbert & Brad Laybourne, *Privacy Issues for the Global Company*, *in* THE OUTSOURCING REVOLUTION: PROTECTING CRITICAL BUSINESS FUNCTIONS USING OUTSOURCING, ASP & WEB SERVICE AGREEMENTS 291, 300 n.4 (2002).

tomer has given prior written consent.[41] In part because of the publicity surrounding its enactment, the VPPA is one of the stronger privacy laws in the United States. With respect to consent, the VPPA is stronger than the CCPA because consent must be "informed, written consent . . . given at the time the disclosure is sought."[42] A customer's advance consent in the video rental agreement will not suffice. The VPPA also requires that video stores destroy rental records within one year after an account is terminated.[43]

The VPPA, nevertheless, has substantial weaknesses. Like the CCPA, it relies primarily on customer self-policing for enforcement. But unlike the FCRA, it offers no practical means by which a customer can learn about security breaches or unlawful disclosures. Even when a customer discovers a breach, effective remedies may be unavailable because to prevail in a VPPA claim, the plaintiff must show that the store made prohibited disclosures knowingly.[44] Proving knowing misconduct can be difficult because the statute is riddled with exceptions and expressly permits disclosure to marketing firms and anyone else if the disclosure is in the "ordinary course of business," all without advance consent or even notice to video store customers.[45]

### *C. Health Insurance Portability and Accountability Act*

In 1996, Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA"),[46] which called on the Department of Health

---

41. 18 U.S.C. § 2710(a)(4) (definition of "video service provider"). The law may not cover newer technologies for obtaining video, such as online downloading of video material. *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 167 (2000).

42. 18 U.S.C. § 2710(b)(2)(B).

43. *Id.* § 2710(e).

44. *Id.* §§ 2710(b)(1), 2710(c) (allowing recovery of actual damages, statutory damages in the amount of $2,500, punitive damages, and attorney's fees). The VPAA does not preempt state law, and several states have enacted laws providing greater protection of video records. *See* § 2710(f). Video rentals in Connecticut and Maryland, for example, are considered confidential and cannot be sold. *See* CONN. GEN. STAT. ANN. § 53-450 (West 2001); MD. CODE ANN., CRIM. § 3-907 (2002). California, Delaware, Iowa, Minnesota, New Hampshire, New York, and Rhode Island have also enacted video privacy laws. *See* CAL. CIV. CODE § 1799.3 (West 1998); DEL. CODE ANN. tit. 11, § 925 (2001); IOWA CODE ANN. § 727.11 (West 2003); MINN. STAT. ANN. § 325I.02 (West 2004); N.H. REV. STAT. ANN. § 351-A:1 (1995); N.Y. GEN. BUS. LAW §§ 670-675 (McKinney 1996); R.I. GEN. LAWS § 11-18-32 (2002). Michigan's law also protects records of book purchases and book borrowing. *See* MICH. COMP. LAWS ANN. § 445.1712 (West 2002).

45. *See* 18 U.S.C. §§ 2710 (b)(2)(D)(ii), 2710(b)(2)(E). "Ordinary course of business" is defined to mean debt collection activities, order fulfillment, request processing, and transfer of ownership. *See id.* § 2710(a)(2).

46. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191,

and Human Services ("HHS") to issue regulations dealing with the privacy of medical information.[47] Acknowledging the sensitivity of health-related information, the final HIPAA rules set a higher level of privacy protection than previous federal laws. They govern the use and dissemination of health information generally and apply to health plans, health care clearinghouses, and certain health care providers.

Under the congressional mandates, HHS promulgated a complex set of rules that, in most instances, requires covered entities to obtain consent before using or disclosing health information when they treat patients, process payments, or perform other health care activities. Unlike other privacy laws, the HIPAA rules include numerous provisions to safeguard patient medical records from unauthorized access.[48] Express patient consent is required for release of personal information in marketing, research, fundraising, and other activities, but no consent is needed when making disclosures to carry out treatment, payment, or health care operations or perform certain other functions specified under the privacy rule.[49] Several other provisions permit dissemination of patient information without consent, but only when personal identifying information has been removed.[50]

Like other privacy laws, the HIPAA rules rely extensively on individuals for enforcement, but they at least grant patients a number of specific rights to support their enforcement efforts. Under the HIPAA regime, patients have a right to access, inspect, and copy information held by covered entities,[51] a right to request an accounting of disclosures that have been made,[52] a right to receive a "notice of privacy practices" from doctors, hospitals, and others in the health care industry,[53] and a mechanism for complaining about privacy practices to HHS.[54]

In addition, the HIPAA rules place more substantive and procedural burdens on covered entities than any previous federal privacy law. Cov-

---

110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). The HHS rulemaking authority was codified at 42 U.S.C. § 1320d-2 (2001). Because of the act's complexity and the strong interests of various competing stakeholders, the HHS rules took years to finalize and did not come into effect until April 2003.

47. 45 C.F.R. § 164.104 (2002).

48. *See id.* § 164.506(a); § 164.508(a)(1). *See generally id.* § 164.506.

49. *Id.* § 164.508. A few categories of disclosures require that the individual be given an opportunity to agree or object to the disclosure—for example, to determine whether information should be included in a hospital directory or given to clergy. *Id.* § 164.510(a). Health care professionals may make some disclosures to friends and family who are involved in a patient's care if such disclosures are found to be in the patient's best interest. *Id.* § 164.510(b).

50. *Id.* § 164.514(b)(2)(i).

51. *Id.* § 164.524(a).

52. *Id.* § 164.528(a).

53. *Id.* § 164.520.

54. *Id.* § 164.530(d).

ered entities must limit use and disclosure of personal information to the minimum amount required to perform a task.[55] They must adopt procedures specifying what information may be viewed by different classes of employees and what information may be released in response to routine and non-routine inquiries from third parties.[56] They must also have written contracts with associated businesses that perform functions on their behalf, which could include law firms, accounting firms, accreditation organizations, and billing services.[57] Finally, to ensure compliance with all these standards, the rules impose detailed security measures on doctors, hospitals, and others who have access to personal health information.[58]

### *D. Gramm-Leach-Bliley Act*

The Gramm-Leach-Bliley Act of 1999 ("GLBA"),[59] which regulates information privacy in the financial services sector, is a far weaker privacy law than HIPAA. The GLBA imposes few limits on the collection and sharing of information by financial services companies. It sets no limits on the type of information that such companies can collect and store in the first instance. It does not limit banks, insurers, investment companies, and other financial services organizations that are affiliated with each other, through common ownership or otherwise, to share "nonpublic personal information."[60] Although affiliates must tell customers that they are sharing this information, individuals cannot block the sharing of this non-public information among affiliated institutions. Because large conglomerates of affiliated entities dominate the financial services industry, sharing of personal information without customer consent is routine.[61]

---

55. *Id.* § 164.514(d)(2).

56. *Id.* § 164.514(d)(3).

57. Agreements must stipulate that the associated business will safeguard the health information and will assist the covered entity in complying with its obligations under the law. *Id.* § 164.504(e)(2)-(3).

58. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, and 164).

59. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–09 (2002)).

60. 15 U.S.C. § 6802(a) (prohibiting disclosure to nonaffiliated third parties). *See also* 12 C.F.R. §§ 216.10(a), 216.7(a) (2003).

61. *See generally* Gregory T. Nojeim, *Financial Privacy*, 17 N.Y.L. SCH. J. HUM. RTS. 81 (2000) (explaining inadequacies of GLBA). The GLBA did not preempt states from enacting stronger privacy rules. *See* Individual Reference Servs. Group, Inc. v. Fed. Trade Comm'n, 145 F. Supp. 2d 6, 17-20 (D.D.C. 2001) (describing GLBA and summarizing legislative history of privacy issues). Privacy laws in Alaska, Connecticut, Illinois, Maryland, Vermont, and North Dakota took advantage of the GLBA invitation and attracted some national

Customers can opt out of the disclosure of certain "nonpublic personal information" that a financial institution wishes to share with nonaffiliated third parties.[62] To do so, however, individuals must take the initiative and read through the often lengthy privacy policies mailed by the financial institution to learn how to exercise their opt-out rights.[63] Unlike HIPAA, the GLBA does not require affirmative consent from the customer for any data collection and distribution to others. The default rule is to collect and share until the customer says otherwise. Even if the customer takes the initiative and exercises the limited opt-out rights, she must trust the financial services companies to honor her request and

---

attention by enacting stronger consumer privacy rights. *See* ALASKA STAT § 21.36.162 (2001); CONN. GEN. STAT. ANN. § 38A-4A (2001); 205 ILL. COMP. STAT. ANN. 5/48.1 (West 2000); MD. CODE ANN. INS. § 9-109(D)(1)-(2) (2002); VT. STAT. ANN. tit 8, § 10203 (2003); N.D. CENT. CODE § 26.1-02-27 (2002). More recently, California followed suit. California Information Privacy Act, ch. 241, Div. 1.2, 2003 Cal. Legis. Serv. 241 (West 2003) (codified at CAL. FIN. CODE § 4050-4060 (2004)). The California law creates a hybrid privacy system requiring express opt-in from consumers before institutions may share their information with nonaffiliated third parties, and an opt-out right for sharing among affiliates. (The bill contains an exception allowing affiliate sharing without consumer permission/notification—a "no-opt"—if four criteria regarding corporate structure and lines of business are met.) *See* California Information Privacy Act, CAL. FIN. CODE § 4053(c)(1)-(3). In comparison, GLBA requires opt-out for nonaffiliated party sharing and allows institutions to share information freely among affiliates. The federal government reacted to these state measures in 2003 by enacting the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 212 (2003), which preempts some aspects of these stricter state privacy laws. The California law recently survived a preemption challenge. Am. Bankers Ass'n v. Lockyer, 2004 U.S. Dist. LEXIS 12367 at *17 (E.D. Cal. June 30, 2004) (dismissing claim that 2003 FCRA amendments preempted California act). At least one court has upheld a state opt-in requirement against First Amendment challenges. *See* Am. Council of Life Insurers v. Vermont Dep't of Banking, No. 56-1-02, 2004 WL 578737 at 6–7 (Vt. Sup. Ct., Feb. 12, 2004).

62. 15 U.S.C. § 6802(b) (obligation to give consumers an opportunity to opt out). There are several exceptions to the opt-out right that permit information sharing over the consumer's objection. If a financial institution engages the services of a separate company, it may transfer personal information to that company by arguing that the information is necessary to the services that the company will perform. Financial institutions can also transfer information to a marketing or sales company to sell new products or jointly offered products (such as co-sponsored credit cards). Once this unaffiliated third party has the personal information, it may share it with its own affiliated companies. *See id.* § 6802(b)(2).

63. *See Am. Council of Life Insurers*, at 6 (noting difficulty in locating and understanding opt-out language in insurance disclosure forms), 2004 WL 578737. Acting Comptroller of the Currency Julie Williams concluded, "Most bank customers can't ever recall seeing something like this . . . . [A]ffiliate-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." Julie L. Williams, Acting Comptroller of the Currency, Remarks Before the Banking Roundtable Lawyers Council (May 8, 1998), *available at* http://www.occ.treas.gov/ftp/release/98%2D50a.txt. *See also* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1087-88 (1999). In contrast to the GLBA, the recently enacted privacy law in California requires an easy-to-read form accompanied by a self-addressed envelope for the consumer to mail back to the financial institution. *See* CAL. FIN. CODE § 4053 (West 2004).

maintain adequate security procedures to prevent unauthorized sharing and access. The law imposes some security procedures on covered entities,[64] but they are not nearly as restrictive as the procedures established in the HIPAA rule. Because customer rights to access records, check for mistakes, and detect unauthorized disclosures are minimal, compliance with the GLBA is largely voluntary.

### *E. Children's Online Privacy Protection Act*

The Children's Online Privacy Protection Act of 1998 ("COPPA"),[65] the first federal law to specifically address Internet privacy concerns, was prompted by a Federal Trade Commission ("FTC") study that found widespread invasion of privacy on Web sites directed at children.[66] If a Web site is aimed at children under age thirteen, the site must post a privacy policy stating the ways in which it collects and shares information.[67] The law does not impose substantive limits on the types of information that sites can collect and share, but before collecting "personal information"[68] about children a site must obtain "verifiable" parental consent.[69] The statute does not mandate any particular method of obtaining parental consent, but the FTC gives site operators several options.[70] COPPA is limited in its practical effects because it applies only to sites that are specifically "directed to children" or where the operator has "actual knowledge" that it is collecting information from chil-

---

64. *See* 18 U.S.C. § 6802(a), (c), (d).

65. 15 U.S.C. § 6501. For the FTC's COPPA regulations, see 34 C.F.R. § 312 (2000). *See generally* Laurel Jamtgaard, *Big Bird Meets Big Brother: A Look at the Children's Online Protection Act*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 385 (2000).

66. In 1998, the FTC concluded that self-regulation was not working to protect the privacy of children online. FED.TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf. Among 212 American commercial Web sites aimed primarily at children aged 15 and under, 186 (88 percent) collected personal identifying information, and 188 (89 percent) collected personal information. *Id.* 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. A more recent FTC study concluded that since the enactment of COPPA, privacy protections for children on the Internet had substantially improved. *See* FED. TRADE COMM'N, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE 1 (Apr. 2002), *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf.

67. 15 U.S.C. § 6502(b)(1).

68. Personal information is defined to include children's first and last names, home addresses, e-mail addresses, telephone numbers, Social Security numbers, or any other personal identifiers of the child or the child's parents. *Id.* § 6501(8).

69. *Id.* § 6501(9).

70. An operator can supply consent forms to be signed and mailed or faxed to the operator, require a parent to use a credit card, have a parent call a toll-free number, or accept an e-mail accompanied by a digital signature. *See* 16 C.F.R. § 312.5(b).

dren under thirteen.[71] Moreover, it is primarily a disclosure law that mandates the posting of privacy policies on Internet sites within its reach and, like the other privacy laws, relies on individual (parent) monitoring for its success. It also contains a number of important exceptions.[72]

### *F. Gaps in the Ad Hoc Array of Privacy Laws and the Electronic Communications Privacy Act*

Each of these sector-specific laws has had some effect on the collection and sharing of information within its scope. With the exception of health information under HIPAA, however, those effects have been marginal. More important, there are substantial gaps in this ad hoc array of privacy laws. The collection and disclosure of information on the Internet is virtually unregulated for industries not covered by the laws discussed above. Most businesses now collect some information online or offline. Many voluntarily publish privacy policies,[73] but there is no law requiring privacy policies or prescribing their content. Consequently, privacy policies can offer little or no privacy protection, and if a privacy policy is breached the individual has little practical recourse. It is usually difficult to show economic injury from a breach. While violation may be an unfair or deceptive practice under the Federal Trade Commission Act,[74] in most circumstances the FTC will obtain only injunctive remedies.[75] For some violations there may be a private remedy under state

---

71. 15 U.S.C. § 6502(a). COPPA also applies to sites directed at general audiences if portions of the site are directed primarily at children. *Id.* § 6501(10)(A)(ii).

72. *See id.* §§ 6502(b)(2)(A)–(E). *See also* FED. TRADE COMM'N, HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE 3 (November 1999), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (operators may obtain a child's e-mail address without getting parental consent in advance when (1) "an operator collects a child's or parent's email address to provide notice and seek consent"; (2) "an operator collects an e-mail address to respond to a *one-time* request from a child and then deletes it"; (3) "an operator collects an e-mail address to respond *more than once to a specific* request—say, for a subscription to a newsletter. In this case, the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child"; (4) "an operator collects a child's name or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must notify the parent and give him or her the opportunity to prevent further use of the information"; or (5) "an operator collects a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.")

73. States have begun to enact laws requiring commercial Web sites to publish privacy policies if they collect personal information from Web users. *See, e.g.*, CAL. BUS. & PROF. CODE § 22575 (West 2004). Unless the laws are uniform, however, Web site operators may have difficulty complying with varying requirements of state disclosure laws.

74. 15 U.S.C. § 45(a).

75. The FTC has settled several cases alleging breaches of privacy policies in the past two years, with defendants agreeing to injunctive relief in each case. *See* FED. TRADE

deceptive-practices statutes, but many require proof of actual injury, prohibit class actions, or place significant procedural obstacles in the way of consumer redress.[76]

Thus, despite years of debate, collection of information about an adult's Web surfing, e-mail, and chat-room communications remains largely unregulated. In 1986, Congress updated laws that authorize wiretapping, eavesdropping, and clandestine surveillance in the Electronic Communications Privacy Act ("ECPA").[77] The ECPA extended wiretap protections to the interception of electronic forms of communication, including cellular phones, e-mail, and computer transmissions,[78] and held out promise as a restriction on data mining on the Internet. The law prohibits only intentional data intercepts, however,[79] and exempts situations in which one party to the communication consents to the interception.[80] Consequently, the law has not curbed privacy invasion via cookie technology, Web bugs, clickstream data recovery, and other surreptitious data collection activities.[81] Even the limited protection of the ECPA is in jeopardy in the aftermath of the September 11 attacks. Under the USA

---

COMM'N, ENFORCING PRIVACY PROMISES: ENFORCEMENT, *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Oct. 24, 2004).

76. *See generally* JONATHAN SHELDON & CAROLYN L. CARTER, UNFAIR AND DECEPTIVE ACTS AND PRACTICES 550-70 (5th ed. 2001) (discussing preconditions to suit under state unfair trade practices statutes).

77. 18 U.S.C. §§ 2511–20, 2701–07. A related federal statute is the Computer Fraud and Abuse Act of 1986 (CFAA). *Id.* § 1030. The CFAA prohibits persons from obtaining access to a computer without authorization ("hacking"). In *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001), the 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. *See also* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001). Although litigation on the scope of the CFAA continues, the $5,000 minimum damage threshold significantly limits the usefulness of the law. Some courts have held that damages under the CFAA may be aggregated in a class action, but only with respect to a single act of wrongful conduct. *See* In re Pharmatrak, Inc. Privacy Litig., 292 F.Supp.2d 263, 266 (D.Mass. 2002). Other courts have denied aggregation of claims altogether. *See, e.g.*, Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 680 (E.D. Tex. 2001).

78. Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 COMMLAW CONSPECTUS 63, 66-67 (1995).

79. 18 U.S.C. § 2511(1)(a).

80. *Id.* § 2511(2)d).

81. For a variety of reasons, most courts have held that the ECPA is not violated by the use of cookies, Web bugs, and similar data-mining tools. *See* In re Pharmatrak Privacy Litig., 292 F.Supp.2d at 266 (failure to establish criminal or tortious intent); In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d at 526; 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) (refusing to dismiss claim that 18 U.S.C. § 2701 (Stored Communications Act) was violated by defendant accessing data contained in cookies it placed in plaintiffs' electronic storage, but dismissing claim under ECPA because plaintiffs failed to show that defendants intercepted messages for purpose of committing tortious or criminal act).

PATRIOT Act[82] and Homeland Security Act,[83] various government personnel can now monitor e-mail and other electronic communications more rigorously and share information more freely.[84]

Data collection and monitoring in another important part of our lives—the workplace—are also largely unregulated. No federal law and few state laws limit a private-sector employer's right to gather and compile personal information about employees, even if the information is unrelated to the job they do.[85] Employers can listen to phone calls, read e-mail,[86] maintain voice-mail records, monitor computer screens, install software that tracks employee keystrokes, and check employee credit reports.[87] The ECPA could restrict the intentional interception of electronic communications in the workplace, but the exemptions for consensual access and business necessity render the law largely ineffective as a deter-

---

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

83. Homeland Security Act of 2002, Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2156-59 (codified at 18 U.S.C. § 2703(e) (2001)). The Homeland Security Act amends the USA PATRIOT Act and lowers the threshold for authorizing Internet service providers to divulge information to government inquirers. The information must be disclosed if the agency has "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

84. *See* Abraham McLaughlin, *CIA Expands Its Watchful Eye to the U.S.*, CHRISTIAN SCIENCE MONITOR, Dec. 17, 2001, at 2 (explaining how USA PATRIOT Act expands authority of law enforcement agencies to share information).

85. *See* ROSEN, *supra* note 41, at 159-63. In 2001, the American Management Association found that 62.8 percent of surveyed employers monitor the Internet connections of their employees and 46.5 percent store and review e-mail. Several Fortune 500 companies said they routinely analyze employee Web surfing and electronic communications to detect inappropriate uses. *See* MARCIA S. SMITH, INTERNET PRIVACY: OVERVIEW AND PENDING LEGISLATION 7-8 (2003), *available at* http://www.epic.org/privacy/internet/RL31408.pdf. Some states have limited workplace surveillance. *See, e.g.*, CONN. GEN. STAT. § 31-48b(b) (prohibiting "electronic surveillance device or system" in workplace).

86. *See* Smyth v. Pillsbury Co., 914 F.Supp. 97, 101 (E.D. Pa. 1996) (not tortious for employer to read employee e-mail). For more on e-mail monitoring, see Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communications to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. LEGIS. 393 (1997); Kevin P. Kopp, *Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861 (1998).

87. *See* AM. MGM'T ASS'N, 2001 AMA SURVEY, WORKPLACE MONITORING AND SURVEILLANCE, POLICIES AND PRACTICES, *available at* http://www.amanet.org/research/pdfs/emsfu_short.pdf (last visited Oct. 26, 2004); 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 (2001); 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.").

rent to employee monitoring.[88] Many employers maintain that employee monitoring is necessary to ensure compliance with office procedures and laws prohibiting sex, race, and disability discrimination.[89] It has also become customary for employers to disclose monitoring practices in employment manuals and other communications with workers, thereby obtaining express or implied consent to eavesdropping, tracking, and other forms of information gathering as well as insulating themselves from potential ECPA liability.[90]

## II. CONDITIONS OF MARKET FAILURE

The legislative choice to protect information privacy primarily through individual self-policing was not entirely irrational.[91] In theory, well-informed individuals and businesses will balance the value of collecting personal information against the value of keeping the information private and within the person's control.[92] Indeed, there are market in-

88. Surveillance tools include "packet-sniffing" software that intercepts and records communications on a network; "keystroke loggers" that capture every key pressed on a computer keyboard; automatic phone monitoring; video surveillance, particularly in rest areas, changing rooms, and public access areas; and "smart ID cards" that track employee movements throughout the day. ELEC. PRIVACY INFO. CTR., WORKPLACE PRIVACY, *available at* http://www.epic.org/privacy/workplace (last visited Oct. 26, 2004). *See also* Fraser v. Nationwide Mut. Ins.., 352 F.3d 107, 113 (3d Cir. 2003) (ECPA not violated when employer read employee e-mails because communications were not "intercepted" in transit as required by act).

89. *See* Corey A. Ciocchetti, *Monitoring Employee E-mail: Efficient Workplaces v. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26, ¶ 4 (2001) (listing reasons why employers monitor employee e-mail usage).

90. *See* GAO, NO. GAO 02-717, EMPLOYEE PRIVACY: COMPUTER USE MONITORING PRACTICES AND POLICIES OF SELECTED COMPANIES 9-12 (Sept. 27, 2002) (describing how companies have developed comprehensive computer use policies and informed their employees), *available at* http://www.gao.gov/new.items/d02717.pdf.

91. The self-regulation lobby has had little difficulty getting its message across. One of the strongest proponents is the Direct Marketing Association ("DMA"), the main trade association for businesses engaged in telemarketing, Internet, and e-mail soliciting, direct mailing, and other forms of marketing goods and services directly to individuals. The DMA maintains a set of Guidelines for Ethical Business Practices that includes a "privacy promise" to consumers. *See* DIRECT MARKETING ASS'N, PRIVACY PROMISE MEMBER COMPLIANCE GUIDE (2003), *available at* http://www.the-dma.org/privacy/privacypromise.shtml. *See generally* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996). The Online Privacy Alliance, a group of multinational corporations and trade associations, also maintains that the enforcement of existing laws by state governments and the federal government, combined with widespread use of privacy policies and trust mark programs, creates "adequate" safeguards for the protection of personal information collected online. *See* ONLINE PRIVACY ALLIANCE, GUIDELINES FOR ONLINE PRIVACY POLICIES, *available at* http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited Oct. 24, 2004). Another free-market proponent is the libertarian organization Privacilla. *See generally* http://www.privacilla.org (last visited Oct. 24, 2004).

92. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for In-*

centives on both sides. Many businesses will collect a minimum amount of customer data and keep it secure in order to avoid negative publicity or to obtain a market advantage by attracting customers from competitors whose data collection and sharing policies are less protective.[93] Many individuals are concerned about identity theft[94] or the embarrassing release of private facts, and they take steps to limit the release of their personal information and monitor its use after release.[95]

The market incentives are weak, however, and the conditions of market failure are strong.[96] There are several reasons why market forces yield a suboptimal privacy regime.

---

*formation Privacy*, 53 STAN. L. REV. 1393, 1447 (2001).

93. In 2000, the FTC praised private sector initiatives to develop self-regulatory regimes but concluded that industry measures were far from adequate and that national privacy legislation was needed. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Oct. 27, 2004). By the end of 2001, however, new leadership at the FTC had retreated from this position and instead called for more rigorous enforcement of existing laws. *See* Fed. Trade Comm'n Chairman Timothy J. Muris, Protecting Consumer's Privacy: 2002 and Beyond, Address before the Privacy 2001 Conference (Oct. 4, 2001), *at* http://www.ftc.gov/speeches/muris/privisp1002.htm; *see also* Timothy J. Muris, Challenges Facing the Federal Trade Commission, Address before the Committee on Energy and Commerce (Nov. 7, 2001), *available at* http://energycommerce.house.gov/107/hearings/11072001Hearing403/Muris678print.htm.

94. *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).

95. Market mechanisms have worked in several noteworthy instances. In June 2003, after protests and adverse publicity instigated by privacy watchdog groups, the retail giant Wal-Mart deferred plans to install radio frequency identification ("RFID") tags on its merchandise and set up receivers at various locations throughout its stores. The RFID sensors not only would track inventory items, but they could not be easily removed or deactivated by consumers even after purchase, thereby creating the possibility that the minitransmitters could track people's shopping patterns and movements wherever they went, long after the sale. *See* Heather Green, *Sensor Revolution: Bugging the World*, BUS. WEEK, Aug. 25, 2003, at 100–01. Wal-Mart has modified its plans in response to consumer privacy concerns but expects to implement the RFID system by the end of 2005. *See* Barnaby J. Feder, *Wal-Mart Hits Snags in Push to Use Radio Tags to Track Goods*, N.Y. TIMES, March 29, 2004, at C4. IBM announced in 1999 that it would pull advertising from any Web site that did not post a privacy policy within ninety days. The announcement was a response to the FTC's call for industry self-regulation of Internet privacy. Jon G. Auerbach, *To Get IBM Ad, Sites Must Post Privacy Policies*, WALL ST. J., March 31, 1999, at B1. One of the most publicized privacy breaches affecting law schools occurred in 1996 when Lexis-Nexis announced a 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 people. After much adverse publicity, the company changed its plans. Kim Bartel Sheehan & Mariea Grubbs Hoy, *Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns*, 28 J. ADVERTISING 37, 40 (1999).

96. Market failure in this sense means that in the absence of government intervention, market participants do not pay for all the harms they cause society by collecting and sharing personal information about individuals. As a result, they compromise privacy interests more

### *A. Lack of Transparency Creates Information Asymmetries*

The operations of the data collection and sharing industry are becoming less and less transparent. The days when individuals filled out survey forms and application cards by hand and businesses stored the information in filing cabinets are long gone. Most data collection is automated, and sharing practices occur outside public view. Individuals have little knowledge about the information being collected and the manner in which it is used or shared. Except in the rare instance when a privacy breach comes to someone's attention, people will never learn about harms resulting from information collection and misuse.[97] As data-mining technologies become more sophisticated, more and more collection and sharing activity will go unnoticed, because it is usually not in the data collector's interest to inform its subjects about the vast amount of information being mined, stored, and distributed. If people are only vaguely aware of a data-sharing activity, they cannot evaluate the extent of any potential injury, and it is difficult for them to take protective measures or to stop the activity from recurring.[98]

Despite the opacity of the data collection industry, individuals do sometimes detect privacy breaches and complain about them. Privacy watchdog groups and the press occasionally expose business plans that outrage the public. Northwest Airlines made headlines early in 2004 when it admitted sharing passenger information with the federal government as part of an ongoing airport security project.[99] Several years ago, DoubleClick was forced to abandon a marketing plan that would have merged data collected online with consumer residence information from

---

than is socially optimal. *See* DENNIS W. CARLTON & JEFFREY M. PERLOFF, MODERN INDUSTRIAL ORGANIZATION 115 (2d ed. 1994).

97. *See* Adam S. Marlin, *Online Identity Theft a Growing Concern*, CNN.COM, Aug. 16, 2000 (describing how an identity thief obtained a doctor's personal information from the Medical Board of California and used it to buy $185,000 of medical supplies on his credit), *available at* http://www.cnn.com/2000/TECH/computing/08/16/id.theft.offline.idg; PRIVACY RIGHTS CLEARINGHOUSE, IDENTITY THEFT VICTIMS' STORIES, LEGISLATIVE TESTIMONY OF JOHN AND JANE DOE (1999), *at* http://www.privacyrights.org/cases/victim5.htm (1999) ("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."); Amy Jo Sutterluety, Identity Theft Resource Center, *The Silent Encroachment on Our Privacy: One Woman's Search for Her Stolen Identity*, *at* http://www.idtheftcenter.org/html/silent.htm (2000) (discussing how identity thieves impersonated a woman).

98. Hahn & Layne-Farrar, *supra* note 8, at 103.

99. Sara Kehaulani Goo, *Northwest Airlines Faces Privacy Suits*, WASH. POST, Jan. 22, 2004, at A12. Northwest shared three months' worth of passenger information with the National Aeronautics and Space Administration for a research project on passenger screening and airport security. *Id.*

a database it had acquired, a combination that would have allowed for more narrowly targeted advertising to consumers.[100] These well-publicized events may suggest that market forces effectively limit data collection and sharing, but they simply highlight the fundamental problem. The noteworthy exceptions illustrate why many consumers are suspicious of the data collection industry and doubt that data collectors can be trusted to keep information to themselves. Eyes open wide when such stories hit the news: information asymmetries are exposed and people wonder how many similar activities go unnoticed.

### *B. Aggregation and Easy Transfer of Data Make Valuation Impossible*

A system that relies on individuals to police their privacy rights presumes that individuals can value privacy rights meaningfully. If people do not know what information is being collected, how it could be used, and what harm might result from its collection and use, they have no way of judging how much it is worth (in time, effort, or money) to keep the information private. To make an informed choice about whether and how to share information, and whether to take the time or spend the money to protect it, people need to know what is at stake. Because it is impossible to know where personal information will end up and how it will be used and combined with other data, it is difficult to assess the risks associated with releasing information or failing to monitor its use after its release.

Even a person acting diligently and breaking through the veil of opacity in the data collection world will seldom be in a position to acquire enough information to value information accurately. A user might, for example, take time to read a Web site's privacy policy and notice that the site shares data only with affiliated companies. She might decide to use the site because the risks seem relatively low. She might feel that she is revealing only a few simple, innocent facts (name, postal and e-mail addresses), or she might presume that any affiliated companies are so few that the risk is small compared to the benefits provided. Both these assumptions could be completely wrong. Merely because she visited that particular Web site, her location information identifies her as a person interested in that subject matter. Affiliated companies could be

100. Bad press caused DoubleClick to abandon the marketing plan shortly after it was announced. Pressure from the FTC also contributed to the change in plans. *See* Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, Federal Trade Commission, to Christine Varney, Hogan & Hartson, Attorney for DoubleClick, Inc. (Jan. 22, 2001), *available at* http://www.ftc.gov/os/closings/staff/doubleclick.pdf.

numerous and involved in entirely different lines of business, each with its own bits of information about her. Learning their identity and business practices is highly impracticable. When users lack the information necessary to evaluate the risk, they can easily undervalue the requested data submission. Collectors of information might know what they intend to do with the data, but individuals who provide the data do not.[101]

Valuation is further complicated when the data collector itself does not know how the information might be aggregated with other data in the future, either for its own purposes or for use by third parties. Even if asked, the data collector cannot provide enough information to give the individual a meaningful choice. Grocery store discount cards ("convenience cards"), for example, are a rare instance in which individuals actually get paid for releasing information, so the practice provides some evidence of how people value information about their purchasing habits. Under a "willingness to pay" valuation approach, a person's shopping list is worth the amount of store discounts that the shopper is willing to accept in trade by using a store convenience card. Yet to value the information in a meaningful way, the shopper needs to know what other information might be added to the database and how the aggregate will then be used by the store owner, whether any other businesses (affiliated or not) will gain access to the data, and if so, what information they will add and how they will use the aggregate. If the store itself does not know how the data might ultimately be aggregated, transferred, reaggregated, and used, it cannot provide an inquisitive shopper with the information she needs. The store might sell the shopping list to a marketing firm along with thousands of other shoppers' lists without any name identification, in which case the shopper might value its release nominally. If the store (or a subsequent purchaser of the information) combines the list with name, address, and Social Security number and then sells it to an insurance trade association, the shopper would likely value it much higher.

Accurate valuation of personal information is practically impossible. We place a great amount of trust in data collectors not to take actions that will harm us. Once information is stored in digital form and capable of being combined with other data, we lose control over its use. Because electronic data can be bought and sold almost instantaneously, we can never know where the information will end up. It is difficult enough to value information when we know about a single user's intended purpose. It is impossible to value when the ultimate destination, aggregation, and use of the information are unknowable.

---

101. *See* HAL R.VARIAN, MICROECONOMIC ANALYSIS 440 (3d ed. 1992).

### *C. Signaling Mechanisms Are Not Yet Effective*

Information asymmetries and data aggregation problems might be ameliorated by shortcuts or signaling mechanisms that supplement an individual's deficient personal knowledge. Evolving signaling mechanisms can assist people in evaluating the privacy practices of many businesses. Voluntary "trust marks"[102] and similar shorthand indicators of privacy standards can signal good privacy practices and thereby help market mechanisms work better. Signaling comes in many forms. Brand names can signal quality of consumer products and services. I might not know much about global positioning systems, but when I see one displaying a Delphi trademark I might associate it with a particular standard of performance if I have had previous experience with the company or know it by reputation. Price can also be a quality signal because higher price usually means better quality. Certification by a competent authority ("USDA Grade A") can also signal important characteristics that help us value things.[103]

Some signals are better than others, however, and in the world of information privacy the current signals are poor. Generally speaking, the most accurate signals are supported by the experience of the person relying on them as proxies for information. A brand name is not a useful signal to someone who has no experience with the brand. Certification can be a poor signal unless the certifying agency is competent and reliable. Effective signaling in the information industry requires us to have experience with the trustworthiness of the privacy signal. This has yet to happen, and without mandatory rules it seems unlikely to happen any time soon.

In theory, privacy seals or trust marks could help individuals gain some confidence in the privacy practices of the businesses they use and the Web sites they visit. Marks could signal which businesses have strong privacy policies and adhere to those policies. They could indicate, for example, that a business collects a minimum amount of information, uses it only for the express purposes stated in the original request, safeguards it against all outside access, and steadfastly refuses to transfer the

---

102. A trustmark program requires a business or Web site licensee to abide by a code of information practices and submit to compliance monitoring in order to display a program's privacy mark. *See* OFFICE OF THE INFO. AND PRIVACY COMM'R/ONTARIO & OFFICE OF THE FED. PRIVACY COMM'R OF AUSTL., WEB SEALS: A REVIEW OF ONLINE PRIVACY PROGRAMS, *available at* http://www.privacy.gov.au/publications/seals.html#2 (last visited Oct. 24, 2004); Rapheal Franz, *Privacy Standards for Web Sites: Web Seals*, INTERNET L.J. (Feb. 5, 2001), *available at* http://www.tilj.com/content/ecomarticle02050103.htm.

103. *See, e.g.*, U.S. DEP'T OF AGRIC., UNITED STATES STANDARDS FOR GRADES OF BUTTER 2 (1989), available at http://www.ams.usda.gov/standards/Butter.pdf.

information to any other entity. At present, however, the scope of trust mark assurance is much narrower than this. The most popular marks, at best, ensure only that the business clearly and accurately discloses a privacy policy, and that the mark issuer has no knowledge that the business is not following its policy as stated. Issuers do not require that subscribers limit or reduce the amount of information they collect, or dictate how collected information can be shared and with whom.[104] Nor do mark issuers perform regular and rigorous audits of their clients to ensure that the mark's standards are being honored.[105]

Because trust marks do not serve as signals of strong privacy protection, they do not yet solve the valuation and aggregation problems that face individuals who wish to police their privacy rights and protect their interests. At most, the marks ensure that privacy policies are disclosed, but they do not make the data collection and sharing industry significantly more transparent. Consumers have no basis for preferring one trust mark over another or a business that participates in a trust mark program over one that does not. Consumers may have a general idea that less collecting and sharing of information is better, but they will not get this information by noting a trust mark on a Web site or company privacy policy.

Trust marks also do little to address the transparency problem. At first glance, they appear to convey useful information about a Web site's privacy practices with an easily recognized symbol. In fact, however, trust marks can disserve the Web site's users by signaling misleading information. All things being equal, a privacy-conscious consumer might prefer a business that participates in a trust mark program over one that does not, so the mark serves a useful, albeit limited, signaling function. But in the data collection industry, things are seldom equal. The consumer has to decide if the added benefits of a non-marking business are worth the risk of giving information to that business. Placing a value on

104. *See* TRUSTE , TRUSTE PROGRAM REQUIREMENTS, *available at* http://www.truste.org/requirements.php (last visited Nov. 15, 2004). To be certified by TRUSTe, the privacy policy need only disclose what personally identifiable information (PII) is collected and how it will be used; the identity of the party collecting PII; whether PII is shared with third parties; the use of any tracking technology; whether PII is supplemented with information from other sources; choice options available to consumers (including a right to opt out of sharing PII with third parties); how consumers can access PII they have provided; that there are security measures in place; and procedures for filing and addressing consumer complaints. *See id. See also* R. Ken Pippin, *Consumer Privacy on the Internet: It's Surfer Beware,* 47 A.F.L. REV. 125, 132 (1999). Joel R. Reidenberg, *E-Commerce and Transatlantic Privacy,* 38 HOUSTON L. REV. 717, 727-28 (2001); John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?,* 39 ALBERTA L. REV. 346, 348-49 (2001) (explaining that TRUSTe, BBBOnline, WebTrust and other seal programs do not require compliance with OECD privacy guidelines).

105. *See* MacDonnell, *supra* note 104, at 392; Smith, *supra* note 85, at 3.

that risk remains problematic, whether or not a mark is displayed. A non-marking business might not collect or share any information at all, whereas a trust mark subscriber might collect data and sell information with impunity. Unless a consumer knows what the mark means and takes the time to read the privacy policy, the mark can give the wrong signal about the company's use of information.

There is reason to doubt that adequate signaling will ever emerge. At present, market incentives do not push trust mark licensors to impose rigorous privacy policies on their licensees. While a licensor will insist on a minimally acceptable privacy standard to make its mark appear to have value, insistence on rigorous standards is likely to drive away licensees who prefer laxer standards. What people need is a signal for determining whether a trust mark itself is a meaningful signal.[106] Without mandatory privacy standards to ensure that a mark is worth something—for example, minimum requirements for displaying a privacy "seal of approval"—signals will remain ineffective bridges of the information gap.

### *D. Technological Solutions Have Minimal Effect*

Concerns about data collection and sharing are frequently met with assurances that the problem is temporary and emerging technologies will address legitimate concerns.[107] Technology promises increased privacy protection, but only when it can be brought into the data collection activity and only to the extent that it can be used effectively. Except for telephone and Internet communications, individuals seldom can use technology to disguise identity or limit the amount of information transferred. When a person is working at an office desk, conducting a banking or insurance transaction in person, or purchasing videos with a credit card at a bookstore, information-blocking technologies are not available.

---

106. One solution, advanced by Colin Bennett, would allow businesses to qualify for certification in one of three tiers: (1) conformity of privacy "policy"; (2) conformity of privacy "procedure"; and (3) conformity of privacy "practice." Only an organization seeking certification in the third tier (the strongest privacy protection policy) would undergo a complete privacy audit to ensure that it honors representations of fair information practices. *See* COLIN J. BENNETT, PROSPECTS FOR AN INTERNATIONAL STANDARD FOR THE PROTECTION OF PERSONAL INFORMATION: A REPORT TO THE STANDARDS COUNCIL OF CANADA (Aug. 1997), *available at* http://web.uvic.ca/polisci/bennett/research/iso.htm.

107. *See* DISSENTING STATEMENT OF COMM'R ORSON SWINDLE, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ONLINE ENVIRONMENT, at 17, 19, 20 (2000) (arguing that the development P3P—platform for privacy preferences—made Internet privacy legislation less desirable), *available at* http://www.ftc.gov/reports/privacy2000/swindledissent.pdf.

For Internet use, computer users can install products that allow for anonymous Web surfing. Firewalls and freeware such as Ad-aware[108] can defend against spyware and some forms of data mining. More complex software can automatically negotiate a user's privacy preferences with Internet sites, assuming that the sites are willing and able to negotiate with the user's computer.[109] Products such as Anonymizer[110] permit users to retain anonymity while Web surfing,[111] and several programs allow Web browsers to display privacy warnings and block cookies.[112]

If technology is to become an effective control mechanism against privacy invasion on the Internet, one of two things must happen. First, Internet users may in time be capable of selecting and working with the required technology.[113] While this transformation may occur, it seems unlikely. Without legal impediments, the data collection industry will surely develop increasingly sophisticated methods of data mining, and the technology required to defend against it will have to keep pace with equal or greater sophistication. Imposing such a burden on Internet users is unrealistic. Second, a universal and mandatory privacy software standard could be developed. To succeed, it would have to be compatible with most Internet sites, personal computers, servers, and interfacing hardware and software, relatively easy for ordinary consumers to use, and readily updated so that data seekers would continue to find it difficult to evade. Creating such a universal standard seems both politically

108. *See* PCWORLD.COM, PRODUCT GUIDES: AD-AWARE V6.181, *available at* http://www.pcworld.com/downloads/file_description/0,fid,7423,00.asp (last visited Oct. 24, 2004).

109. Lawrence Lessig calls this service an "electronic butler." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999). Seeking to force data miners to pay for information about Web browsing behavior, a company called Lumeria offered to block transmission of subscribers' data to Web sites they visit and then sell the subscribers' data in anonymous form to marketers, paying royalties to its clients. *See The Coming Backlash in Privacy*, ECONOMIST, Dec. 9, 2000, at 5.

110. *See* Anonymizer Online Privacy and Security, *at* http://www.anonymizer.com (last visited Oct. 28, 2004). The Electronic Privacy Information Center maintains a list of privacy enhancement tools, with links for downloading. *See* ELECTRONIC PRIVACY INFORMATION CENTER, EPIC ONLINE GUIDE TO PRACTICAL PRIVACY TOOLS (2003), *available at* http://www.epic.org/privacy/tools.html.

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

112. WORLD WIDE WEB CONSORTIUM, THE PLATFORM FOR PRIVACY PREFERENCES 1.0 (P3P1.0) SPECIFICATION, W3C RECOMMENDATION (2002), *at* http://www.w3.org/TR/P3P.

113. *Exposure in Cyberspace*, WALL ST. J., Mar. 21, 2001, at B1 (posting survey showing that almost 30 percent of computer users did not know about cookies and almost 40 percent had no idea how to deactivate them).

and technologically infeasible at present. If mandated by government, it might face constitutional challenges as well.[114]

For the time being, economic incentives in the Internet world and beyond produce technologies that enhance data collection and sharing more than they restrict it.[115] Because personal information is perceived as a valuable commodity, technological developments continually increase data collection and decrease our ability to impede the process. This makes privacy protection even more difficult for people who might be interested in curbing data collection practices by policing their information in the marketplace.[116]

### *E. Accountability Problems Insulate Privacy Violators from Exposure*

Without accountability, market forces cannot effectively curb harmful behavior. For individuals to protect their privacy interests, they must be able to identify the culprit who broke a law, breached a voluntarily adopted privacy policy, or allowed access to a database because of lax security procedures. For the system to work, businesses that collect data must fear that they will be exposed and held accountable if they do something wrong. Without adequate deterrents to inhibit the unlawful collection and sharing of information, the self-policing system breaks down.

There are two fundamental accountability problems. First, individuals seldom know when a privacy breach has occurred. For consumer rights in other contexts, it is often more obvious that a wrong has occurred. When a product does not function as expected, or when a service provider does shoddy work, the injured person sees the consequences. This seldom happens with breaches of information privacy. The vast majority of data collecting—lawful and unlawful—occurs outside public view.[117] Individuals do not know when information collection and shar-

---

114. *See* Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1052 (2000).

115. Joel R. Reidenberg, Oversight Hearing on Privacy and Electronic Commerce Before the House Subcomm. on Courts and Intellectual Property, *House Comm. on the Judiciary* (May 18, 2000).

116. Joel R. Reidenberg, *E-Commerce and Transatlantic Privacy*, 38 HOUSTON L. REV. 717, 723 (2001). *See* John Hanchette, *New Microsoft Software Raises Privacy Protection Concerns*, INDIANAPOLIS STAR, Aug. 26, 2001, at D1 (describing Microsoft's plans to combine personal identification information with a powerful information distribution network).

117. Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 63, 64-66 (Philip E. Agre & Marc Rothenberg eds., 1997).

ing has affected them for good or for bad. If a breach of privacy norms results in media exposure, identity theft, or some other cognizable injury, the affected person may learn about it in due course. Less obvious breaches remain hidden for long periods, possibly forever.

Second, when an injury or breach is detected, individuals may find it impossible to trace the problem to a particular cause or source. For some privacy breaches, the source will be readily identifiable. If a university mistakenly puts students' Social Security numbers on the Internet or allows a hacker to gain access to the system, students know that the university is the source.[118] But with personal information residing in countless databases, often there will be no way to locate the entity that caused a particular problem, sold the data, or permitted the hack or leak that ultimately caused the injury. Even with an obvious injury such as identity theft, it may be impossible to learn how the thief obtained the personal information. The thief might have taken Social Security numbers from a university database, driver's license numbers from a convenience store scanner,[119] addresses from an insurance company, or credit card numbers from the marketing affiliate of a credit card issuer. Tracing the injury to the point of origin will often be difficult or impossible.

## III. THE LIMITS OF THE UTILITARIAN MODEL AS A TOOL FOR EVALUATING PRIVACY POLICY

We are burdened with self-policing our privacy interests because legislators have often taken a utilitarian approach to evaluating competing policies in privacy debates. This has inhibited the creation of more restrictive privacy policy in the non-governmental sector. Legislative processes involve the interplay of competing interests. The focus of privacy debates has centered on whose particular interests would be jeopardized by limiting information collection and sharing and whether jeopardizing those interests is, on balance, good for society. Privacy advocates are continually asked to show how a particular data collection or sharing activity invades privacy and, if it does, to convince lawmakers

118. *See supra* notes 96 and 101.

119. Business scanning of driver's licenses has become increasingly common, usually for verification of age, as when someone wants to buy beer at a liquor store. When a scan occurs, information from the license can be stored in a database and, unless prohibited by law, used for other purposes. Depending on the state of issuance, the data can include a person's name, address, date of birth, height, weight, sex, eye color, hair color, Social Security number, organ donor status, medical indicators, alias names, electronic image of signature, digital fingerprints, and even a facial recognition template. *See* Jennifer S. Lee, *Welcome to the Database Lounge*, N.Y. TIMES, Mar. 21, 2002, at G1. *See generally* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595, 627 (2004).

that protecting the privacy interest is not outweighed by the interests of others in gaining access to the information in question.[120]

Privacy advocates have not acquitted themselves well. With few exceptions, they have not persuaded policymakers that the benefits of strong privacy protection outweigh the costs. One possible conclusion to draw from this failure is that the benefits of more privacy protection might not be as great as proponents believe. If the benefits of privacy protection were real and significant, or if the consumer costs of data proliferation were very high, people would demand more privacy and would pressure businesses (in the market) and legislators (in the state house) to satisfy their concerns. Moreover, if benefits and costs are so difficult to quantify, then perhaps they simply do not exist, or at least the adverse effects created by gaps in current privacy laws are greatly exaggerated. It is possible that except for a small enclave of privacy advocates, people just do not care enough about the problem, and their indifference is perfectly rational because the stakes are low.

The counterresponse, however, is to question whether the task put to privacy advocates is the right one. The choice of utilitarian reasoning—often reduced to cost-benefit analysis ("CBA") in policy debates[121]—fixes the outcome in favor of the side that can more easily quantify results. In privacy debates, this generally favors the side arguing for more data collection and sharing. Although CBA can mean different things in various contexts, the term here means a strategy for making choices in which quantifiable weights are given to competing alternatives.[122] The most common CBA methodology is the "willingness to pay" approach, which involves numerical weighting and ranking of individual preferences based on how much individuals would pay to obtain a particular benefit or avoid a particular risk.[123] Cost-benefit analysis is thus most frequently used to show policymakers which available option is likely to produce the largest net measure of good consequences for society, under

120. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 174–75 (1995).

121. Although CBA is not necessarily an expression of utilitarianism (the aim of which is to maximize social utility) or consequentialism (the right way to assess alternatives is to look at the consequences they produce), it is often associated with those moral philosophies and is used to support conclusions anchored in them. *See* Robert H. Frank, *Why Is Cost-Benefit Analysis So Controversial?*, 29 J. LEG. STUD. 913, 915 (2000); Steven Kelman, *Cost-Benefit Analysis: An Ethical Critique,* REG. Jan.-Feb. 1981, at 33; Martha C. Nussbaum, *The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis,* 29 J. LEG. STUDIES 1005, 1028-29 (2000).

122. *See* Nussbaum, *supra* note 121, at 1028. LESTER B. LAVE, THE STRATEGY OF SOCIAL REGULATION: DECISION FRAMEWORKS FOR POLICY 17-25 (1981) (discussing CBA in monetized and other forms).

123. Nussbaum, *supra* note 121, at 1028.

the assumption that the winner of that contest is the preferred alternative.[124]

In the context of privacy policy, market solutions and CBA assume that personal information is a property right or commodity that can be bought and sold like any other. The discussion below demonstrates how this assumption ignores other generally recognized principles for allocating rights and liberties. Only by deemphasizing the commodity aspects of information privacy and focusing on other values in keeping information private can a different analytical framework emerge.[125] Many people would say, for example, that they value the dignity and autonomy that come from knowing that their data are reasonably secure and are not being bought and sold without permission or for purposes they do not approve. People feel less vulnerable knowing that their data either are not being collected or at least are protected from misuse after being collected. For many in our society, these perceptions are worth respecting in their own right, whether or not they can be quantified in a way that exceeds the economic costs they impose on those who want to collect and share the information for their own purposes. Cost-benefit analysis is difficult to defend as a method for attaining a moral and just outcome in the privacy context because it does not account adequately for important privacy values.[126]

As a practical matter,[127] two basic conditions limit the usefulness of CBA as a methodology for making any public policy decision. First, the costs of a policy change are more easily quantified than its benefits. Second, and more important, comparing costs and benefits is hugely problematic when diverse societal interests are involved. Difficulties with both quantification and comparability have an impact on the debate over information privacy.

---

124. This method of evaluating options that involve winners and losers is one variant of the Kaldor-Hicks criterion. It involves two steps: (1) every affected person's gain or loss is measured by the maximum amount he or she would pay to receive the gain or avoid the loss, and (2) one option ranks higher than the other if the total amount that the winners would be willing to pay exceeds the amount that the losers would demand. *See* Nicholas Kaldor, *Welfare Propositions of Economics and Interpersonal Comparisons of Utility*, 49 ECON. J. 549, 549-50 (1939); J.R. Hicks, *The Foundations of Welfare Economics*, 49 ECON. J. 696 (1939).

125. One of the standard critiques of CBA is that it treats risks to societal values as commodities. *See* Lewis A. Kornhauser, *On Justifying Cost-Benefit Analysis*, 29 J. LEG. STUD. 1037, 1045 (2000).

126. *See* Mathew Adler, *Incommensurability and Cost-Benefit Analysis*, 146 U. PA. L. REV. 1371, 1373-75 (1998) (reviewing criticism of CBA as a criterion for moral rightness).

127. My position is that CBA does not work well in practice as a decision procedure in privacy analysis, not that it is normatively deficient in a theoretical sense. For a general discussion of the weakness of CBA as a normative legal philosophy, see Jules L. Coleman, *Efficiency, Utility and Wealth Maximization*, *in* MARKETS, MORALS AND THE LAW 95 (1988); Ronald M. Dworkin, *Is Wealth a Value?*, 9 J. LEGAL STUD. 191 (1980).

### *A. The Benefits of Privacy Protection Are Difficult to Quantify*

As a general principle, the costs of a policy change are easier to quantify than the benefits of the change.[128] Stakeholders are keenly aware of their current costs and can usually predict with some degree of confidence how the change will affect them. Benefits of the change are usually more speculative. An automobile manufacturer, for example, can quantify how a change in toxic emission controls will increase production cost, but the societal benefits of the change are more speculative. This is particularly true with information privacy. Due in large part to the valuation problems discussed above,[129] there is little consensus on how to measure the benefits of increased privacy protection or the societal costs of more data proliferation. One of the most comprehensive cost-benefit reports on information privacy in the private sector included much data on the costs of increased privacy protection but concluded that to be "truly balanced" it would have also included figures on the consumer benefits of increased privacy protection.[130] The authors acknowledged that "putting real numbers to heterogeneous individuals' valuations for privacy is a difficult task."[131] Policy decisions therefore tend to be driven by cost considerations (the best available quantification), and in privacy debates this leads to a bias in favor of the status quo. In the world of data collection and sharing, the status quo means few barriers imposed by law. If CBA is the chosen analytical model and the benefits of change do not demonstrably outweigh the asserted costs, then policymakers are inclined to leave things as they are.[132]

This is not to say that CBA is irrelevant in public policy debates on information privacy. Cost-benefit analysis is indispensable, inevitable, and useful for bringing to the attention of policymakers important facts that might, for political reasons or by simple oversight, otherwise escape attention.[133] It can also assist us when there is some doubt about where

---

128. *See* Robert H. Frank, *Why Is Cost-Benefit Analysis So Controversial?*, 29 J. LEG. STUD. 913, 928 (2000).

129. *See supra* text accompanying notes 97-118.

130. Hahn & Layne-Farrar, *supra* note 8, at 157.

131. *Id.*

132. This recalls the story of Buridian's ass, who saw two haystacks but could not decide which one was the best. The ass, being a strict optimizer, chose neither (because neither was clearly the best) and starved to death. *See* Amartya Sen, *The Discipline of Cost-Benefit Analysis*, 29 J. LEG. STUD. 931, 940-41 (2000).

133. *See* Cass Sunstein, *Cognition and Cost-Benefit Analysis*, 29 J. LEG. STUD. 1059, 1060 (2000). In its early use, CBA was encouraged and sometimes mandated in government decision making as a strategy for limiting the role of politics in the creation of public investment policy. *See* THEODORE M. PORTER, TRUST IN NUMBERS: THE PURSUIT OF OBJECTIVITY IN SCIENCE AND PUBLIC LIFE 189 (1995).

to set a threshold level of basic entitlement. Seeing the cost of various levels of protection is helpful in avoiding absurdly utopian decisions that can cause great harm or, for political reasons, have no chance of success.[134] We live in a world of scarce resources, and we understand that all rights impose societal costs. We must therefore keep costs in mind when determining the appropriate levels of privacy protection. It is important to ask how much it would cost financial institutions if we required them to obtain express consent from customers before sharing personal information among affiliated companies. We should not, however, base information privacy decisions solely upon CBA or require defenders of a privacy right to support their position with CBA evidence that outweighs evidence about regulatory costs.

We should openly acknowledge that non-economic values are legitimate in privacy debates, just as they have been recognized in other areas of fundamental importance. Decisions about the societal acceptance of disabled citizens, the codification of collective bargaining rights for workers, and the adoption of fair trial procedures for the accused did not depend entirely, or even primarily, on CBA outcomes. Difficulties in quantifying costs and benefits do not present insurmountable obstacles when policymakers address matters of basic human dignity. The protection of personal data should be viewed in a similar way, and CBA should play a smaller role in privacy debates.

### *B. Cost-Benefit Analysis Works Poorly with Diverse and Incomparable Societal Interests*

In the context of privacy debates, the quantification problem is not simply that our measuring tools are inadequate for the task. When considering privacy policy alternatives, we are faced with a fundamental incomparability among competing options.[135] Comparing disparate cate-

134. Nussbaum, *supra* note 121, at 1035.

135. Philosophers distinguish between incommensurability and incomparability, although the words sometimes are used interchangeably and there are no standard definitions. *See* Adler, *supra* note 126, at 1385. If things are commensurable, they can be cardinally ranked precisely in terms of the same unit at some point along a single scale, continuum, or metric. Comparability means that alternatives can be ordinally ranked (ordered) but not necessarily cardinally ranked. If two things are comparable, one alternative can be better than the other without a determination of precisely how much better in terms of a common unit (such as money) or precisely where the two rest on the metric. *See* Ruth Chang, *Introduction* to INCOMMENSURABILITY, INCOMPARABILITY, AND PRACTICAL REASON 2 (Ruth Chang ed., 1997). Incomparability is most often used when discussing the ordering of options or alternatives and deciding which one is preferred; incommensurability is used to discuss other relationships (values, goods, reasons, life plans). *See* Matthew Adler, *Law and Incommensurability Introduction*, 146 U. PA. L. REV. 1169, 1170-71 (1998). For law and policy, where decisions often are reduced to which option or alternative is preferred, comparability is the

gories of benefits and injuries is extremely difficult in any circumstance, and in privacy debates the categories vary widely. What is the value of knowing that the details of one's life are not open to public view or of knowing the societal cost of database stereotyping and profiling? How can one compare it to the value of that information to a bank, hospital, or marketing firm? When policymakers are asked to compare the two, how can they rationalize a decision favoring one or the other?

Incomparability is a common phenomenon in everyday life. When two things cannot be aligned on a single metric or scale, we say that they are incomparable.[136] For example, there is no single scale on which to compare an afternoon of work at my office desk with a round of golf at the local club with my wife.[137] I might expect to derive pleasure from each activity, but if I chose a scale comparing degrees of pleasure alone, I would miss important parts of the calculus. The round of golf costs time and money but may be more fun than work, and work at the office may be productive monetarily and professionally and enjoyable in other ways. How do I decide if the benefits of recreation exceed the costs of obtaining it?

Two things are comparable only when they can be compared by reference to some definite and shared value, so that any non-measurable differences are not significant.[138] Apples and oranges are hard to compare if we do not identify a shared value that can be used as a basis for the comparison. If the chosen value is prevention of scurvy, oranges are better. If the value is suitability as a pie filling, apples probably win. If, in the golf example, the chosen or "covering" value[139] is wealth accumulation, we can compare each alternative along a wealth accumulation scale, and the time at work will likely be preferred to the golf game. If the covering value is family harmony, then golfing with my wife may win out. Every choice is governed by some value, and the value chosen for

---

more relevant idea. *Id.* at 1176.

136. Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 MICH. L. REV. 779, 796 (1994). Joseph Raz describes the related idea of incommensurability: two things are incommensurable if we cannot say that either one is better than the other; nor can we say that they are of equal value. JOSEPH RAZ, THE MORALITY OF FREEDOM 322, 328 (1986). If values are incommensurable, they also lack the property of transitivity: A is neither better nor worse than B. A* is better than A. But A* is also neither better nor worse than B. For example, a person might think that lunch with a friend is neither better nor worse than a $50 gift. A $60 gift is better than a $50 gift, but the person has no clear preference between lunch with a friend and a $60 gift either. *See also* MARGARET JANE RADIN, CONTESTED COMMODITIES 115-22 (1996).

137. *See* Sunstein, *supra* note 136 at 798.

138. John Finnis, *Commensuration and Public Reason*, in INCOMMENSURABILITY, INCOMPARABILITY, AND PRACTICAL REASON 215, 218-19 (Ruth Chang ed., 1997).

139. Chang, *supra* note 135, at 7. Cheese and chalk are incomparable until we assign a covering value. Cheese is better than chalk as a housewarming gift. If we cannot find a value that covers both items, then comparability fails. *Id.* at 29.

the comparison helps justify the decision. The choice between seemingly incomparable things becomes easier once a covering value is identified, and a shift in covering values can make the decision clearer or the outcome different.[140] Thus, when making difficult decisions in our everyday lives, we often struggle over which covering value to prefer.

A similar phenomenon is at work in the formulation of public policy. Policymakers are often asked to compare incomparable alternatives. Should we enjoy the economic and security benefits of oil drilling in Alaska or the beauty and ecological purity of a pristine wilderness? Our most intense public debates reveal disagreements over the appropriate covering value to be pursued. Less often, they involve arguments over the particular amount of a chosen value (once agreed upon) that is assigned to the competing choices.[141] Environmentalists may value wilderness in a fundamentally different way than economists do. They may pursue preservation not as a means to ensure that future generations will have adequate oil supplies (which might be reduced to a common value in economic terms) but out of a sense of awe and wonder inspired by the unspoiled area.[142] People who refuse to trade environmental quality for monetary or security benefits are often making a claim about the way the environment should be valued[143]—that environmental quality is somehow more important and more valuable than money and security.[144] The debate is really about which value should be pursued. Once that decision is made, the comparison is much easier and the preferred choice becomes clear.

Cost-benefit analysis, as a normative tool, assumes that there is a single covering value or metric along which things should be com-

140. *Id.* at 7-8.

141. *Id.* at 9.

142. *See* Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 MICH. L. REV. 779, 792 (1994). Positive theories of environmental regulation often try to assess issues by referring to people's preferences for environmental quality along the same metric—utility or willingness to pay. B. Peter Pashigan, *Environmental Regulation: Whose Self-Interests Are Being Protected?*, *in* CHICAGO STUD. IN POL. ECON. 489, 529 (George J. Stigler ed., 1988).

143. Trade-offs can be made rationally when we can compute the value of alternative things on a common scale, roughly enough to justify a decision. If, however, choosing one requires an uncalculated loss of the other because it is valued differently, then the decision either lacks a rational basis or we need to justify it on other grounds. Thus, in John Stuart Mill's discussion of "higher pleasures," fundamental rights cannot be traded off against utilitarian concerns because they are essentially priceless. Steven Lukes, *Comparing the Incomparable: Trade-Offs and Sacrifices*, in INCOMMENSURABILITY, INCOMPARABILITY, AND PRACTICAL REASON 184, 188 (Ruth Chang ed., 1997). *See* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY, at xi (1977) (some individual rights should not be set aside for any instrumental value).

144. *See* Sunstein, *supra* note 142, at 836-37.

pared.[145] Economists may be reluctant to impose a theory of value, but CBA, to be useful in practice, depends on comparing things along the same scale, so a covering value must be assigned.[146] For ease of application, the chosen scale is usually money or its equivalent. This often reduces to the willingness-to-pay model because it yields data that can be aligned on a single scale. The willingness-to-pay model measures relative preferences between a particular risk or benefit in reference to a constant value and thereby conveniently manages the incomparability problem.[147] In privacy debates, this has some intellectual appeal, as one side of the equation—the costs of increased privacy regulation—can often be stated in terms of money or its equivalent. If a Web site operator can no longer collect and share personal information with advertisers, it will lose revenue, operate less efficiently, or lose stock value. As a result, the site may either charge a fee for access to its content or restrict its content, for it can no longer afford to devote so many resources to development. Because these costs are real, it makes sense to ask how much individuals will benefit from the change. To make the comparison, we need to quantify those benefits in like monetary terms.

By converting all values to money, the incomparability problem is lessened,[148] but only if we accept the legitimacy of money as the covering value. In the privacy debate, the legitimacy of monetizing individual privacy preferences is highly suspect. Benefits are often personal, emotional, intangible, and not readily quantifiable. Preferences on privacy matters are generally muddled, incoherent, and ill-informed. If privacy preferences are real but not sufficiently coherent to form a sound basis for valuation,[149] any attempt to place a monetary value on them loses meaning. The choice of CBA as the model for justifying decisions fixes

145. *See id.* at 860-61.

146. John Broome, *Cost-Benefit Analysis and Population*, 29 J. LEGAL STUD. 953, 956 (2000).

147. Henry S. Richardson, *The Stupidity of the Cost-Benefit Standard*, 29 J. LEGAL STUD. 971, 972 (2000).

148. The comparability problem does not necessarily go away, however, simply because things are valued in the same way. Even if things can be assessed under the same covering value, they might still be incomparable. For example, two children may be incomparable even though a parent values each in the same way. We cannot say that the valuation of one is merely some fraction of the other. *See* Sunstein, *supra* note 142, at 799. Nor does it mean that a particular outcome is directed even if we can rank its value on a particular scale. We might agree, for example, that prostitution is wrong because it improperly values human sexuality, yet still oppose criminalization because we think that the coercive power of the state should be reserved for more serious wrongs or that the available remedies will not redress the wrong. *Id.* at 819. *Cf.* Adler, *supra* note 126, at 1409 (a rational decision might be based on "second order considerations" that countermand the option supported by another rational decision-making procedure).

149. Broome, *supra* note 146, at 958.

the end, because the chosen covering value will usually result in a decision favoring data proliferation over data protection. The point here is not that privacy and money are inherently incomparable,[150] but that the comparison is often meaningless. Valuing the costs and benefits of privacy protection or invasion is impossible—quite possibly in theory, and most definitely in practice.

Constructing plausible measures of costs and benefits for large and diverse segments of society is always difficult, and much of the work of modern-day economists involves finding ways to quantify and compare things that at first seem unquantifiable and incomparable. Analysts typically estimate costs and benefits either by drawing inferences from observed market behavior or by doing preference surveys, both of which can yield information about preference valuation.[151] Both these approaches are problematic, however, when weighing information privacy concerns. Inferences drawn from market behavior are most reliable as indicators of individual preferences when markets are working competitively and efficiently.[152] Strong conditions for failure in data collection markets, as discussed in Part II above, cast suspicion on conclusions drawn from individuals' behavior in those markets. With respect to surveys,[153] the difficulties that individuals have in assessing the risks of data collection and sharing, and in placing a value on these risks, undermine the usefulness of survey responses on the subject.[154] Without

150. *Cf.* Jason Scott Johnson, *Million Dollar Mountains: Prices, Sanctions, and the Legal Regulation of Collective Social and Environmental Goods*, 146 U. PA. L. REV. 1327, 1333-34 (1998). Johnson points out that incomparability examples often involve a purported exchange of something—such as time spent with a spouse—for money, an exchange that is socially or legally frowned upon. Johnson argues that such examples do not show that the two are inherently incomparable, but that people object to the monetization of the exchange as a behavioral or social construct. If those constructs were to change, Johnson notes, the comparability problem would go away.

151. Robert H. Frank, *Why Is Cost-Benefit Analysis So Controversial?*, 29 J. LEG. STUD. 913, 917 (2000).

152. *See* JAMES M. HENDERSON & RICHARD E. QUANDT, MICROECONOMIC THEORY: A MATHEMATICAL APPROACH 105 (2d ed. 1971). *See generally* ELIZABETH ANDERSON, VALUE IN ETHICS AND ECONOMICS (1993); JAMES GRIFFIN, WELL-BEING: ITS MEANING, MEASUREMENT, AND MORAL IMPORTANCE (1986).

153. Data for CBA often come from so-called contingent valuation surveys. People are asked hypothetically how much they would be willing to pay to see various contingencies happen. For survey methodology, see CAMERON MITCHELL & RICHARD T. CARSON, USING SURVEYS TO VALUE PUBLIC GOODS: THE CONTINGENT VALUATION METHOD (1989).

154. *See* Manoj Hastak et al., *The Role of Consumer Surveys in Public Policy Decision Making*, 20 J. PUB. POL'Y & MARKETING 170 (2001); George R. Milne & Andrew J. Rohm, *Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives*, 19 J. PUB. POL'Y & MARKETING 238 (2000) (using eight-page survey to determine privacy preferences regarding opting choices in mail, telephone, and Internet communications). *See generally* Amartya Sen, *Rationality and Social Choice*, 85 AM. ECON. REV. 1, 17 (1995) ("There are plenty of social choice problems in all this, but in analyzing

knowing how information might be used against a person's interests, how it might be aggregated with other data, and who might ultimately gain access to it, a survey respondent's answer to a valuation question is virtually meaningless. In addition, survey responses can be self-serving, especially when nothing real is at stake, a condition that further undermines the reliability of the data for making policy decisions.[155]

To some extent, these arguments merely illustrate two of the recognized limits of CBA. First, as a normative tool, CBA works only when costs and benefits can be quantified with some confidence.[156] Results are only as reliable as the data inputs; if either the cost or benefit side of the equation is wrongly assessed, the resulting conclusion is suspect. Second, CBA need not be normatively determinative.[157] It does not purport to tell us whether any of the available options would result in a denial of a basic right or benefit that individuals can legitimately demand regardless of its costs. Even if the calculations are perfect, CBA does not tell us which is the just result. The abolition of slavery is a standard example.[158] Slavery was wrong even if the benefits of freeing slaves might not have exceeded the costs imposed on the landed gentry and the Southern economy. While economic arguments on either side of the debate can be proffered, abolitionism was not wrong if it turns out that the cost-benefit evidence of abolitionists is less than persuasive. The same can be said for other entitlements. In standard CBA analysis, many citizens would probably demand only a small amount of money to give up their right to vote in a local election. Yet in our society all citizens have a fundamental right to vote as part of a package of basic entitlements, and no one would seriously argue that its value depends on how much money

---

them, we have to go beyond looking only for the best reflection of *given* individual preferences, or the most acceptable procedures for choices based on those preferences.").

155. Economists often observe that a person's answers to hypothetical questions are not necessarily reliable. *See* Richard Craswell, *Incommensurability, Welfare Economics, and the Law*, 146 U. PA. L. REV. 1419, 1429 (1998). For example, more than 90 percent of drivers think that they are above average in driving ability; 94 percent of college professors believe they are more productive than their colleagues. *See* Frank, *supra* note 121, at 929. Moreover, even if a person's answers do accurately reveal her preferences at that time, there is no reason to believe those preferences will remain constant or would be the same in other settings. Craswell, *supra* note 155, at 1428-29.

156. *See* John Finnis, *Commensuration and Public Reason*, in INCOMMENSURABILITY, INCOMPARABILITY, AND PRACTICAL REASON 215, 218-19 (Ruth Chang ed., 1997).

157. *See* Mathew Adler, *Incommensurability and Cost-Benefit Analysis*, 146 U. PA. L. REV. 1371, 1377-78 (1998) (explaining how CBA may be "morally significant" even when it is not "morally conclusive").

158. Another is Mahatma Gandhi's insistence on nonviolence irrespective of the consequences. *See* Amartya Sen, *The Discipline of Cost-Benefit Analysis*, 29 J. LEG. STUD. 931, 937 (2000).

people would accept in trade.[159] The right is something that one should not be expected to forgo merely because the voter would pay more for other things or because someone else values it more than the voter does.

Cost-benefit analysis, as a pragmatic tool, asks us to examine the costs and benefits of alternatives before making a decision, but it does not tell us which alternative we should choose. Nor does the use of CBA mean that the most efficient or cost-effective result is necessarily the right one. In privacy debates, however, CBA takes on a normative dimension because the goal of privacy policy in the non-governmental sector has been, broadly speaking, to enact laws that provide net benefits to individuals while imposing the lowest possible cost on the information-sharing industry. Because businesses have for decades viewed information as a valuable and tradable entitlement, those who attempt to restrict it are asked to justify the change by showing how society would thereby be improved. If CBA is used to determine which alternative will yield the greatest benefit at the lowest cost, then it becomes not just one of many available tools but the dominant methodology in setting policy on information privacy. When this happens, policymakers should be reminded of the incomparability problem and should limit the role of CBA. Rather than using CBA as the determinative decision method, they should recognize the incomparability problem and let CBA inform the debate but not end it.

## IV. MOVING BEYOND COST–BENEFIT ANALYSIS AND ADDRESSING THE INCOMPARABILITY PROBLEM

If in privacy debates we are often trying to compare fundamentally incomparable things, we can proceed down one of two paths. The first is pragmatic and institutional. Cost-benefit analysis, though a crude and imperfect legislative tool, may be better than any practical alternative. For purposes of developing public policy, it may make sense to act as if costs and benefits of competing alternatives are comparable even when we know they are not.[160] If the alternative is ad hoc decision making, CBA is less likely to result in a gross misallocation of resources.[161]

159. Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 MICH. L. REV. 779, 849 (1994).

160. *See* Adler, *supra* note 157, at 1407 ("CBA is, without more, neither better nor worse than any alternative decision procedure that determinately picks out an option that is incomparable from the option picked out by CBA.").

161. *See* Sunstein, *supra* note 136, at 842; Craswell, *supra* note 155, at 1459 (propounding, but then critiquing, the idea that when incomparable choices are at issue, a government decision can be justified on whatever choice emerges from the democratic process).

Cost-benefit analysis at least has a rational basis and may be better than less rational alternatives.

The second path is to identify and apply a different normative theory of privacy that helps us assess the validity of competing ideas. Since Congress began debating this issue forty years ago, there have been many attempts to develop a compelling theory of privacy entitlements.[162] We do not as yet, however, have a consensus about the importance of information privacy in the digital age or its status as a fundamental entitlement. The relative newness of the problem in its current form, its evolutionary nature, and the technological complexities affecting (and sometimes creating) various aspects of the surrounding issues make it difficult to construct a defensible normative theory of information privacy that adequately addresses the competing and incomparable values driving the debates. Moreover, the long-term effects (good and bad) of widespread data collection and manipulation are only beginning to show themselves. We may not yet know enough about the problem to proceed with much confidence that we are getting the theory right.

While we await the emergence of a normative theory of information privacy, policymakers must, of course, make choices. When they do, they frequently decide by reacting to evolving events and recent experience. Such decisions can be ad hoc and irrational, but they are not necessarily so merely because no normative theory of privacy entitlements supports them. An inductive approach to privacy law asks how our public and private institutions have begun to recognize privacy norms and attempts to extract a theory from the practice. Developing patterns may indicate that a moral theory of privacy rights is emerging—unnamed and unarticulated as yet, but real nonetheless. Indeed, we are beginning to see a set of generally accepted privacy principles coalesce. Seemingly incomparable values are being compared; decisions are being made in Congress and, more often, state legislatures. Identifying the patterns could provide a better understanding of how we actually value privacy than any theoretical model might suggest. Policymakers should be sensitive to these developments and adopt privacy rules that recognize and further emerging values.

---

162. Some of the more thought provoking treatments of privacy law and theory over the last twenty-five years include ROSEN, *supra* note 41; CHARLES J. SYKES, THE END OF PRIVACY (1999); PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS (1998); JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY (1997); FERDINAND DAVID SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1992); DAVID O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY (1979); and ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

### *A. "Notable" Values Trump Competing "Nominal" Values*

A crucial step in developing a moral theory of information privacy is to identify fundamental entitlements.[163] What ends should we seek when we strive for an ideal privacy policy? What interests are so important that they should be preserved even at great cost? These important questions are often missing from the information privacy debates—in part because our ends still tend to be vague, abstract, and conflicting. We understand that information in databases can be useful and beneficial, but we do not want information used in ways that will harm us, and we do not want it released to others who may use it for purposes we do not favor. Our sensibilities on this issue are conflicting and ambiguous, for the problem is relatively recent, at least with respect to the digital database.[164] We want to maximize the good and minimize the bad, but at present we do not know much about either.

We might study international human rights declarations, consider our constitutional heritage, or consult religious traditions and customs that help describe the fundamental entitlements of individuals in society. These sources guide us in determining public policy on important societal issues such as involuntary servitude, armed conflict, child labor, pornography, race and gender discrimination, and prisoners' rights. They may be less useful, however, in valuing our information privacy concerns. How important is it that banks not share with their affiliates a customer's Social Security number and employment history without the customer's informed consent? Shared views of fundamental human rights, constitutional traditions, or religious tenets may help steer our judgments on matters of major importance, but they are not likely to be much help in answering countless questions at the margin during periods of evolving sensibilities.[165]

---

163. *See* Richardson, *supra* note 147, at 984-85 (noting that a crucial step in rational decision making is to transform abstract goals (e.g., to be successful) into more concrete and specific ends (e.g., to be an Olympic figure skating champion); if ends are too vague, one cannot coherently devise a plan to achieve them).

164. *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy,* 78 WASH. L. REV 1, 2 (2003).

165. Privacy interests against government intrusion are rooted in the U.S. Constitution, particularly in the First Amendment protections of association, speech, and religion and the Fourth Amendment protection against unreasonable searches and seizures. The right to read anonymously, for example, is protected from government invasion. *See* Stanley v. Georgia, 394 U.S. 557, 565 (1969) (right to read obscene material in one's home); Lamont v. Postmaster General, 381 U.S. 301, 307 (1965) (striking down law that prohibited Post Office from delivering communist literature). Privacy rights of individuals in non-government relationships, however, are not firmly anchored in the federal Constitution. Some state constitutions recognize privacy rights in private sector relationships. *See, e.g.,* CAL. CONST. art. I, § 1; Semore v. Pool, 217 Cal. App. 3d 1087 (4th Dist. 1990) (drug testing).

Nevertheless, it may be that a normative theory of information privacy is beginning to emerge. One way to identify it is by looking at the relatively easy cases, situations that are not morally ambiguous. Sometimes people are asked to compare diverse values, one of which is clearly important while the other is trivial. When this happens, people make rational choices, feeling confident that they are correct even if they cannot give a reason or theory that justifies their choice. Decisions favoring "notable" privacy values have been preferred over competing "nominal" values, and we do not feel the need to identify a specific explanation of why this is right.[166] This may suggest that an unstated or second-level normative theory either exists or is developing, one which may become clearer in time as more notable/nominal decisions are made and more patterns emerge.

Despite the basic incomparability of competing values in everyday life, people have no trouble making decisions when it is clear, for whatever reason, which alternative is best. Even when the alternatives are valued differently, it is often possible to say that a very large amount of one is better than a small amount of the other. Suppose a person receives an unexpected $5,000 bequest and is debating whether to give the money to charity or invest it for retirement. We might say that the competing values—generosity and prudence—are equally valid and worthwhile.[167] A person might conclude that one choice is better with respect to generosity and one is better with respect to prudence, but there seems to be no covering value that has both generosity and prudence as parts, so the two cannot be compared on the same scale. The person could flip a coin or use some other irrational decision method. Alternatively, however, the choice may become clear if the person learns that a $5,000 donation will allow a deserving charity to remain solvent and a $5,000 investment will supplement the retirement fund by only a small percentage. Even the environmentalist who believes that wilderness and cash are incomparable may rationally allow degradation of a very small area in exchange for a large amount of money.[168] When people do this, they are deciding that it is better to further one value in a big way even as they diminish a competing incomparable value in a much smaller way.[169]

---

166. Chang, *supra* note 135, at 32.

167. *Id.* at 31.

168. Sunstein, *supra* note 136, at 803.

169. Chang, *supra* note 135, at 32. Notable/nominal examples suggest that perhaps differently valued things really are comparable in a theoretical, if not a practical, sense. Two things may exist on the same scale or metric, but if our tools for measuring their positions are not adequately refined, they appear incomparable. Ruth Chang gives the following example. We might say that Mozart and Michelangelo are incomparable because they were creative in very different ways. Yet suppose there is another painter, Talentlessi, who has only a nominal level

People make choices between seemingly incomparable things all the time, and they can do so rationally. A person is not acting irrationally by preferring a perceived notable value over an incomparable nominal value, even if she cannot state a normative theory to explain why the decision is right.[170] A similar phenomenon may be seen in the formulation of public policy. Notable values may be preferred over nominal ones in the enactment of laws and the implementation of policies even if policymakers cannot explain why one alternative is better than the other. Moreover, by observing a number of such decisions over time, we may begin to see a pattern develop and covering values emerge that can serve as guides to later decisions that are closer to the margin.

Now that information privacy has reached the digital age, we can identify at least two areas of concern in which notable/nominal decisions reveal important privacy entitlements. One is identity theft, more specifically the harms (mainly financial) that result from one's personal information being used to commit unauthorized or fraudulent acts. The other is the privacy of our personal medical history. In these two areas, legislatures (at the state level first, then the federal) have had little difficulty recognizing notable privacy interests and taking steps to protect them.

### *B. Comparing the Incomparable in Emerging Privacy Policy*

Like Alexander Bickel three decades earlier, Cass Sunstein has championed "incompletely theorized agreements" in reaching important public policy decisions.[171] Indeed, a consensus may gradually emerge precisely because the exact grounds for a decision are not made explicit. When this happens, decision makers leave the debate open to varying

---

of visual arts creativity compared to Michelangelo. We have no trouble saying that Michelangelo is more creative than as Talentlessi. Most people would also say that Mozart was clearly more creative than Talentlessi even though they were creative in different ways. If this is the case, it cannot be the diversity of creative values that accounts for incomparability. If we think of Talentlessi as at one end of a general creativity continuum and Michelangelo at the other, then if Mozart is comparable with Talentlessi, he is comparable with anyone else on the continuum. The source of our difficulty, therefore, is not that Mozart and Michelangelo are incomparable with respect to their creativity. The problem is that both are at the high end of the general creativity scale and our measuring tools are not refined enough to rank them. *Id.* at 14-15. Even if this is so, it does not solve the practical problem of comparing alternatives in the development of public policy. For practical purposes, it makes little difference if two alternatives are theoretically incomparable (incapable of being measured on the same scale) or are comparable but our measuring tools are inadequate to rank them. In either situation, a notable/nominal comparison may reveal a rational choice.

170. Sunstein, *supra* note 136, at 811.

171. *See generally* CASS R. SUNSTEIN, LEGAL REASONING AND POLITICAL CONFLICT (1996).

lines of argument and differing points of view. Decisions are made incrementally without any declaration of an overarching theory or universal standard.[172] With respect to privacy policy, Willis Ware similarly observed that we can probably never agree on what privacy is because it means such different things to different people.[173] For purposes of policy making, Ware argued, it is more important to develop a consensus on what we consider an "invasion" of privacy.[174] This back-end approach focuses on events and on societal reactions to those events. It also tracks and reflects usage of evolving technologies as society adapts to new intrusions and adjusts the boundaries of acceptable conduct, rather than *a priori* prescribing those boundaries.[175]

Sometimes we are not able to decide between two seemingly incomparable things simply because we do not yet have enough information. Through using inductive or experimental reasoning, experience may supply the information we need to make the better choice. At a personal level, for example, a student might have to choose between two roommates, one of whom is clever and funny but sloppy, the other tidy but boring.[176] Cleverness and cleanliness are vastly different values, so it may be impossible to compare the two potential roommates in the abstract. If the student has never lived with boring or sloppy people, she may have no basis for comparing the two choices. Through prior experience, however, the student may have learned that she can live with boring people reasonably well but sloppy people drive her mad. In light of this experience, the choice between the two incomparable roommates becomes clear.[177]

---

172. This is of course a hallmark of the common law as well. Courts usually decide cases by limiting the holding to the particular facts at issue, avoiding bold declarations or major shifts in doctrine, allowing the law to develop incrementally and reveal its nuances over time. *See, e.g.*, Szajna v. General Motors Corp., 503 N.E.2d 760 (1986) (declining to abrogate privity doctrine generally but deciding to apply manufacturer's warranty to buyer in the case at hand).

173. Willis A. Ware, *A Taxonomy for Privacy*, *in* REPORT ON THE NATIONAL SYMPOSIUM ON PERSONAL PRIVACY AND INFORMATION TECHNOLOGY 16 (1981). *See also* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 67-68 (1997) (one of the benefits of not embracing a general definition of privacy is that "we can better understand privacy by characterizing the contexts in which it arises or is invaded as a concern" (quoting FERDINAND SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1992))).

174. Defining a term by giving examples of its opposite is not uncommon in law. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 205, cmts. a and d (defining "good faith" performance of a contract through examples of "bad faith" performance).

175. Ware, *supra* note 173, at 4.

176. Elijah Millgram, *Incommensurability and Practical Reasoning*, *in* INCOMMENSURABILITY, INCOMPARABILITY, AND PRACTICAL REASON 151, 160 (Ruth Chang ed., 1997).

177. One way to reason inductively in formulating public policy is through analogies drawn from experience: What was the resolution of previously decided similar cases?

As policymakers consider privacy policy in the United States, what experience is most relevant as an inductive guide? One fertile source might be the experience of other nations or international law and custom.[178] Data proliferation is a worldwide phenomenon, and many nations have been struggling with similar public policy issues over the past twenty years. Common themes have emerged. Instead of beginning with a presumption of legitimacy for commercial exploitation of personal information, the privacy policies of many other nations—particularly in Europe—aspire to a higher level of data protection for all citizens.[179] Information policies tend to have broad applicability and cut across economic sectors.[180] There is an underlying presumption that the collection and sharing of personal information, particularly in the private sector, should not be commonplace. Information can be collected only for specified purposes, used in ways that are compatible with those purposes, and stored no longer than is necessary.[181] Individuals must be notified that information is being collected, apprised of the purposes of the data collection, and told the identity of the person responsible for collecting and controlling the information after it has been stored.[182] Affirmative consent is required in many situations when data is to be collected or shared, with less responsibility on the individual to opt out of data sharing.[183] Independent, national supervisory authorities oversee, investi-

---

Through this process, we seek consistency among various judgments. *See* Sunstein, *supra* note 136, at 858.

178. *See generally* PRIVACY & HUMAN RIGHTS 2003: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2003) (survey of privacy laws in fifty-five countries compiled by the Electronic Privacy Information Center).

179. *See* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L. J. 461, 469 (2000). Whether the higher aspirations of the European Union match reality remains to be seen. *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) ("Even though EU-based sites are obligated by law to give consumers the option to opt-out of a website's mailing list, they were less likely to have that option than U.S.-based sites.").

180. *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).

181. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 13-14 (1996).

182. *Id.* at 15.

183. 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, for example, mandates that the national laws of all member states protect information about each identifiable individual even if the data are publicly available. 1995 O.J. (L 281) 31 (1995) [hereinafter "EU Directive"]. National 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" (such as medical information) and certain "black list" data are not collectable at all without the affirmative consent of the indi-

gate, and enforce legal norms. National "ombuds" may serve as advocates for those who feel that a breach has occurred. 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.[184] Civil liability and "dissuasive penalties" are often available for noncompliance with legal norms.[185] Many of these safeguards and remedies are lacking in U.S. information policy.

Transnational experience with privacy laws may have limited value, however. In the United States, several long-standing norms are in conflict with expectations of privacy, and these norms may not be as deeply rooted in other nations. Critics of centralized privacy controls have argued that adopting a European-style privacy policy may not fit with our constitutional traditions regarding free speech, our trust in the efficiencies of competitive markets, and our suspicion of government-imposed solutions to private-sector problems.[186] These competing norms have slowed privacy policy in the United States, and we can expect their influence to continue for some time. If a comprehensive privacy policy is to develop in this country, it must be reconciled with these countervailing influences. Consequently, while experience drawn from world privacy models can be helpful, it is not likely to be as compelling as experience drawn from our own cultural heritage.

Recent privacy trends in the United States reveal evidence of consensus as experimentation with privacy regulation moves forward at the federal level and, more frequently, in the state legislatures. Two general categories of particularly sensitive data are evolving.[187] For several years, the public has become increasingly concerned about identity theft

---

vidual. These include data revealing racial or ethnic origin, political views, religious beliefs, and membership in a trade union. *Id.* at art. 8(1)–8(2).

184. *See, e.g.*, Italian Data Protection Act (1996), *available at* http://www.privacy.it/legge675encoord.html. The foreword 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. See generally* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK (2000).

185. EU Directive, *supra* note 183, arts. 23–25.

186. *See, e.g.*, Volokh, *supra* note 114; Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L.J. 173, 231-32 (1999) (arguing against following EU approach to information privacy in the United States). *Cf.* U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (invalidating, on First Amendment grounds, FCC regulation requiring customer opt-in for use in marketing).

187. On information sensitivity, see RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW (1989). Wacks undertook a detailed study of privacy law in England and produced a table of "sensitivity grading of personal information" in which he classified various pieces of data as "high sensitivity," "moderate sensitivity," or "low sensitivity." *Id.* at 230-38. *See infra* text accompanying note 214.

and the corresponding need to protect personal information against misuse. There is also a shared belief that information about an individual's medical history should be safeguarded even if the costs of doing so are high.

### 1. Protecting Individual Identity

Personal identity is undoubtedly a cherished value in contemporary society. Except in unusual circumstances, people are highly offended when others steal their identity. Injuries resulting from impersonation can take several forms. If someone publishes under your name a letter to the editor of a newspaper, your reputation might be injured by any controversial views the letter expresses; the impersonation might cause you to suffer mental anguish and to expend time and money in correcting the public misperception of your character and beliefs. If a co-worker surfs the Web from your office computer and sends pornography from your e-mail account to everyone on your company's distribution list, you may lose not only your employer's respect but even your job.

Recent experience with the modern version of identity impersonation reveals a narrower concern. People are primarily troubled by the financial implications.[188] The problem is not theft of identity per se but theft of personal information that leads to financial loss or hardship. Recent laws and enforcement efforts are designed to address the growing problem of criminals who impersonate others to purchase goods and services on credit and to steal their financial assets. In dealing with this type of identity theft, policymakers have begun to recognize certain kinds of previously unprotected personal information that cause consumers difficulty. Two items in particular, credit card numbers and Social Security numbers ("SSNs"), have received the most attention. Legislatures began to enact laws protecting these identifying numbers once it became clear that the stakes were high. As a result, card numbers and SSNs are now generally considered worth protecting at considerable effort and expense.

Credit card fraud was the most common form of identity theft in 2003.[189] Because merchants now accept credit and debit cards in tele-

188. According to the Federal Trade Commission, 42 percent (214,905) of all complaints filed with the agency in 2003 related to identity theft. FED. TRADE COMM'N, NATIONAL AND STATE TRENDS IN FRAUD AND IDENTITY THEFT, JAN.–DEC. 2003, at 3–4 (Jan. 22, 2004), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud_2003.pdf. The most common complaints involved credit card fraud (33 percent), phone or utilities fraud (21 percent), and bank fraud (17 percent). *Id.* at 3, 10. More than half of the complaints came from individuals age 18-39. *Id.* at 11.

189. *Id.* at 3.

phone, fax, Internet, and other transactions in which the customer is not physically present, the purchaser's identity cannot be verified by matching a signature or checking a driver's license photograph. Consequently, knowledge of a person's card number alone is enough to commit fraud. Although a card holder is not responsible for unauthorized credit or debit card purchases,[190] stolen card numbers can cause a myriad of problems for consumers as they try to prove the fraud, undo the damage, and prevent it from recurring.[191]

Recognizing the great harm that unauthorized card use can inflict on consumers, businesses and governments have succeeded in securing card numbers from much unnecessary recordation and disclosure. In the private sector, newer technologies for processing card transactions have largely eliminated the carbon-copy credit card receipts that thieves could easily retrieve from trash receptacles. Sales on the Internet now usually move through encrypted servers that make card number theft more difficult, and most credit cards now have security codes imprinted on them as an added impediment to fraudulent use.[192]

In the public sector, over the past ten years several state initiatives began to limit the public display of card numbers in a variety of ways. Many states first banned merchants from requiring the display of a credit card or the recording of a card number as a condition for accepting payment by check.[193] This eliminated the opportunity for thieves to see the

---

190. Under 15 U.S.C. § 1643(a)(1)(B) (2000), a credit card holder's liability for unauthorized use cannot exceed $50. Liability for unauthorized use of a debit card, however, can exceed $50, but only if the debit card holder fails to notify the bank about the unauthorized withdrawal in a timely manner after learning about the withdrawal or receiving evidence of the withdrawal on a bank statement. *Id.* §1693g(a). The $50 liability is often waived by the card issuer. *See, e.g.*, the "zero liability" policy of the VISA card program, *at* http://www.usa.visa.com/personal/secure_with_visa/zero_liability.html?it=il_/personal/cards/benefits/zero_liability.html (last visited Oct. 24, 2004). An additional consumer risk with debit cards is that the consumer's bank account may be emptied before she realizes that the fraud has occurred. It may take days to rectify the problem, during which time the consumer may have bounced checks and lost access to deposited funds.

191. *See* U.S. GEN. ACCOUNTING OFFICE, REPORT TO CONGRESSIONAL REQUESTERS, IDENTITY THEFT: PREVALENCE AND COST APPEAR TO BE GROWING, GAO-02-363 (Mar. 1, 2002), *available at* 2002 WL 383568 (reporting that the leading types of nonmonetary 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).

192. Netscape developed secure socket layer ("SSL") technology for encrypting personal information before transmitting it over the Internet. Both Netscape Navigator and Internet Explorer use SSL, and many Web sites also use it when they transmit credit card information. URLs for sites using SSL normally carry the "https" designation rather than "http." *See* Brad Smith, *Keying Into Security*, WIRELESS WEEK, May 1, 2003, at 6.

193. *See, e.g.*, CAL. CIV. CODE § 1725(a)(1) (West 1998) (prohibiting the requirement of presenting credit or debit card as condition of check acceptance and the recording of card number on back of check); 810 ILL. COMP. STAT. ANN. 5/3-505A(1)–(2) (West 1993); MASS.

card number as the check moved through the bank collection process. Beginning in the late 1990s, many states enacted card number truncation statutes. These laws typically require that electronically produced debit and credit card transaction receipts truncate the card number so that only a few digits appear for identification purposes.[194] In late 2003, recognizing the importance of the issue and the need for uniformity, Congress passed a national standard which, when fully effective in a few years, will mandate that only the last five digits of a credit or debit card number appear on electronically printed receipts nationwide.[195]

While a stolen credit or debit card number can cause financial headaches, a stolen Social Security number can cause even more damage.[196] Perhaps because the SSN was created as an identifier for governmental programs, for many years there were few laws regulating the use of SSNs in the private sector. Most employers, banks, and other businesses are required by law to obtain an SSN for reporting purposes (such as income tax collection), and many other businesses request the numbers for identification purposes without legal mandates. Credit card and insurance applications, for example, usually ask for an SSN to verify identity in situations where the applicant may have the same or a similar name as others. Until recently, very few states had laws that prevented businesses from requesting an individual's SSN, and there were few restrictions on what businesses could do with the number once they got it. Even though an individual could refuse to give an SSN to a business, in most instances it was perfectly lawful for the business to refuse service if the number was not provided.[197]

---

ANN. LAWS ch. 93 § 105(a)–(b) (Law. Co-op. 1994); OR. REV. STAT. § 646.892 (2003); WISC. STAT. ANN. § 423.402 (West 1998).

194. *See, e.g.*, ARIZ. REV. STAT. § 44-1367 (2003); CAL. CIV. CODE § 1747.09 (West Supp. 2004) (renumbered from CAL. CIV. CODE § 1747.9 to § 1749.09 by 2004 Cal. Legis. Serv. 183 (West)); LA. REV. STAT. ANN. § 9:3518.3 (West Supp. 2004); ME. REV. STAT. ANN. tit. 10, § 1141(1) West Supp. 2003); MD. CODE ANN., COM. LAW II § 14-1318(c) (Supp. 2003); MO. STAT. REV. § 407.433.3 (Supp. 2000); N.J. STAT. ANN. § 56:11-42 West Supp. 2004); OKLA. STAT. ANN. tit. 15, § 752A (West Supp. 2004); VA. CODE ANN. § 11-33.2 (Supp. 2004); WASH. REV. CODE ANN. § 63.14.123 (West Supp. 2004). Many of the state truncation laws are summarized on the Web site of the National Conference of State Legislatures, *available at* http://www.ncsl.org/programs/lis/privacy/CreditCardReceipts.htm (last visited Oct. 24, 2004).

195. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 113 (2003) (amending 15 U.S.C. § 1681c (2000)). The five-digit requirement applies only to receipts printed electronically. *Id.* § 113(g)(2). The law does not take effect until three years after enactment for machines put in use on or before December 31, 2004. *Id.* § 113(g) (3).

196. *See* Lesley Mitchell, *New Wrinkle in ID Theft; Thieves Pair Your SS Number with Their Name, Buy with Credit, Never Get Caught; Social Security Numbers a New Tool for Thieves*, SALT LAKE TRIB., June 6, 2004, at E1.

197. *See* Soc. Sec. Admin., Publ'n No. 05-10002 (July 2004), *available at* http://www.ssa.gov/pubs/10002.html.

Protecting an individual's SSN is now generally regarded as an important societal value. In the government sector, SSNs have long been treated as deserving some measure of protection. The Privacy Act of 1974[198] established guidelines under which any federal or state agency may ask for a person's SSN. Individuals may not be required to give their SSN to a government agency without authorization by statute.[199] In addition, agencies may not deny a right, benefit, or privilege to anyone because of their refusal to disclose their SSN.[200] The Drivers Privacy Protection Act of 1994 includes an individual's SSN among the class of "highly restricted personal information."[201]

Cultural and legal pressures are moving the private sector in the same direction, as SSNs are increasingly considered to be sensitive information. The SSN was not designed to serve as the universal personal identification it has become. Pervasive use of the number has led to the escalation of the crime of identity theft.[202] Because a person's SSN is readily accessible to so many other people, it is possible for thieves to misappropriate an individual's SSN, open fraudulent credit accounts, gain access to financial and other personal information, drain the victim's financial assets, and tarnish the victim's personal credit history. In an effort to protect the confidentiality of SSNs, many states no longer use them as driver's license numbers.[203] Universities are limiting their use

198. 5 U.S.C. § 552a (2000).

199. Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (Dec. 31, 1974).

200. *Id.* § 7(a)(1).

201. "'[H]ighly restricted personal information' means an individual's photograph or image, social security number, medical or disability information." 18 U.S.C. § 2725(4).

202. *See* FED. TRADE COMM'N, PROTECTING AGAINST IDENTITY THEFT, *at* http://www.consumer.gov/idtheft/protect_againstidt.html#5 (last visited Oct. 24, 2004) (cautioning consumers to guard their SSNs carefully).

203. *See* J. Radick, *What's Required on a Driver's License*, PRIVACY J., at 3 (July 2001) (legislatures in about half the states have passed laws allowing drivers to remove their SSNs from driver's licenses). *See, e.g.*, MISS. CODE ANN. § 63-1-35 (1996). See also *Winners and Losers . . . State by State Analysis of Current Driver's License Laws and Requirements*, *at* http://www.networkusa.org/fingerprint/page4/fp-04-page4-winners-losers.html (last visited Oct. 24, 2004) (compiling state driver's license requirements). The trend was in the other direction a decade ago. In 1996, Congress passed a law requiring SSNs for use in various public records, as part of a movement toward a national identification card. *See* Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (requiring SSNs for any professional license, commercial driver's license, occupational license, marriage license, divorce decree, child support order, paternity judgment, or death certificate). After refusing to appropriate funds for the Department of Transportation to implement the new identification standards, Congress repealed the SSN requirement in October 1999. Department of Transportation and Related Agencies Appropriations Act, Pub. L. No. 106-69, § 355, 113 Stat. 986, 1027 (1999). *See also* Alexander L. Mounts, *A Safer Nation?: How Driver's License Restrictions Hurt Immigrants and Noncitizens, Not Terrorists*, 37 IND. L. REV. 247, 255 (2003).

as student identification numbers.[204] In California, legislation now restricts how businesses can use and disclose their customers' SSNs, although it does not regulate their collection.[205] For example, insurance companies, while still allowed to collect customers' SSNs, are not permitted to print them on wallet-sized proof-of-insurance cards.[206] Banks and investment companies may not require customers to transmit their SSNs over the Internet when conducting business online unless the number is encrypted.[207] Social security numbers may not be printed on documents sent through the mail, with some exceptions.[208] Other states have begun to prohibit commercial or other entities and government agencies from requiring customers to provide their SSN as part of the record for a transaction or service. A Rhode Island law, for example, subjects most commercial entities to fines if they violate the prohibition and record an SSN without specific statutory authority.[209] Several other states have recently enacted restrictions on the release or disclosure of an individual's SSN without authorization.[210]

Although federal bills have been introduced that would restrict the recordation, use, and release of SSNs in the private sector nationwide,[211]

---

204. *See, e.g.*, ALA. CODE § 16-5-7 (2002) (prohibiting state schools from using SSN as student ID number); N.Y. EDUC. LAW § 2-b (McKinney Supp. 2004) (prohibiting all public schools, including colleges and universities, from displaying, posting, or listing student SSNs); R.I. GEN. LAWS § 16-38-5.1 (a)–(b) (2001) (prohibiting all public schools, including colleges and universities, from using SSNs and from publicly displaying four or more consecutive numbers from an SSN); VA. CODE ANN. § 2.2-3808(B) (Michie 2003) (prohibiting use of SSNs on student IDs); WISC. STAT. ANN. § 36.11(35) (West 2002) (prohibiting use of SSNs on student IDs).

205. CAL. CIV. CODE § 1798.85(a)(1)–(5) (West Supp. 2004). *See* U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE CHAIRMAN, SUBCOMM. ON SOCIAL SECURITY, COMM. ON WAYS AND MEANS, H.R., GAO-04-11, at 20–23 (Jan. 2004).

206. CAL. CIV. CODE § 1798.85(a)(2).

207. *Id.* § 1798.85(a)(3).

208. *Id.* § 1798.85(a)(5). Other provisions of this law prohibit companies and individuals from posting or publicly displaying SSNs or from requiring people to log onto a Web site using an SSN without a password. *Id.* §§ 1798.85(a)(1), 1798.95(a)(4).

209. R.I. GEN. LAWS § 6-13-17(b) (2001). Rhode Island law prohibits most vendors from requiring consumers to provide their SSN as a condition of sale. *Id.* § 6-13-17(a). It exempts, however, insurance companies, state or federally licensed financial services companies, health care or pharmaceutical services providers, and credit card companies. *Id.* § 6-13-17(a)(1)–(2).

210. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-1373 (West Supp. 2003) (effective January 1, 2005; similar to California law but adding certain restrictions for state agencies and political subdivisions); GA. CODE ANN. § 33-24-57(f) (Supp. 2004) (effective July 1, 2004, but directed at insurance providers only); MO. ANN. STAT. § 407.1355 (effective July 1, 2006; similar to California law, but without specifically prohibiting printing of number on cards required to gain access to products or services); TEX. BUS. & COMM. CODE ANN. § 35.58(a) (Vernon Supp. 2004–05) (effective March 1, 2005; containing only the "print on card" restriction); UTAH CODE ANN. § 31A-22-634 (2003) (effective July 1, 2004; directed at insurance providers only).

211. *See, e.g.*, Social Security Number Misuse Prevention Act, S. 228, 108th Cong.

legislative efforts have stalled as Congress weighs the consequences of privacy protection against the commercial need to use SSNs to verify identity.[212] Restricting access to SSNs might harm some consumers and could possibly aid identity thieves by making identity verification more difficult for businesses.[213] Yet as more states experiment with various restrictions on the use of and access to SSNs, pressure for a national standard is mounting, much as it did with credit and debit card number truncation. If restrictions prove workable in one or more states, concerns about verification problems exceeding the benefits of added security may soon dissipate.

### 2. Protecting Personal Medical and Health Information

While concern about identity theft primarily reflects a fear of financial hardship, people tend to regard information about their personal medical history as highly sensitive for reasons that usually have little to do with the financial effects of disclosure. Information sensitivity depends on several factors,[214] and our heightened sensitivity toward personal health information shows these factors at work.

- *Character of the information.* For certain classes of information, its collection and use do not give rise to strongly held expectations of individual control. For others, the subject matter is so personal that most of us expect a great deal of control. People tend to be highly sensitive about disclosure of information regarding their sexual practices, for instance, but are much less concerned whether others know how they make a living.

- *Potential recipients of the information.* Determining whether information is sensitive requires, in part, an inquiry into the potential for sharing the information with unintended recipients. A patient who has no objection to his doctor's sharing information about his illness

(2003); Social Security On-line Privacy Protection Act of 1996, H.R. 1287, 105th Cong. (1997); *see generally* U.S. GEN. ACCOUNTING OFFICE, SOCIAL SECURITY NUMBERS: ENSURING THE INTEGRITY OF THE SSN, GAO-03-941T (July 10, 2003), *available at* http://www.gao.gov/new.items/d03941t.pdf (cautioning Congress that widespread availability of SSNs in corporate databases may facilitate identity theft).

212. *See* U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE CHAIRMAN, SUBCOMM. ON SOCIAL SECURITY, COMM. ON WAYS AND MEANS, H.R., SOCIAL SECURITY NUMBERS, GAO-04-11, at 23 (Jan. 2004), *available at* http://www.gao.gov/new.items/d0411.pdf.

213. *Id.*

214. RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 227-29 (1989) (discussing these factors).

with other medical staff would likely be very upset if the doctor disclosed the same information to a prospective employer.

- *Scale of the disclosure.* An individual's objection to disclosure of even the most trivial data will likely grow in proportion to the number of persons to whom the disclosure is made. Thus, disclosure of the name of one's personal physician on a paper application form that will be read by perhaps three or four people may be regarded as less objectionable than posting the same information on an Internet site that is accessible to millions. Similarly, as a public policy problem, releasing drug prescription information about thousands of people in a computer database may raise stronger privacy objections than releasing the same information from a single individual's file.

- *Purpose of collection, use, or disclosure.* Individuals are less likely to resist giving information when the purpose of disclosure is to advance their own interests, as when a physician transmits a patient's medical record to her insurance company for reimbursement. People are more likely to object if the purpose is less benign or if the information is used for purposes of which they were not aware. Thus, they might object to sharing their medical records with a drug company for marketing purposes.

In 1989, Raymond Wacks identified hundreds of categories of private information and classified them as items of high, moderate, or low sensitivity. Of twenty-three high-sensitivity categories, nineteen concern human health, physiology, sexuality, or medical procedures.[215] The high sensitivity of health information is hardly surprising. For more than two millennia, at least since the Hippocratic Oath,[216] the privacy of patient information has been essential to Western physicians. Standards of ethics have long protected health information vigorously in many health care professions.[217] In modern times, however, personal health informa-

215. *Id.* at 242. Among the other four, three concerned election voting behavior and the fourth was "non-factual information . . . recorded by police or obtained from informants." *Id.*

216. A standard version of the oath (ca. 400 B.C.) includes: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about." CODES OF MEDICAL ETHICS, OATHS, AND PRAYERS: AN ANTHOLOGY 19-20 (1989).

217. *See* Pachowitz v. Ledoux, 666 N.W.2d 88, 96–97 (Wis. Ct. App. 2003) (emergency medical technician violated patient privacy by disclosing medical information to co-worker). *See generally* CODES OF PROFESSIONAL RESPONSIBILITY: ETHICS STANDARDS IN BUSINESS, HEALTH, AND LAW (Rena A. Gorlin ed., 4th ed. 1999) (selected ethical codes for health care professions).

tion is collected, shared, and used by many organizations outside the medical professions, including employers, insurers, government program administrators, financial institutions, lawyers, and many others. As health-related data proliferate, privacy concerns increase.

Medical privacy is one area in which cost-benefit analysis has been the least influential as a decision-making method. In the preamble to the HIPAA privacy rule, the Department of Health and Human Services declared that medical privacy is a "fundamental right" different from "ordinary economic good[s]."[218] The department expressly acknowledged that while CBA has a role in the weighing of options, "[a]t the same time, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom."[219] To safeguard this fundamental right, the HIPAA regulations impose complex controls over the collection and distribution of health information on virtually every entity that handles health information, and they do so at substantial cost.[220] Before the HIPAA rules took effect, every state had laws protecting medical information to some extent,[221] but those laws lacked consistency. The HIPAA rules established national privacy standards and fair information practices that provide a base level of protection for individuals as they deal with health care providers, health plans, and health care clearinghouses.[222]

Other recently enacted federal laws treat medical information as highly sensitive. The Public Health Service Act requires a person's written permission prior to any disclosure of information related to substance abuse and to treatment for chemical dependency in a federally funded program.[223] The Drivers Privacy Protection Act includes "medical or

---

218. Standards for Privacy of Individually Indentifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

219. *Id.* at 82,464.

220. Estimates of compliance costs for the health care industry range from $17.5 billion in the first ten years to at least $43 billion in the first five years. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,761 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164) ($17.5 billion estimate); *Analysis of HHS Cost Estimates for the Final HIPAA Privacy Regulation,* report from Robert E. Nolan Company, Inc., to Blue-Cross BlueShield Association (March 2001), *at* http://www.hipaadvisory.com/action/Compliance/BCBSPrivacy.pdf ($43 billion estimate).

221. *See* ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1997 ed.); Standards for Privacy of Individually Indentifiable Health Information, *supra* note 218, at 82,464.

222. Health and Human Services Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.502(a) (2003). *See generally* Susan M. Gordon, *Privacy Standards for Health Information: The Misnomer of Administrative Simplification,* 5 DEL. L. REV. 23 (2002); *supra* text accompanying notes 46–58.

223. Health and Human Services Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. § 2.31(a)(1) (2003) (implementing § 543 of the Public Health Service Act, 42 U.S.C. § 290dd-2 (1994)).

disability information" within the class of "highly restricted personal information" that states must protect in motor vehicle records.[224] A 1996 amendment to the Fair Credit Reporting Act provides that a consumer reporting agency cannot issue a credit report containing medical information about a consumer unless the consumer consents in advance to its release.[225] The Fair and Accurate Credit Transactions Act of 2003[226] strengthened this protection by requiring consumer consent to be written, specific, and with full disclosure of the use for which the agency will release the information.[227] In addition, creditors may no longer access a consumer's medical information in connection with a credit eligibility decision;[228] moreover, with limited exceptions, affiliated companies can no longer share medical information freely among themselves.[229]

Public concern about medical privacy may have been driven by factors far different from those that fuel financial privacy reform and identity protection, but the progress toward a national consensus has traveled a similar path. In both sectors, a consensus on basic privacy entitlements was shaped by the continual accumulation of individual experience, the occasional experimentation of state legislatures, and the creative initiative (both privacy enhancing and privacy defeating) of private sector actors. Over time, "incompletely theorized agreements" about privacy rights have emerged, and we now have a growing list of unacceptable privacy invasions.

## CONCLUSION

In this Article I have supported the idea of examining the practical effects of proposed privacy alternatives and using cost-benefit analysis as an evaluative tool in the policy-making process, but I have opposed the tendency to rank alternatives according to CBA as the determinative basis for deciding information privacy issues. Collecting cost-benefit information can raise red flags about a proposed policy resolution and pose fundamental questions about the use of governmental power in regulating privacy in the non-governmental sector. It should not, however, be the exclusive, or even the dominant, decision-making tool.[230]

---

224. 18 U.S.C. §§ 2721(a)(2), 2725(4) (2001).

225. 15 U.S.C. § 1681b(g).

226. Pub. L. No. 108-159, 117 Stat. 1952 (2003).

227. *Id.* § 411 (amending 15 U.S.C. § 1681b(g) (2001)).

228. *Id.* § 411(g)(2). Federal banking agencies and the National Credit Union Administration will issue regulations, however, that permit creditors to use medical information for "legitimate operational, transactional, risk, consumer and other needs." *Id.* § 411(g)(5)(A).

229. *Id.* § 411(g)(4).

230. *See* Henry S. Richardson, *The Stupidity of the Cost-Benefit Standard*, 29 J. LEGAL

Part of the appeal of CBA is that it promises efficient use of scarce resources and provides a methodology for pursuing that end. Cost-benefit analysis is invaluable in setting commercial policy because policymakers are often asked to set rules for efficient allocation of economic resources. Advertising regulation, competition law, standards for weights and measures, and other commercial matters demand close examination of the economic effects of alternative solutions. Setting privacy policy is different, however, because important costs and benefits associated with this basic entitlement cannot reliably be reduced to economic terms. A different approach is needed if we are going to achieve a fair and just balance among competing interests.

If we jettison CBA as the dominant decision rule for information privacy policies and agree that economic interests are not controlling when it comes to protecting our personal information, we need a consensus on what basic privacy entitlements exist. We will reach a consensus sooner if we acknowledge the limits of CBA in the formulation of privacy policy and look to other sources for guidance on what is most important about our privacy concerns and what is in greatest need of our attention. Because information privacy in the digital era is still a relatively new concern, a consensus about legitimate entitlements has yet to coalesce. Through experience and experimentation over time, however, those entitlements may emerge.

There is virtue in being patient when creating a national public policy to address a new and dynamic problem. The slow pace of privacy regulation in the United States, as compared to the rush to regulate in Europe, may be beneficial in the long run. During this period of evolving responses to the proliferating database problem, policymakers can take time to find guidance in many sources and learn from diverse experiences as they attempt to define our most vital privacy interests and devise appropriate ways to safeguard them. Besides identity theft and medical privacy, it may be difficult to identify areas in which widely shared beliefs about privacy entitlements currently exist. Other candidates may soon emerge. There is a growing concern, closely related to medical privacy, about the collection, use, and disclosure of genetic information. Several states now have laws protecting genetic information and requiring consent for certain uses beyond those addressed by HIPAA.[231] With regard to privacy in the workplace, states are beginning to prohibit certain employer surveillance activities in the private sec-

---

STUD. 971, 974 (2000).

231. *See, e.g.*, N.J. STAT. ANN. § 10:5-43 to 10:5-49 (West 2002); N.M. STAT. ANN. § 24-21 (Michie 2002). *See generally* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA (Mark A. Rothstein ed., 1997).

tor.[232] On the other hand, there seems to be less agreement as to the need to regulate certain Internet practices, such as the content of Web site privacy policies and the use of cookie technologies and other consumer tracking devices.

The passive approach carries a price, of course, and it is not insubstantial. During this period of evolving sensibilities, the privacy interests of many citizens will be compromised in ways that could be prevented by stronger laws and more rigorous enforcement. For those who are harmed when their personal information falls into the wrong hands, there is little comfort in knowing that they are participants in a larger evolutionary process of policy formulation to benefit future generations. Moreover, as businesses continue to collect, manipulate, and share personal data in increasingly sophisticated (and profitable) ways, practices and attitudes about privacy may crystallize, thus making it more difficult to change the status quo and initiate sweeping reforms at a later time. Arguments against policy change become stronger as vested interests become more entrenched.

While we search for a normative theory of information privacy and a shared consensus about privacy entitlements in the digital age, the passive, inductive path may be the way of practical necessity. It is an uneven path, however, and it leads to an uncertain destination. In time we may learn that the virtues of a passive privacy policy did not outweigh the vices. The long-term effects of data proliferation remain to be seen, yet the stakes are high. The genie may be out of the bottle already,[233] and if we wait much longer to establish effective controls, it may be too late to put it back.

232. *See, e.g.*, CONN. GEN. STAT. ANN. § 31-48b(b) (West 2003) (prohibiting "electronic surveillance device or system" in the workplace). *See generally* Sharona Hoffman, *Preplacement Examinations and Job-Relatedness: How to Enhance Privacy and Diminish Discrimination in the Workplace*, 49 U. KAN. L. REV. 517 (2001).

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