1994

Setting Standards for Fair Information Practice in the U.S. Private Sector

Joel R. Reidenberg
Fordham University School of Law, JREIDENBERG@law.fordham.edu

Setting Standards for Fair Information Practice in the U.S. Private Sector

*Joel R. Reidenberg**

INTRODUCTION

The Information Superhighway in the United States and the emerging Global Information Infrastructure place standards for the treatment of personal information at the forefront of policy discussions among businesses, governments, and citizens.[1] Because the control of information means power, standards for the treatment of personal information have significant societal implications. Legal rules, industry norms, and business practices collectively form these standards.[2] Financially, the standards for the control of flows of personal information have a large economic impact. Businesses rely on personal information for activities ranging from back-office personnel management to product sales. Standards allocate both economic benefits and burdens. Politically, adequate standards for the treatment of personal information are a necessary condition for citizen participation in a democracy.[3] Since ancient Greece, a citizen's right to

---

* © Joel R. Reidenberg, 1995. Associate Professor, Fordham University School of Law. A.B., Dartmouth 1983; J.D., Columbia 1986; D.E.A., Univ. de Paris I (Pantheon-Sorbonne) 1987. An earlier version of this Article was presented at the Annenberg Conference on Information Privacy and the Public Interest (Washington, D.C., Oct. 6, 1994). Sections I and III were inspired by a discussion at the Fordham Faculty Scholarship Colloquium. Sections II and IV draw extensively on my work for the Study of American Data Protection Law, a report for the European Commission with Professor Paul M. Schwartz, under the direction of Professor Spiros Simitis. I would like to thank profoundly Paul Schwartz and Spiros Simitis for their endless encouragement and thoughtful comments and Carl Felsenfeld, Martin Flaherty, James Fleming, Robert Kaczorowski, Steve Thel, and William Treanor for their insightful reviews of an earlier draft. I am also grateful for the valuable research assistance provided by Françoise Gamet, Laura Sigal, Daniel Mollin, and Daniel Galpern. I remain responsible for all errors and omissions. Fordham University School of Law Faculty Research Grants supported work on this Article.

1. *See, e.g.*, Information Infrastructure Task Force, National Information Infrastructure: Agenda for Action 9-10 (Sept. 1993); Europe and the Global Information Society: Recommendations to the European Council 18 (May 26, 1994), *available on* Internet World Wide Web at http::://www.earn.net (also known widely as the Bangemann Report).

2. "Legal rules" consist of statutory mandates, regulatory obligations, and court decisions. "Industry norms" come from business sector aspirations and expectations. "Business practice" describes the actual treatment of information in commercial contexts rather than a legally mandated treatment or an aspiration goal.

3. *See* Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707, 732-37 (1987). During the Middle Ages in Europe, serfs were also denied the right to express

participate in society has depended on the ability to control the disclosure of personal information.[4] Without appropriate standards, citizens may be unduly constrained in their interactions with society. Socially, the treatment of personal information is an element of basic human dignity. Fair treatment of personal information accords respect to an individual's personality. Standards, thus, structure social relationships.

The terminology for standards of fair information practice has been poorly defined in the United States. The term "privacy" is often used to describe the allocation of rights to personal information.[5] This rhetoric is confusing. "Privacy" serves as a catch-all term, protecting a variety of interests ranging from government intrusion into the bedroom[6] to the inviolability of telephone communications.[7] Although fair information practices may be subsumed under the broad "privacy" label, the standards represent a narrower and distinct interest: maintaining the integrity of personal information and fairness to the individuals about whom the data relates. Specifically, such standards apply to the collection, storage, use, and disclosure of personal information.

For the business community, the U.S. standards for the treatment of personal information have never been more important. For almost twenty years, industry has avoided the imposition of legal rules through the promotion of self-regulatory policies.[8] Yet, in the last few years, both the development of industry norms and the implementation of appropriate business practices for self-regulation, as well as the consensus on a self-regulatory model, have broken down. Public opinion no longer views industry treatment of personal information as benign, and Congress is waking up from years of dormancy. At the same time, Europe is exerting

---

an opinion because they had no control over access to property and consequently no control over the flow of information from that space. *See* Blaise Lemper, Informatique et Democratie 19 (1987) (stating that the *droit à la parole*—the right to participate in public debate—was only accorded to those with rights to exclude others from access to property or a private space). In essence, the rules for access to and use of personal information determine the extent and quality of a citizen's participation in democracy.

4. *See* Lemper, supra note 3, at 19 (noting that a Greek citizen needed to control a "private" space in order to participate in public life). In essence, privacy is a precondition for democracy. Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States 32 (1992).

5. *See, e.g.*, Alan F. Westin, Privacy and Freedom (1967).

6. *See* Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965).

7. *See, e.g.*, Telecommunications Network Security: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce, 103d Cong., 1st Sess. 31-41 (1993) [hereinafter Hearings] (statement of Raymond G. Kammer, Acting Director, National Institute of Standards and Technology, Dept. of Commerce) (discussing the use of the Clipper Chip to assure that the nation's telecommunications infrastructure was compatible with wiretaps); *see also* Jaleen Nelson, Note, Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and its Effect on Free Flow of Information and Privacy, 41 UCLA L. Rev. 1139, 1147-55 (1994).

8. *See, e.g.*, U.S. Privacy Protection Study Comm'n, Personal Privacy in an Information Society (1977) [hereinafter Privacy Comm'n].

greater pressure on companies with global information needs. After a decade of little activity, foreign countries have begun to restrict information flows to destinations perceived as lacking sufficient standards. The European Union's proposed Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data has further renewed international debate on the treatment of personal information by U.S. businesses.[9]

The confluence of plans for an Information Superhighway, actual industry self-regulatory practices, and international pressure dictate renewed consideration of standard setting for fair information practices in the U.S. private sector. The legal rules, industry norms, and business practices that regulate the treatment of personal information in the United States are organized in a wide and dispersed manner. This Article analyzes how these standards are established in the U.S. private sector.

Part I argues that the U.S. standards derive from the influence of American political philosophy on legal rule making and a preference for dispersed sources of information standards. American standards are characteristically ad hoc and narrowly targeted. The driving force behind such narrow fair information practice standards is the philosophy that government should be limited and that a "marketplace of ideas" allows only minimal restrictions on flows of information, including personal information. As a corollary, this philosophy encourages dispersion in standard-setting authority. Part I consequently sets out the variety of sources for standards in the absence of general legal rules for fair information practice.

Part II examines the aggregation of legal rules, industry norms, and business practice from these various decentralized sources. This Article proposes that standards must be considered in the context of particular situations. This section draws on a checklist of commonly accepted, international principles of fair information practices and analyzes several contexts in key industrial sectors to understand the sufficiency of U.S. rules, norms, and practices. This Part concludes that important deficiencies exist in the U.S. treatment of personal information. Moreover, these deficiencies are significant in light of foreign scrutiny of international data flows.

Part III ties the deficiencies back to the underlying U.S. philosophy and argues that the adherence to targeted standards has frustrated the very purposes of the narrow, ad hoc regulatory approach to setting private sector standards. This section argues that instead of minimizing the manipulation of citizens and their thinking through unfettered flows of information, the private sector has established a "smoke screen" that in effect enables subtle, yet significant, manipulation of citizens through

9. *See* Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 Iowa L. Rev. 445 (1995). The proposed directive calls for restrictions of data flows to nonmember countries that lack a sufficient level of data protection.

hidden control of personal information.

Part IV addresses the irony that European pressure should force the United States to revisit the setting of standards for the private sector. This section argues that this pressure should instigate a return to the basic goals of American political values regarding the use and flow of information and should result in more comprehensive, yet flexible, legal rules. This Part concludes with a theory for global data flows on the basis of the use of decentralized U.S. standards despite differing national legal rules and European scrutiny.

I. THE ZEALOUS ADHERENCE TO THE PURSUIT OF TARGETED STANDARDS

Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector.[10] Legal rules have developed on an ad hoc, targeted basis,[11] while industry has elaborated voluntary norms and practices for particular problems.[12] Over the years, there has been an almost zealous adherence to this ideal of narrowly targeted standards. In other countries, the response to the Information Age has been quite different. Foreign nations have enacted broad, sweeping "data protection" laws to establish fair information practices in both public and private sectors.[13]

In democratic society, information standards reflect specific conceptions of governance.[14] An individual's desire for seclusion from the public realm opposes the societal value in a free flow of information for economic or political gain. Legal rules for the treatment of information set

---

10. *See, e.g.*, S. Rep. No. 1183, 93d Cong., 2d Sess. 14 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6929, 6932-34 (explaining the decision not to extend the Privacy Act of 1974 to cover the private sector); Robert M. Gellman, Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions, 6 Software L.J. 199 (1993); Arthur R. Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, 67 Mich. L. Rev. 1089 (1969).

11. *See* Joel R. Reidenberg, Privacy in an Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195 (1992).

12. *See, e.g.*, Privacy Comm'n, supra note 8, at 34 ("In the private sector, the Commission specifies voluntary compliance when the present need for the recommended change is not acute enough to justify mandatory legislation . . . ."); Direct Marketing Ass'n, Mail Preference Service (describing a DMA program for consumers to have their names and addresses suppressed from mailing lists for junk mail solicitations).

13. *See, e.g.*, Private Registers Etc. Act, No. 293, 1978 (Den.), *amended by* Act No. 383, 1987, *translated in* Danish Ministry of Justice, Pub. No. 622 (Oct. 2, 1987); Loi du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés (Fr.), *reprinted in* A.C.M. Nugter, Transborder Flow of Personal Data Within the EC 353-63 (1990); Wet Persoonsregistraties, 1988 (Neth.) (Act of Dec. 27, 1988 providing rules for the protection of privacy in connection with personal data files), *reprinted in* Nugter, supra, at 397; Data Protection Act, 1984 (U.K.), *reprinted in* Nugter, supra, at 365; *see also* Data Protection Roundup, Privacy Laws & Bus., Oct. 1994, at 2-8 (summarizing the status of data protection legislation in 35 countries).

14. *See* Bennett, supra note 4, at 32.

boundaries for state intrusion into a citizen's life and for state control of a citizen's conduct. For private interactions and the relationships between citizens, both law and practice set the balance between dignity and free flows of information. In American society, two powerful political values have driven the pursuit of narrowly targeted standards: (1) the desire to minimize restrictions on information flows and (2) the desire to disperse standards setting.

A. The Desire to Minimize Restrictions on Information Flows

At its founding, the American democracy faced two broad ideological commitments: one republican and the other (since termed) liberal. The republican commitment emphasized self-government, while the liberal commitment focused on individual rights. The Constitution of the United States reflected a synthesis of these two commitments.[15] In the course of its development, American politics enshrined a belief in limited government distinct from foreign models of democracy. While both state and national governments intervened in the economy from the birth of the republic, American political thought has consistently had a strong antistatist element. Even as the role of government in society through regulation of social welfare increased during both the Progressive Era and the New Deal Era, American political philosophy still reflected a substantial degree of hostility toward the regulation of private relations.[16] Elsewhere, namely in continental Europe, prevailing politics viewed the government more benevolently. Professor Glendon has aptly observed that the discourse of American politics is now cast in terms of "rights talk."[17] This rhetoric of rights emphasizes limitations on government power over the citizen. While the emergence of an American welfare state during the twentieth century may have signaled a greater role for government in the marketplace, the idea that the government should not intervene in the marketplace of ideas in the absence of compelling needs remains dominant. Rather than government action, private relationships or private contracts, thus, become a principal source of regulation for information flows.

1. The Constitutional Emphasis on Restraining Government

These liberal and republican influences commit the American Constitution to insuring citizens access to government, while also emphasizing the protection of citizens from government. The principal

15. *See* Martin Flaherty, History "Lite" in Modern American Constitutionalism, 95 Colum. L. Rev. 523 (1995).

16. *See* Morton J. Horwitz, The History of the Public/Private Distinction, 130 U. Pa. L. Rev. 1423, 1426 (1982).

17. *See* Mary A. Glendon, Rights Talk: The Impoverishment of Political Discourse 1-17, 47-75 (1991).

focus of the Constitution is the division of authority between the states and the federal government and the allocation of power across the branches of federal government.[18] At the federal level, the Constitution enumerates government powers, and the Bill of Rights sets out due process requirements, prohibits random searches and seizures, and guarantees freedom of assembly and freedom of the press.[19] While no explicit protection for fair information practices appears in the Federal Constitution, the Supreme Court has found implicit constitutional protection for privacy.[20] The privacy cases establish the individual as the "lone-bearer" of powerful rights of autonomy against the government.[21] In essence, the Supreme Court's "rights" jurisprudence, especially in the privacy area, emphasizes protections of the citizen against the government, rather than direct protection of citizens against each other.[22] The Court has required that state action be present to apply constitutional protections; private conduct is not sufficient. As Professor Tribe wrote: "Nearly all of the Constitution's self-executing, and therefore judicially enforceable, guarantees of individual rights shield individuals only from government action. Accordingly, when litigants claim the protection of such guarantees, courts must first determine whether it is indeed government action—state or federal—that the litigants are challenging."[23]

Similarly, state constitutions focus on the role of the state government with respect to citizens. While several state constitutions do contain explicit rights to privacy, most restrain the government from intruding on citizens' privacy, rather than protect citizens directly from each other.[24] The California Constitution is the rare exception.[25] Although the California

18. *See* id. at 4.

19. U.S. Const., amends. I, IV-V, XIV, § 1.

20. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152 (1973) (stating that although "[t]he Constitution does not explicitly mention any right of privacy, . . . the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution") (citations omitted); Griswold v. Connecticut, 381 U.S. 479, 484-85 (1964) (stating that the right of privacy is created by several fundamental constitutional guarantees).

21. Professors Glendon and Sandel have criticized the right to privacy as evolving toward an individual's right to make choices free of government interference. *See* Glendon, supra note 17, at 57 (arguing that privacy has been redefined as the right to make decisions without governmental intrusion); Michael J. Sandel, Moral Argument and Liberal Toleration: Abortion and Homosexuality, 77 Cal. L. Rev. 521, 527-28 (1989). For a critique of this view, see generally Linda McClain, Rights and Irresponsibility, 43 Duke L.J. 989 (1994).

22. *See* Jed Rubenfeld, The Right of Privacy, 102 Harv. L. Rev. 737 (1989) (arguing that the privacy cases are about protecting citizens against the government's ability to dictate choices that are fundamental to human individuality); Sandel, supra note 21, at 525 (arguing that "old privacy" cases emphasize protection against state surveillance and "new privacy" cases emphasize protection of individual decisions or autonomy against government restrictions on particular forms of conduct).

23. Lawrence H. Tribe, American Constitutional Law § 18-1, at 1688 (2d ed. 1988) (footnotes omitted).

24. *See, e.g.*, Ariz. Const. art. II, § 8; Ill. Const. art. I, § 6.

25. *See* Cal. Const. art. I, § 1.

Privacy Clause affords restraints on individual action, in practice, Privacy Clause cases emphasize protection against the state.[26]

In developing the state and federal constitutional emphasis, the U.S. Supreme Court eventually supported the growth of economic and social regulation during the Progressive and post-New Deal eras against challenges of intrusive government.[27] This constitutional acceptance reflected an emerging belief in the use of law as an instrument for the enhancement of personal freedom through social welfare.[28] The Supreme Court, however, preserved scrutiny of regulation to assure that government secured, rather than intruded upon, the participation of citizens in society.[29]

The constitutional emphasis on protection against the government formed the basis of a legal canon that enshrines free flows of information and minimal restrictions on the treatment of information. As Justice Brandeis once wrote, the First Amendment secures the "freedom to think as you will and to speak as you think."[30] To have this liberty of thought, information must be freely available. The prevailing U.S. doctrine for the treatment of personal information does not look to the positive use of regulation to secure such freedom.[31] To ensure information is freely available, American courts have long been committed to the "marketplace of ideas."[32] Under this canon, democracy functions best when ideas, no matter how well founded or repugnant, vie openly for acceptance in society. For political discourse, the free expression of ideas means that government-imposed restrictions on information are disfavored. Beyond the political realm, the Supreme Court extends, at least to some extent, this principle of minimally restrained information flows to the communica-

---

26. *See* J. Clark Kelso, California's Constitutional Right to Privacy, 19 Pepp. L. Rev. 327, 418 (1992) (discussing the impetus for the constitutional amendment that added the privacy clause). While the political debate surrounding the amendment to the California Constitution adding this right to privacy suggested that regulation of the private sector was one of the objectives, the cases interpreting the provision generally have a nexus with state action. *E.g.*, Porten v. University of San Francisco, 134 Cal. Rptr. 839 (Cal. Ct. App. 1976) (involving personal information disclosed to a state agency in connection with a student loan application). The California Supreme Court recently held that the Privacy Clause applies to purely private conduct. Hill v. NCAA, 865 P.2d 633 (Cal. 1994).

27. *See* West Coast Hotel v. Parrish, 300 U.S. 379 (1937) (upholding wage regulation against constitutional attack).

28. *See, e.g.*, Occupational Health and Safety Act, 29 U.S.C. §§ 651-678 (1988 & Supp. V 1993). Congress intended OHSA health and safety regulations to foster citizens' ability to work. Id. § 651.

29. *See* United States v. Carolene Prods., 304 U.S. 144, 152-53 n.4 (1938).

30. Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring).

31. *See* Cass R. Sunstein, The Partial Constitution 197-257 (1993) (arguing that, although prevailing constitutional interpretations exalt wholly unregulated speech, government intervention in the "marketplace of speech" can be understood as consistent with the Constitution).

32. *See, e.g.*, Turner Broadcasting Sys. v. FCC, 113 S. Ct. 1806, 1808 (1993); Virginia State Bd. of Pharmacy v. Virginia Citizen Consumer Council, 425 U.S. 748, 770 (1976).

tion of ideas unrelated to political discourse— "commercial speech."[33]

2. *The "Right to Privacy" Between Citizens*

For the treatment of personal information between citizens, "the right to privacy" first emerged as a narrow tort claim against yellow journalism. Samuel Warren and Louis Brandeis launched the tort based on "the right to privacy" in a law review article that sought to justify restricting the behavior of the tabloid press in Boston.[34] In the ensuing century, the common-law tort developed four distinct branches: (1) the misappropriation of name or likeness for commercial purposes, (2) the public disclosure of private facts, (3) intrusion upon seclusion, and (4) false light publicity.[35]

Scholars have debated theories of privacy ever since Warren and Brandeis immortalized the phrase "the right to be let alone."[36] Each branch of the common-law tort, however, focuses precisely on narrow restraints of private conduct and minimizes restrictions on information flows.[37]

The misappropriation tort is a right only against the unauthorized use of a person's name or likeness for commercial purposes.[38] The tort seeks to protect the commercial value of an individual's identity.[39] This original purpose of this action emphasized protection from unauthorized

---

33. *Virginia State Bd. of Pharmacy*, 425 U.S. at 770-73.

34. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

35. *See* Restatement (Second) of Torts § 652 (1977) (categorizing the various privacy tort actions); William Prosser, The Right to Privacy, 48 Cal. L. Rev. 383, 389 (1960) (arguing that "the law of privacy comprises four distinct kinds of invasions of four different interests of the plaintiff"). The false light branch of the privacy tort is similar to defamation. However, unlike actions for defamation, the false light privacy tort does not seek to protect an individual's reputation and is not predicated on malice.

36. Although the phrase "the right to be let alone" is often attributed to Warren and Brandeis, they were actually quoting the leading torts treatise of the day: Cooley on Torts. Scholarly debate on privacy theories has flourished. *See, e.g.*, Edward Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev. 962, 963 (1964); Charles Fried, Privacy, 77 Yale L.J. 475, 475 (1975); Jack Hirshleifer, Privacy: Its Origin, Function, and Future, 9 J. Legal Stud. 649, 649 (1980); Robert C. Post, Rereading Warren and Brandeis: Privacy, Property and Appropriation, 41 Case W. Res. L. Rev. 647, 647 (1991) [hereinafter Post, Rereading]; Robert C. Post, The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 Cal. L. Rev. 957 (1989); Westin, supra note 5, at 346-49.

37. Professor Glendon argued that the Warren and Brandeis formulation of the right to privacy is consistent with the John Stuart Mill tradition of protecting individuals. Glendon, supra note 17, at 54.

38. *See* Restatement (Second) of Torts § 652C (1977) (describing the tort of appropriation of name or likeness).

39. *See, e.g.*, Goodyear Tire & Rubber Co. v. Vandergriff, 184 S.E. 452, 454 (Ga. 1936) (discussing Georgia's codification of the tort); Freihofer v. Hearst Corp., 480 N.E.2d 349, 353 (N.Y. 1985) (interpreting the tort's codification by New York State); Bartholomew v. Workman, 169 P.2d 1012, 1014 (Okla. 1946) (discussing the tort at common law).

endorsements in advertisements and unauthorized commercial uses of photographs of individuals.[40] Individuals have a right to the commercial value in their name and image. As such, the tort imposes only narrow restrictions on the circulation of names and images.

The action for public disclosure of private facts limits the circulation to the general public of information that is shockingly offensive and not otherwise publicly available.[41] The protection is designed to prevent the wide dissemination of embarrassing facts[42] and, thus, imposes a specific narrow restraint on information flows.

The tort of intrusion upon seclusion focuses on the gathering of information rather than on the circulation of that information. This tort protects individuals from highly offensive methods of gathering information in private areas;[43] the action only sanctions conduct that offends the sensibilities. As such, this tort too has a limited scope in the scheme of restraints on information flows.

Finally, the tort protecting individuals against publicity that places a person in a false light only offers protection against the wide dissemination of information that is misleading or erroneous.[44] The tort relaxes the scienter requirements of actions for defamation, yet still preserves a narrow scope.

In isolation, each of these torts does not provide broad restriction on the circulation and treatment of personal information.[45] Together, however, they do suggest a somewhat more active role of law in regulating conduct between citizens in comparison to the traditional constitutional preferences regulating conduct between the state and its citizens. The combination of narrow rights still does not offer more than a small set of targeted restrictions on information flows.[46]

This philosophical antigovernment sentiment and doctrinal restraint on government continues to translate into specific hostility for comprehensive rules on the treatment of personal information. Self-

---

40. *See* Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68 (Ga. 1905).

41. *See* Restatement (Second) of Torts § 652D (1977) (describing the tort of public disclosure of private information).

42. Wide dissemination may not be necessary if sufficient embarrassment would occur within the individual's local community. *See* Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. 1990) (holding that disclosure by employer of employee's mastectomy to several co-workers satisfied the requirement for public disclosure of the private fact).

43. *See* Ault v. Hustler Magazine, Inc., 860 F.2d 877, 882 (9th Cir. 1988) (rejecting claim of intrusion because the plaintiff agreed to be photographed), *cert. denied*, 489 U.S. 1080 (1989).

44. *See, e.g.*, Polin v. Dun & Bradstreet, Inc., 768 F.2d 1204 (10th Cir. 1985) (denying claim for false light intrusion where the plaintiff's credit report was disseminated to 17 people); Restatement (Second) of Torts § 652E (1977) (describing actionable false light publicity).

45. *See* Reidenberg, supra note 11, at 221-27 (discussing tort actions for dissemination of personal information).

46. *See* id. at 234.

regulation, or the voluntary adherence to fair practices, by the private sector is the preferred mechanism to assure fair treatment of personal information in American society. Following the principle of free flow of information, legislatures respond only to specific issues;[47] legal rules, if any, are justified only when they narrowly target particular problems. These legal rules tend to develop as an ad hoc response to public scandal.[48] Consequently, such rules are sectoral in nature.

3. *The Underlying Purposes for Minimal Restrictions on Information*

The adherence to free flows of information and the corresponding preference for targeted standards of fair information practice pursue two underlying objectives: the avoidance of a manipulated citizenry and the prevention of the abuse of power. Because information is power in the Information Society, the control of information empowers the manipulation of citizens. In contrast, unfettered information flows enhance citizens' capacity to make free and informed decisions. If information is available and citizens have fair access, then information may not be censored or structured by the government to control citizen thinking or decision making.[49]

Privacy torts suggest a similar concern about deceptive information. As a right, privacy torts may offer rules of civility reflecting community judgments.[50] The justification for minimizing tort restrictions on information flows and allowing only targeted rules for the treatment of personal information is to prevent thought control. Targeted legal rules

---

47. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1988); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2520, 2701-2709 (1988 & Supp. V 1993), *amended by* Pub. L. No. 103-414, 1994 U.S.C.C.A.N. (108 Stat.) 4279; Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1988); Cable Communications Policy Act, 47 U.S.C. § 551(a) (1988); *see also* Privacy Comm'n, supra note 8, at 34 ("In the private sector, the Commission specifies voluntary compliance when the present need for the recommended change is not acute enough to justify mandatory legislation."); Gellman, supra note 10, at 203-08 (explaining the weak results of legislative attempts to codify standards of fair information practices); Reidenberg, supra note 11, at 220-29 (arguing that state legislation is narrowly focused). In the public sector, legislatures have sought broader regulation. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1988); California Information Practices Act of 1977, Cal. Civ. Code §§ 1798-1798.78 (West 1985 & Supp. 1995); New York Personal Privacy Protection Law, N.Y. Pub. Off. §§ 91-99 (McKinney 1988 & Supp. 1995); Wisconsin Personal Information Practices Act, Wis. Stat. §§ 19.35-19.36, 19.62-19.80 (1993-94); *see also* Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553 (1995) (criticizing public sector information practices).

48. The Video Privacy Protection Act of 1988, for example, responded to public outrage when the video rental records of a nominee to the Supreme Court were publicized. 18 U.S.C. § 2710 (1988). Likewise, the Fair Credit Reporting Act responded to consumer horror stories of dealings with credit reporting agencies. *See* 15 U.S.C. §§ 1681a-1681t (1988 & Supp. V 1993).

49. Implicit in fair access to information is the assumption that transaction costs related to the circulation of information will be either trivial or of equal significance to all citizens. This is not the case. *See* infra text accompanying notes 196-98.

50. *See* Post, Rereading, supra note 36, at 651-52.

showing the community ethos reflect attempts to restrain manipulations of citizens. The minimalist restraint on misappropriation of personal information and the narrow "false light" protection strive to harness the circulation of deceptive information that may manipulate citizens' perceptions of each other.[51]

Scrutiny of government actions and targeted standards for fair information practices assuage the public fear of the abuse of power. Restraints reserve to citizens the power to control information flows against government manipulation. Even beyond the issue of government rule making, the fear of concentrations of information and "Big Brother" led to protections against government surveillance and public sector information processing activities.[52] Constraints protect citizens against intrusions on personal privacy by the powerful institutions of government.

The goal of preventing abuse of power is also at the heart of the privacy torts. Warren and Brandeis sought to rein in what they perceived to be an abuse of journalistic power. Unlike typical torts based on fault, the resulting "privacy" torts emphasize rights based on prohibitions.[53] The "rights" approach rather than "fault" approach blurs the historical division between public and private law.[54] The "rights" orientation supports the political significance of information standards as protection against abuses of power. Privacy rights become part of the rhetoric of coercive power akin to government power. As a right, the torts empower citizens to block specific manipulative actions or abuses by others. The torts reserve to citizens the ability to prevent private power from intruding on personal privacy and to secure against the misappropriation of personal information.

B. The Dispersion of Standards of Fair Information Practice

As a corollary to minimal state regulation of information flows, the American system values a dispersion of standards for fair information practice. There are no universal rules and there is no discrete source, such

---

51. *See* supra text accompanying notes 30-33 (American legal policy has supported free information to promote free thinking).

52. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1988) (structuring federal government information practices); Right to Financial Privacy, 12 U.S.C. §§ 3401-3422 (1988 & Supp. V 1993) (protecting citizens from government access to bank account records); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, 2701-2711 (1988 & Supp. V 1993) (protecting the confidentiality of communications from the government); David Flaherty, Protecting Privacy in Surveillance Societies 321, 367-70 (1989) (arguing that U.S. protection against government surveillance is inadequate); Paul M. Schwartz, Data Processing and Government Administration: The Failure of the American Response to the Computer, 43 Hastings L.J. 1321 (1992) (arguing that protections are inadequate, particularly in light of social welfare program).

53. *See* David W. Leebron, The Right to Privacy's Place in the Intellectual History of Tort Law, 41 Case W. Res. L. Rev. 769 (1991).

54. *See generally* Horwitz, supra note 16 (noting that American legal thought generally sought to distinguish tort issues from constitutional or public law issues).

as one sectoral rule or one industry norm or practice, to provide all the standards for a particular context. Fair treatment of personal information relies on the aggregation of standards from various sources. This diversity promotes the goal that no single actor, whether it be the government through its power to make legal rules or a private firm through market power and contractual relationships, should control information flows.

In theory, the decentralization of fair information practice standards through legal rules, industry norms, and business practice offers flexibility to tailor the standards for specific conditions. The different forms of standards coupled with the variety of standard makers—namely government, industry groups, and individual companies—can target problem issues. This theory draws on the same thinking as the federalist goal of making the states "laboratories" for appropriate kinds of regulation.[55] Within this paradigm, standards for information practices may arise at the federal, state, and even private sector level to best meet particular issues.

As a matter of legal policy, the decentralization of standards implies that fair treatment of personal information will emerge from overlapping and substitutable sources. Legal rules may overlap business practice, and either set of standards may substitute for the other type of standard. For example, either legal rights or the technical characteristics of an information system may achieve the result of fair treatment of personal information.[56] Decentralization also means that the mechanism to achieve fair information practices is secondary to the actual results. This policy is justified only if the combination of varied sources of standards provides a full set of fair information practices.

In specific cases, the actual contours of fair information practice evolve from two sources: (1) legal rules and (2) industry norms and business practice. Each source has different characteristics and values. Only the combination of treatment under the standards from each of these sources can completely develop fair information practices in the private sector.

1. Legal Rules

The most powerful standards for the treatment of personal information are established through direct legislation. Specific laws, such as the Fair Credit Reporting Act[57] or the Video Privacy Protection Act,[58]

55. This famous description of the goals for federalism comes from a Brandeis dissent in New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932). For purposes of fair information practices regulation, only the basic concept is significant for U.S. standards setting in the private sector. The actual nuances and evolution of federalism are beyond the scope of this Article.

56. *See generally* Joel R. Reidenberg, Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms, 6 Harv. J.L. & Tech. 287 (1993).

57. 15 U.S.C. §§ 1681-1681t (1988).

58. 18 U.S.C. §§ 2710-2711 (1988).

set targeted rules for the treatment of information. Other legal doctrines may also indirectly have an impact on the treatment of personal information and, thus, establish additional legal rules. For example, the Equal Employment Opportunity Act[59] establishes, to some degree, standards for the treatment of data pertaining to racial or ethnic origin. Similarly, tort rules such as defamation can have a dramatic impact on business treatment of personnel records. Employers' fear of liability constrains the retention and dissemination of personal information relating to employees.

2. *Industry Norms and Business Practice*

Business and management decisions set standards. While commercial policies are the driving force behind the existence or lack of existence of business practices,[60] several different forces mold business treatment of personal information. Standards may emerge from: (a) the technical network structure, (b) industry codes of conduct, (c) company policies, (d) contractual arrangements, and (e) pressures for good corporate citizenship. Because business decisions are flexible and can easily change, the establishment of standards through business practice depends upon the extent to which such standards are actually implemented by specific companies. In any specific situation, however, the effectiveness of business practice to achieve fair information practice will depend upon the harmonization of commercial interests with individual interests.

a. Technical network structure

Technology itself may structure the treatment of personal information. Technical decisions such as the frequency of data purges, or back-up storage, "hard wires" rules for the treatment of personal information directly in the network. An information network may gather and store significant amounts of personal information and make the information accessible to anyone with network privileges, or the computer system may keep only limited information and restrict access to certain authorized corporate officers. These choices in network structure and technology embed default rules or practices into the architecture of an information network.[61] Although technology can be modified, these business practices do provide a robust means of establishing standards for fair information practice.

---

59. 42 U.S.C. §§ 2000e to 2000e-17 (1988 & Supp. V 1993).

60. *See generally* H. Jeff Smith, Managing Privacy: Information Technology and Corporate America 85-86 (1994) (noting that short-term profit incentives impede corporate information privacy policy making).

61. *See* Reidenberg, supra note 56, at 296-301.

b. *Industry codes of conduct*

Industry codes of conduct set voluntary benchmarks for companies.[62] At best, they establish an ethos for an industrial sector. The actual treatment of personal information by companies in the industry is not reflected by the existence or nonexistence of a sectoral code. To the extent that a code reflects customary industry practice, it may have an important influence on specific companies. However, an industry code itself is a weak source for standards because such codes are voluntary and lack enforcement; the only true site of self-regulation remains at the level of company activity.

c. *Company policies*

Actual company policies and their specific implementation offer important standards of fair information practices.[63] Company policies designed for a variety of purposes are relevant sources for fair information practices. If the implementation of a company data security policy means that strict limits are placed upon access to personal information, the result is an important standard for fair information practices with respect to that company. Nonetheless, company policies and their implementation offer "soft" standards; they are neither legally binding nor industry-wide.

d. *Contractual arrangements*

Contractual arrangements may arise from two sets of relationships. Companies may contract directly with individuals and may stipulate in such a contract how an individual's personal information will be treated. Companies may also contract with business customers and similarly provide for the treatment of personal information by the business customer. In this case, protection of an individual's personal information is an incident of the contract between the company and its business customer. Each set of arrangements may establish legally binding standards because of the enforceability of contracts.[64]

---

62. *See, e.g.*, Direct Marketing Ass'n, Guidelines for Personal Information Protection [hereinafter DMA Guidelines]; Information Industry Ass'n, Fair Information Practices Guidelines (1994).

63. *See, e.g.*, American Express, An Important Notice to Our Cardmembers Concerning Cardmember Privacy, Mailing and Telemarketing Options (1993); Citibank Mastercard & Visa, Privacy Policy (1993).

64. In the case of contracts between businesses, the individuals protected by terms in the agreement are third party beneficiaries. *See* John D. Calamari & Joseph M. Perillo, The Law of Contracts 691-702 (3d ed. 1987). Because courts limit the enforcement rights of third party beneficiaries, those individuals will only be able to recover under specific circumstances. Id.

e. *Good corporate citizenship*

Finally, pressures from public opinion, academia, advocacy groups, and government officials may also set the tone for business practice. These pressures place the good name and image of companies at risk if treatment of personal information is unfair. To promote good corporate citizenship, some companies have implemented new practices. Companies such as Equifax and Dun & Bradstreet have recently even included commitments to privacy in their annual reports.[65] American Express now provides a detailed privacy notice to cardholders on an annual basis.[66] These pressures and incentives form moderately strong standards because companies expect some form of public sanction to result from poor practices such as lost business, lost goodwill, or constraining government regulation. Nevertheless, nothing about corporate citizenship pressures is legally binding.

The dispersion of standards for fair information practice across legal rules, and industry norms and business practices, reinforces narrowly targeted treatment of personal information. Each type of standard takes a particular perspective on fair information practice and addresses particular contexts or characteristics of the treatment of personal information. Under the U.S. scheme, no single standard seeks to cut across boundaries of law and industry practice.

II. THE DISAPPOINTING AGGREGATION OF DISPERSED STANDARDS

The pursuit of targeted standards at a time of explosive growth in wide-scale information processing activity makes the actual determination of rights, responsibilities, and practices in American society complex. The varied standards for fair information practice offer overlapping, yet distinct, treatment of personal information. Only the combination of legal rules, industry norms, and business practices can properly define the scope of standards for the treatment of personal information in the private sector.

The assessment of U.S. standards requires a comparison with a benchmark for principles of fair information practice. A variety of American, international, and foreign legal instruments have articulated

---

65. *See* Dun & Bradstreet Corp., Annual Report to Stockholders (1993), *available in* LEXIS, COMPNY Library, SECOL File; Equifax Inc., Annual Report to Stockholders (1992), *available in* LEXIS, COMPNY Library, SECOL File; Equifax Inc., Annual Report to Stockholders (1991) [hereinafter Equifax 1991 Report], *available in* LEXIS, COMPNY Library, SECOL File.

66. The exact wording of this notice is contained in an assurance made by American Express to the Bureau of Consumer Frauds and Protection of the New York Attorney General's Office. *See In re* American Express Travel Related Servs., Inc., Agreement of Voluntary Assurances (May 8, 1992) (on file with the University of Iowa College of Law library).

commonly accepted standards.[67] These commonly accepted standards provide a thorough set of criteria to evaluate the development of U.S. standards. While the legal instruments approach standards for the treatment of personal information comprehensively, the existence of a comprehensive set of standards still comports with the ad hoc and targeted U.S. approach. Standards themselves do not offend the value of minimal restrictions on information flows. Standards are necessary for a fair "marketplace" of personal information. Moreover, the entire set of commonly accepted standards need not appear in any single U.S. source; the collection of American standards from all U.S. sources can treat personal information according to the commonly accepted standards.

The appropriate analytic method to assess American standards is to focus on particular contexts for information processing. An accurate general assessment is precluded by diverse needs for personal information in the private sector and targeted standards from dispersed sources; the multitude of practices and narrow standards defy universally applicable conclusions. The measure of fair treatment of personal information, thus, becomes the extent to which the benchmark principles are satisfied in particular contexts through the aggregation of the dispersed standards. For the analysis to be meaningful, the contexts must be drawn from key industrial sectors that represent major information processing activities with a significant impact on society.

A. The Benchmark: Commonly Accepted Standards

In the United States and abroad, there is a consensus on the general principles necessary for the fair treatment of personal information in the private sector. The U.S. Department of Health, Education and Welfare wrote one of the first sets of guidelines for the treatment of personal information.[68] The U.S. government supported similar voluntary guidelines adopted several years later by the Organization for Economic Cooperation and Development (OECD).[69] Many major American companies publicly declared their acceptance and support of these OECD principles.[70] These core principles are also embodied in a number of U.S. laws.[71] Elsewhere in North America, Québec has adopted legislation

---

67. *See* infra text accompanying notes 68-78.

68. *See* Flaherty, supra note 52, at 306; Privacy Comm'n, supra note 8, at 15 n.7.

69. *See* Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. (C 58 final) (Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981) [hereinafter OECD Guidelines]. The U.S. government participated in the negotiations. *See also* Joel R. Reidenberg, The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services, 60 Fordham L. Rev. S137, S167 (1992) (comparing the OECD Guidelines with the European Convention).

70. *See* General Accounting Office, Privacy Policy Activities of the National Telecommunications and Information Administration (Aug. 31, 1984), *cited in* Gellman, supra note 10, at 227 n.60; U.S. Council for Int'l Business, List of U.S. Corporations Supporting the OECD Privacy Guidelines (1983).

71. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1988) (establishing core principles for

recently mandating comparable basic principles.[72] Across the Atlantic, the European treaty on data protection[73] contains a set of basic principles similar to the OECD Guidelines.[74] Although the United States is not a party to the treaty, the treaty mandates the enactment in signatory countries of laws containing the core principles. More recently, the European Union's proposed directive on data protection models its standards for the fair treatment of personal information around the same set of basic principles that exist in various European national laws.[75] Likewise, in Asia, data protection policies look to the basic principles found in the OECD Guidelines and European treaty.[76]

The basic principles of this global consensus form four sets of standards: (1) standards for data quality, (2) standards for transparency or openness of processing, (3) standards for the treatment of particularly sensitive information, and (4) standards for the enforcement of fair information practices.[77] While the precise requirements and interpretations for data quality, transparency, sensitive information, and enforcement vary,[78] the core elements are commonly accepted by the global community.

---

the public sector); Video Privacy Protection Act, 18 U.S.C. § 2710 (1988) (establishing core principles for video records); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1988) (establishing core principles for the cable communications sector).

72. *See* An Act respecting the protection of personal information in the private sector, 1993 S.Q. 503 (Can.) (to be codified at R.S.Q. ch. P-39.1).

73. Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Eur. T.S. No. 108 (Jan. 28, 1981), *reprinted in* 20 I.L.M. 317 [hereinafter European Convention].

74. *See* Jon Bing, The Council of Europe Convention and the OECD Guidelines on Data Protection, *in* Regulation of Transnational Communications, 1984 Mich. Y.B. Int'l Legal Stud. 271; P. Howard Patrick, Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and the OECD Guidelines, 21 Jurimetrics J. 405 (1981); Reidenberg, supra note 69, at S143-46.

75. *See* Proposal for a Council Directive on the Protection of Individuals in Relation to the Processing of Personal Data, Eur. Comm. Doc. COM(90)314 final-SYN 287 (July 17, 1990) [hereinafter Original Proposal]; Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Eur. Comm. Doc. COM(92)422 final-SYN 287 (Oct. 15, 1992) [hereinafter Amended Proposal]; Common Position Adopted by the Council with a View to Adopting Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (C 93) 1 [hereinafter Common Position]; Simitis, supra note 9.

76. *See* Reidenberg, supra note 69, at S151-52.

77. Some scholars have even argued that these norms form customary international law. *See* Olga Estadella-Yuste, Transborder Data Flows and Sources of Public International Law, 16 N.C. J. Int'l & Comm. Reg. 379 (1991).

78. *See generally* Reidenberg, supra note 69.

1. Data Quality Standards

The benchmark of data quality consists of commonly accepted standards to assure that personal information is acquired legitimately and is used in a manner that treats fairly the interests of individuals, industry, and society. These standards provide value to personal information. A key commonly accepted standard requires that personal information only be collected lawfully for specific purposes.[79] This basic standard imposes an obligation on data collectors to determine the uses of each piece of personal information prior to its collection and an obligation to obtain such information solely through lawful means. Another core element stipulates that personal information be used by the collector only in a manner compatible with the purpose for collection and that unrestrained secondary use is inappropriate.[80] This critical standard binds the treatment of personal information to the uses for which the information was collected.

The commonly accepted data quality standards also concur that personal information must be relevant for the purpose intended by the collection of the information. This core element proscribes the collection of extraneous personal information.[81] While this principle of data quality provides no clear guidance to determine whether particular information is necessary for an identified collection purpose, the commonly accepted standard imposes on collectors of personal information an obligation to resist the desire to acquire as much information as possible.

The timeliness of information is also an important core element of data quality standards. There is, thus, a commonly accepted standard that collectors should not store personal information any longer than necessary to accomplish the purposes for collection.[82] This is designed to assure the validity of personal information in circulation.

Data quality further demands accuracy of personal information. Commonly accepted standards assure this aspect by providing individuals with access to their personal information and the ability to require correction of inaccurate data.[83] Finally, data quality also requires measures to assure the integrity of personal information. There is a common standard that security measures are necessary to protect personal information against destruction or unauthorized alteration.[84]

---

79. *See* Common Position, supra note 75, art. 6(1)(b); European Convention, supra note 73, art. 5; OECD Guidelines, supra note 69, art. 9.

80. *See* Common Position, supra note 75, art. 6(1)(b); European Convention, supra note 73, art. 5b; OECD Guidelines, supra note 69, arts. 9-10.

81. *See* Common Position, supra note 75, art. 6(1)(c); European Convention, supra note 73, art. 5c; OECD Guidelines, supra note 69, art. 8.

82. *See* Common Position, supra note 75, art. 6(e); European Convention, supra note 73, art. 5e; OECD Guidelines, supra note 69, art. 8.

83. *See* Common Position, supra note 75, art. 12; European Convention, supra note 73, art. 8c; OECD Guidelines, supra note 69, arts. 12-13.

84. *See* Common Position, supra note 75, art. 17; European Convention, supra note 73,

2. *Standards for Transparency of Information Processing*

The benchmark of transparency consists of commonly accepted standards that assure the openness of information processing.[85] Global consensus dictates that the circulation of personal information be open to scrutiny by individuals and not obscured from view.

The core elements for the transparency of information processing assure the participation of individuals in the treatment of their personal information. The first commonly accepted standard is that the very existence of information processing activities must be transparent to citizens.[86] The core standard requires that collectors of personal information give individuals notice for the collection of personal information. In some cases, the commonly accepted transparency standards go further and require that collectors obtain the affirmative consent from individuals for certain processing and use of personal information.[87]

3. *Special Protection for Sensitive Data*

For information practices to be fair, benchmark standards recognize that certain personal information is inherently more sensitive than other data. A commonly accepted standard establishes that the treatment of sensitive information warrants greater scrutiny and protection.[88] Specifically, data pertaining to characteristics such as race, religion, health, or political beliefs must be accorded a higher level of protection.

4. *Enforcement of Fair Information Practices*

The benchmark of enforceability includes commonly accepted standards to assure the implementation of fair information practices.[89] The core elements of this consensus on enforceability has two components. First, there must be supervision and oversight of the treatment of personal information. Second, there must be a remedy for aggrieved individuals.[90]

---

art. 7; OECD Guidelines, supra note 69, art. 11; *see also* Office of Technology Assessment, U.S. Congress, Information Security and Privacy in Network Environments (1994) (discussing the critical importance of security for network information).

85. This use of the term "transparency" comes from the trade meaning rather than certain business meanings that refer to hidden, back-office activities. In the trade sense, transparency means that rules, regulations, and practices should be open to scrutiny. Certain business usages of "transparency" mean that intermediary business functions are hidden from customers.

86. *See* Common Position, supra note 75, arts. 7(a), 10(1), 11(1); European Convention, supra note 73, art. 8a; OECD Guidelines, supra note 69, art. 13a.

87. *See* Common Position, supra note 75, art. 7(a); European Convention, supra note 73, art. 5b; OECD Guidelines, supra note 69, arts. 9-10.

88. *See* Common Position, supra note 75, art. 8; European Convention, supra note 73, art. 6; OECD Guidelines, supra note 69, art. 3(a).

89. *See* Common Position, supra note 75, arts. 28, 30; European Convention, supra note 73, art. 13; OECD Guidelines, supra note 69, art. 19.

90. From a U.S. perspective, the acceptance of private remedies as a commonly accepted

The common acceptance of these two core standards provides significant strength to the benchmarks.

B. The Search for Benchmark Standards in Key Contexts

The multitude of data processing situations, the targeted nature of U.S. standards, and the multilayered regulatory framework in the United States necessitate a context-specific methodology to analyze the implementation of benchmark standards.[91] Narrowly targeted standards can only make sense against the backdrop of their intended applications.

For the analysis to be meaningful, the identification and selection of information processing contexts must be appropriate. The contexts should reflect key industries or sectors in American life that have a significant impact on society. While many activities satisfy this criteria, two major areas clearly qualify: direct marketing and employment. Within each of these areas, the treatment of personal information is diversified in all senses. The provision of information is diversified, the providers of information are diversified, and the uses of information are diversified. The complexity of contextual analysis calls for even greater selectivity. Narrower contexts within each area should reflect representative treatment of personal information within the industry or sector. For example, in the employment field, the treatment of personnel records by employers represents a critical information processing context. The treatment of personal information in personnel records is vital to labor markets and has a significant impact on employees and society. By careful selection of contexts, the analysis and comparison of U.S. standards against the commonly accepted benchmark standards offers a concrete assessment of key fair information practices in the U.S. private sector.

1. Direct Marketing

The direct marketing industry has become a major force in the American economy.[92] In offering valuable shopping services to consumers, direct marketing relies on the gathering of massive quantities of personal information. Fair information practices for direct marketing focus on how particular individuals are identified for solicitations and how names are exchanged among collectors of personal information. The receipt of unwanted commercial solicitations may be a nuisance, but junk mail and junk calls are not in themselves an issue of fair information practice.

---

standard is not entirely clear. At the international level, the United States has often objected to mandatory rules that have private remedies. Yet, where U.S. legal rules provide for standards of fair information practice, private remedies are included.

91. *See* Reidenberg, supra note 56, at 296 (arguing that general principles seeking to balance free flows of information with human rights will necessarily require contextual interpretations).

92. The direct marketing industry as a whole claims to contribute $350 billion to the gross national product. Larry Jaffee, Catalog Revenue in 1992 Reached $51.5 billion: WEFA Group Study, DM News, July 5, 1993, at 4.

One of the most important contexts for the treatment of personal information in direct marketing is the profiling of information.[93] By cross-referencing numerous items of personal information, individual profiles are developed. These profiles may consist of a single characteristic, such as subscribers to Penthouse[94] or denture adhesive buyers.[95] They may also consist of a more complete set of characteristics such as married, middle-aged, "large size" women with children and moderate incomes who purchase particular types of underwear.[96] A list of individuals who meet specified characteristics conveys far more than innocuous name and address data and implicates the benchmark standards for the treatment of personal information.

This industry obtains discrete bits of personal information from many sources. Interactive communications now leave significant amounts of personal information behind, such as the details of an individual's use of identifiable network services. Transaction data, typically derived from calls to toll-free numbers and mail order purchases, offer a wealth of information about individuals.[97] For example, calls to a touch tone health information center generate data on the phone subscriber and on that household's interest in particular diseases or health products. Subscription lists from publications and purchasing patterns at stores all leave similar traces of individual behavior.[98] Public records also provide personal information to this industry. Property records, for example, indicate the value or purchase price of an individual's home as well as any outstanding mortgage amounts.[99]

Direct marketers' treatment of personal information for profiling demonstrates a surprising absence of many benchmark standards. In contrast to other U.S. industries, no identifiable sectoral law targets direct marketing.[100] Sectoral laws in other fields, such as home entertainment,

---

93. Profiling must be distinguished from the commercialization of personal information in the form of list sales or rentals. The exercise of fair information practices to create the profile does not imply that fair practices are employed to commercialize the personal information. The opposite is also true. High standards for the commercialization of lists do not necessarily reflect on the standards implemented for the creation of the underlying profiles.

94. *See* General Media Handles Newly Merged Database, DM News, Dec. 5, 1994, at 31 (including the list of Penthouse subscribers).

95. *See* LH Management Advertisement, DM News, June 20, 1994, at 33; Sea-Bond Denture Names Requestors, DM News, Mar. 27, 1995, at 52.

96. *See* Venture Communications Advertisement, DM News, Dec. 26, 1994, at 27.

97. *See* Jonathan Berry et al., Database Marketing: A Potent New Tool for Selling, Bus. Wk., Sept. 5, 1994, at 56, 56-62.

98. Catalogs containing thousands of such lists are already in existence. *See* Standard Rate & Data Serv., The Bullet: Direct Mail List Rates and Data, Sept. 1993.

99. Both LEXIS and Westlaw have searchable files containing such information.

100. Legislation limiting junk phone calls is not designed as a fair information practices law. *See* Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (Supp. IV 1992). Only provisions related to the maintenance of "do not call" databases impact on the treatment of personal information.

address some marketing uses of personal information.[101] Thus, industry norms and business practices largely set the standards for the treatment of personal information in this sector. The industry trade association, the Direct Marketing Association (DMA), has developed a code of conduct[102] and has a Privacy Task Force to promote voluntary, self-regulatory standards within the sector.[103] In fact, the DMA has engaged in a major effort to promote the implementation of information practice standards.[104] Nevertheless, company practices for profiling remain the principal source of actual standards.

a. Profiling and data quality standards

Compared to the benchmark of commonly accepted standards for data quality, direct marketing standards in connection with profiling are disappointing. The legal rules are exceedingly sparse.[105] Profiles themselves are only rarely subject to legal restraints for collection purposes,[106] and virtually no legal rules restrict secondary use of information for profiling, the collection of unnecessary information, or the duration of storage. Because of public outrage to particular abuses, rare exceptions are found in the home entertainment and credit reporting fields.[107]

Technical arrangements for the computer systems that process direct marketing profiles do not routinely provide standards for the core elements of the data quality benchmark. For example, the information system at Metromail, one of the nation's largest list brokers, is not even configured to accommodate requests for access to personal information

---

101. *See* 18 U.S.C. § 2710(b)(2) (1988) (video records); 47 U.S.C. § 551(c)(2)(C) (1988) (cable communications records).

102. DMA Guidelines, supra note 62.

103. Recently, the Direct Marketing Association released a Fair Information Practices Manual to elaborate standards for the treatment of personal information. Direct Marketing Ass'n, Fair Information Practices Manual (1994) [hereinafter DMA Manual].

104. Id.

105. Only a few laws limit marketing uses of personal information gathered from specific sources. *See, e.g.*, 18 U.S.C. § 2710 (1988) (providing that video stores may keep personal information to fulfill the purpose of collection); 47 U.S.C. § 551(a)(1) (1988) (providing that cable company may collect personal information from subscribers only if it specifies the reason and informs subscribers). Other key sources of profile information, such as telephone and purchase transaction records, are unrestricted. Another prime source, state driver's license records, however, soon will be subject to restrictions. *See* Omnibus Crime Act of 1994, 18 U.S.C. §§ 2510-2515 (1994). California Senator Barbara Boxer's amendment to the crime bill (Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 1994 U.S.C.C.A.N. (108 Stat.) 2099-2102, to be codified at 18 U.S.C. §§ 2721-2725) required that state departments of motor vehicles offer drivers the ability to opt out of the now public disclosures of data such as height, weight, hair color, eye color, and corrected vision. Imposition of the restrictions were motivated by a stalking case in California in which a murderer found the victim by accessing state motor vehicle records.

106. *See* Mass. Gen. L. ch. 175I (1992).

107. *See* Reidenberg, supra note 11, at 219-20, 234-36.

profiles.[108] Even having protections against the misuse of profiles through seeding lists[109] does not deal with underlying secondary use of information in the creation of the profile.

To some extent, technical structures do address other aspects of the data quality benchmark. System planning can limit the duration for which companies store personal information for profiling. While the capacity for retaining massive volumes of information has increased, and the associated costs have decreased, capacity and cost are not unlimited for most companies.[110] Consequently, companies will schedule data purging for their systems. Similarly, security choices are often built into profiling systems; computer system access is likely to be restricted.

In terms of industry norms, the trade association guidelines attempt to set out standards for data quality. The guidelines state that "[p]ersonal data should be collected by fair and lawful means for a direct marketing purpose" and should only be used for marketing purposes.[111] However, little credence can be given to this pronouncement. The trade association itself opposes limitations on secondary use,[112] and the broadness of the purpose specification frustrates any meaningful standard. All personal information can be used for a marketing purpose.

As for business practice, companies are often not very responsible in setting data quality standards. For example, Fingerhut, a large catalog marketing company, has a privacy policy that says any relevant "information will be used and maintained for marketing purposes."[113] Fingerhut's policy does not require the company's managers to articulate any specific purpose for data collection.

Secondary use of personal information for profiling is widespread in the direct marketing sector. A review of any list catalog, such as the Standard Rate & Data Services catalog, or the trade paper DM News, demonstrates the extent of secondary uses. Profiles of political conservatives,[114] liberals,[115] women who buy wigs,[116] impotent middle-aged men,[117] gamblers,[118] male buyers of fashion underwear,[119] and

---

108. Telephone interview with Mary E. Doher, Metromail (July 26, 1994), confirmed in Letter from Joel R. Reidenberg to Mary E. Doher (Aug. 16, 1994) (on file with the University of Iowa College of Law library).

109. This is a process whereby decoy names are used to determine if a profile is being used in accordance with the list rental or sale agreement.

110. *See* John Verity, Silicon and Software that Mine for Gold, Bus. Wk., Sept. 5, 1994, at 62.

111. DMA Guidelines, supra note 62, arts. 1, 5.

112. *See, e.g.*, Direct Marketing Ass'n, Grassroots Advocacy Guide for Direct Marketers 50 (1993) (suggesting ways for direct marketers to oppose legislative proposals that would prohibit secondary uses of credit information for marketing purposes).

113. Fingerhut Companies, Inc., Consumer Privacy Guidelines, art. 1.

114. *See* Conservative Business File Names Community Leaders, DM News, May 23, 1994, at 44.

115. *See* American List Counsel, Inc. Advertisement, DM News, Dec. 26, 1994, at 11.

116. RMI Direct Marketing, Inc. Advertisement, DM News, Mar. 20, 1995, at 17.

117. *See* Just Lists Offers "Male Potency" File, DM News, Apr. 19, 1993, at 37.

buyers of "skimpy swimwear and related items such as clingy short dresses and skirts,"[120] are just a few examples of the profiles being developed.

Similarly, companies do not seem to pay attention to the other benchmarks of data quality. The relevance standard poses problems for the direct marketing industry. Any information can be included in some form of profile at a later date, and companies, such as Reader's Digest, even collect information about nonresponses to solicitations. Major industry players ignore the benchmarks offering individuals access to personal information held by companies. For example, Metromail does not provide access to personal information to the concerned individuals[121] despite its history of membership on the DMA Privacy Task Force, a group dedicated to promoting fair information practices within the trade association, and the company's purported adherence to the DMA Guidelines. Typical responses from companies when faced with a request for access to profile information is "it's proprietary" or "we won't tell you."[122]

In contrast, there are instances when company policies include practices covered by the core elements of data quality. This rare case occurs most often for security. Direct marketing companies typically include standards for security practices to protect their commercial interests.[123]

---

118. Dunhill Unveils Casino Gamblers, DM News, May 23, 1994, at 48; National List Exchange Advertisement, id. at 40.

119. Brawn of California Offers Three Lists, DM News, Apr. 5, 1993, at 34.

120. Sunup Sundown Available from TCI List Management, DM News, Dec. 20, 1993, at 27.

121. The DMA Guidelines call for access to personal information held by direct marketers. DMA Guidelines, supra note 62, art. 5. *Compare* Letter from Mary E. Doher, Metromail, to Joel R. Reidenberg (Aug. 10, 1994) *with* Letter from Joel R. Reidenberg to Mary E. Doher (Aug. 16, 1994) (both on file with the University of Iowa College of Law library). Initially, Metromail ignored the follow-up request for adequate and accurate disclosure of the personal information. Subsequent to mention of this practice at the Annenberg Conference, Metromail offered a dubious explanation. *See* Letter from Thomas E. Hiller, Vice President, Metromail, to Joel R. Reidenberg (Oct. 17, 1994) (explaining that Metromail sold public record information, but that Metromail did not provide the information on request to the individual concerned in order to protect the person's privacy) (on file with the University of Iowa College of Law library). Metromail provided a catalog of consumer lists, marked to show the lists containing the requestor's personal information, as a full disclosure. Id. The catalog does not include all the consumer lists that Metromail sells, however, and thus cannot be an accurate response to the request for access.

122. *See, e.g.*, Letter from Susan Coe Heitsch, Vice President, First Card, to Joel R. Reidenberg (May 10, 1993) ("[Y]our name was obtained from one of the mailing lists which we purchased. Both the source of this list and the credit criteria which qualified you . . . are proprietary in nature, and for this reason, I am unwilling to disclose this information.") (on file with the University of Iowa College of Law library).

123. For example, Fingerhut's policy notes that "[o]nly those employees needed to carry out the business functions involved may have access to information about any . . . customer." Fingerhut, supra note 113, art. 4.

b. *Profiling and transparency standards*

Standards covering the transparency benchmark are similarly weak for information profiling in the direct marketing industry. Legal rules are virtually nonexistent.[124] Technical arrangements do not deal with notice or consent issues.

The DMA tried to address transparency by creating an industry-wide "opt-out" program.[125] These mail and telephone preference services offered by the DMA strive to suppress mail or telephone solicitations to individuals who have requested not to receive junk mail and junk calls. Because these programs operate after the profiling has taken place, they are not standards for transparency of profiling. Rather they reflect standards for transparency of list exchanges.[126] In any event, the programs are not very successful; individuals are unaware of their existence,[127] and corporate compliance cannot be measured.

In practice, companies frequently fail to provide meaningful notice of information practices. Typical statements on consumer catalogs sent to individuals use language like "[f]rom time to time, companies and organizations ask to send their catalogs and brochures to our customers. . . . we allow it."[128] Other companies, such as American Express, offer "better disclosure."[129] Commonly, companies ask individuals to fill out surveys with the promise of "free savings" or "valuable coupons." These surveys rarely identify the survey organization, the beneficiary, or the intended uses of responses.[130] Metromail, in one recent example, even affirmatively misled individuals as to the nature and purpose of its information gathering.[131] In fairness, however, companies are increasingly

---

124. Only the laws governing cable communications and video privacy protection appear to require any sort of notice for the collection and use of personal information. *See* 18 U.S.C. § 2710 (1988); 47 U.S.C. § 551 (1988).

125. *See* Data Protection, Computers, and Changing Information Practices: Hearings Before the Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations, 101st Cong., 2d Sess. 44 (1990) (statement of Richard A. Barton, Senior Vice President, Direct Marketing Ass'n); DMA Manual, supra note 103.

126. They offer notice that profiles will be sold to others and provide a means for individuals to prevent such sales. The opt-out programs by their very nature do not address notice for the profiling activities themselves.

127. Mary J. Culnan, Consumer Attitudes Toward Secondary Information Use, Privacy, and Name Removal: Implications for Direct Marketing, Paper presented at Symposium on Consumer Privacy, Chicago/Midwest Direct Marketing Days (Jan. 20, 1993) (revised manuscript on file with the University of Iowa College of Law library).

128. Fingerhut Corp., Catalog Payment Chart (on file with the University of Iowa College of Law library).

129. American Express discloses annually: "[W]e develop mailing lists based on information you provided to us on your initial application and in surveys, information derived from how you use the Card that may indicate purchasing preferences and lifestyle, as well as information available from external sources." American Express, supra note 63.

130. *See, e.g.*, Survey Savings Form (on file with the University of Iowa School of Law library).

131. *See* R R Donnelley Unit Faces FTC Scrutiny over Phone Survey, Wall St. J., Dec. 29,

offering individuals the ability to opt out of future use of personal information for marketing profiles.

c. *Profiling and sensitive information*

The commonly accepted benchmark standards for the treatment of sensitive personal information are virtually nonexistent in the context of profiling. Health information, for example, has few applicable legal protections.[132] Aside from rare state statutes limiting insurance information and marketing profiles,[133] state tort law, in theory, imposes legal rules for profiling sensitive information. The tort protecting against the public disclosure of private facts ostensibly covers the treatment of sensitive information. However, a basic element of the tort is the wide dissemination of personal information.[134] This makes tort claims hard to sustain for typical disclosures in the marketing context; the disclosures are often between two companies.[135] Additionally, few technical protections in the profiling systems would appear to offer special safeguards for sensitive information.[136]

Industry norms and business practice similarly ignore standards for sensitive data. For example, the DMA Guidelines do not even mention sensitive data.[137] In fact, the DMA Guidelines can even be read to approve of weaker standards for sensitive information than for ordinary personal information. The guidelines define personal data as "[i]nformation which is linked to an individual . . . and which is not publicly available or observable"[138] and, thus, exclude "public" information from any protection. Since data such as race and physical handicaps are readily observable, they would not qualify for the narrow protections of

---

1994, at C10.

132. *See* The Fair Health Information Practices Act of 1994: Hearings on H.R. 4077 Before the House Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations, 103d Cong., 2d Sess. 358 (1994) (statement of Paul Schwartz, Associate Professor, University of Arkansas-Fayetteville Law Center); Office of Technology Assessment, U.S. Congress, Protecting Privacy in Computerized Medical Information (1993); Robert M. Gellman, Prescribing Privacy: The Uncertain Role of Physician in the Protection of Patient Privacy, 62 N.C. L. Rev. 255 (1984) (arguing existing ethical and legal standards inadequately aid physicians protecting patient confidentiality); Paul M. Schwartz, The Protection of Privacy in Health Care Reform, 48 Vand. L. Rev. 295 (1995).

133. *See, e.g.*, Mass. Gen. L. ch. 175I (1992) (regulating the collection of information for insurance purposes).

134. *See* Polin v. Dun & Bradstreet, Inc., 768 F.2d 1204, 1206-07 (10th Cir. 1985) (holding that distribution to small group of recipients does not qualify for the tort).

135. Recently, courts have found, however, special protection for the disclosure of HIV diagnoses. *See* Estate of Behringer v. Medical Ctr. at Princeton, 592 A.2d 1251 (N.J. Super. Ct. Law Div. 1991); Award in HIV Disclosure, N.Y. Times, May 11, 1994, at A23 [hereinafter Sullivan v. Delta Airlines].

136. *See* Berry et al., supra note 97, at 56-57, 60 (describing database marketing systems).

137. *See* DMA Guidelines, supra note 62.

138. Id. at 2.

the DMA Guidelines.

Companies themselves seem to reject higher standards and treat sensitive data as the key to valuable profiles. TRW, for example, sells ethnic lists that can be segmented with detailed demographic information (e.g., age, income, and marital status).[139] Claritas offers a profiling product that "makes it easy to keep up with the Joneses . . . as well as the Johnsons, the Francos, the Garcias, the Wongs and all the others,"[140] and Metaxa found its niche profiling Greeks who drink liquor.[141] Profiles of political opinions and sexual orientation are also readily available. One company boasts: "Gay men and lesbians . . . . we've got the lists . . . . [s]electable by . . . zip, sex, gift amount [donors to gay causes] . . . . They're yours."[142]

Health information is similarly exempt from special consideration in the context of profiling. Johnson & Johnson profiled 5 million incontinent, elderly women and said the activity was "consistent with current direct marketing industry practices."[143] Metromail, a one-time member of the DMA Privacy Task Force, profiled millions of Americans with specific health conditions (i.e., allergies, bleeding gums, and epilepsy) and said, "We feel this data is less suspect in terms of privacy than other data."[144]

d. Profiling and standards enforcement

In the context of direct marketing and profiling, the enforceability of fair information practices for profiling is limited. The absence of legal rules translates into an absence of legal recourse for individuals facing unfair information practices. Contractual remedies are only available to businesses that are party to a profiling contract and could only rarely be available to individuals.[145] Industry norms and business practice are also extremely weak on remedies for individuals. The DMA and its Ethics Committee offer very limited industry oversight. Unfortunately, the Ethics Committee is not an independent oversight authority charged with properly balancing standards for information practice. It has rarely sanctioned members for unfair information practices, and it can have little credibility when members of the DMA Privacy Task Force itself ignore the DMA Guidelines.[146]

---

139. TRW Target Marketing Servs., Ethnic Markets Consumer Database (Fall 1992).

140. Claritas Advertisement, DM News, May 23, 1994, at 26.

141. Jerrold Ballinger, Metaxa to Roll Out Mailing Effort to Greek-Americans by End of Year, DM News, Mar. 1, 1993, at 2.

142. Letter from Strubb Media Group, Inc. to Direct Marketers (on file with the University of Iowa College of Law library).

143. Larry Tye, List-Makers Draw a Bead on Many, Boston Globe, Sept. 6, 1993, at 12.

144. Ray Schultz, Carlson, Metromail Offer Medical Data, DM News, June 21, 1993, at 1.

145. Individuals can assert contract remedies only if the agreement between the contracting businesses specifically provides for individual recourse or if the individuals are third party beneficiaries.

146. *See* Paul M. Alberta, DMA Suspends Direct American, DM News, July 19, 1993, at 1.

2. *Employment*

Employment is critical to a healthy economy, and significant amounts of personal information are critical to support employment relationships. During the last twenty years, the American workplace has undergone a substantive information revolution. The impact of information technology on business decision making and increasing federal and state governmental regulation of employment require employers to obtain and maintain more employee personal information.[147]

Personnel record keeping is a vital activity in the labor market. Employers must use personal information for basic management activities including hiring, payroll processing, performance evaluations, and promotion decisions. Standards for the treatment of personal information must strike a difficult balance between employer needs for a productive and safe work environment and employee rights to privacy.[148]

The treatment of personnel records generally addresses the commonly accepted benchmark standards. Legal rules, industry norms, business practice, and computer system architecture all exist to protect the treatment of personal information in the employment context. There are direct state laws governing information practices in the workplace and indirect rules arising as a result of other labor laws, such as the Labor Management Standards Act, the Employee Retirement Income Security Act, and the antidiscrimination laws. Information systems establish structural separations between the personnel department and other divisions of companies, and corporate policies also exist to go beyond the other norms.

a. Personnel records and data quality standards

The benchmark standards for data quality are met to a certain degree in the context of the treatment of personnel records. Legal rules require purpose specifications for the collection of some personal information.[149]

This is the only case publicly reported in the trade industry newspaper over the last several years. Significantly, even founding members of the DMA Privacy Task force do not seem to take the trade association's commitment to fair information practices seriously. *See* Robin Smith, DMA Privacy Task Force Works for Self-Regulation, DM News, Feb. 1, 1993, at 36 (responding in a letter to the editor to an article written by Rob Jackson of Donnelley Marketing on privacy and marketing databases: "[W]hat distresses me is that Mr. Jackson appears to be totally unaware of the work of the Direct Marketing Association's privacy task force, made up of industry leaders including, as a founding member, John Cleary, president of Donnelley Marketing.").

147. *See* David Linowes, Privacy in America 24 (1989) (arguing that personal privacy is being invaded by employers who are required by law to obtain personal information).

148. *See* Frank J. Cavico, Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects, 30 Hous. L. Rev. 1263, 1266 (1993).

149. *See e.g.*, 29 U.S.C. § 211(c) (1988) (prescribing the information that employers must collect and maintain for payroll purposes); N.J. Stat. Ann. § 34:11-56a20 (West Supp. 1994);

Legal rules, in a few states, indirectly limit secondary uses of personal information through the imposition of restraints on the disclosure of personnel records.[150] They also impose relevancy with limitations on the collection of certain types of unnecessary information for personnel records.[151] Finally, legal rules in a number of states assure accuracy by providing employees with statutory rights of access to their records and statutory rights of correction for inaccurate information, in addition to common-law duties.[152]

Additional benchmark standards for data quality are set in computer system structure. Technical decisions often set company standards for information retention. Large corporations, for example, establish record system retention policies in order to limit the sheer size of archival records.[153] As an illustration, IBM updates its files regularly and deletes stale data on an identified schedule.[154]

Industry norms and business practice can similarly offer important purpose specifications and limitations on secondary use through data security programs.[155] Fears of discrimination lawsuits and "smoking guns" constrain employers from seeking overly extensive or sensitive personal information without strong reasons.[156] Company policies routinely give employees access to their personnel files.[157] In addition, business practice often includes security for employment records to prevent unauthorized

---

N.Y. Lab. Law § 679 (McKinney 1988).

150. *See* Cal. Lab. Code § 1198.5 (West Supp. 1995); Conn. Gen. Stat. § 31-128f (1993); Ill. Comp. Stat. ch. 820, §§ 40/1-40/13 (1992); Mass. Gen. L. ch. 149:52C (1992).

151. *See* 42 U.S.C. § 12112(d) (Supp. II 1991) (prohibiting collection of job applicant's medical information if not specifically related to job performance); Conn. Gen. Stat. Ann. § 31-51i (West 1994) (imposing restrictions on use of information about arrest record of job applicant obtained from application form); Ill. Comp. Stat. ch. 820, § 40/9 (1992) (prohibiting collection of certain information of employees' nonemployment activities); Md. Code Ann. Lab. & Empl. §§ 3-701, 3-702 (Michie 1991 & Supp. 1994) (prohibiting collection of certain psychological information); N.Y. Exec. Law § 296(1)(d) (McKinney 1993) (restricting employers from requesting certain information from job applicants); *see also* Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77 (Cal. Ct. App. 1991) (holding that employer may not collect information related to employee's religious beliefs or sexual orientation), *rev. dismissed*, 862 P.2d 148 (Cal. 1993).

152. *See e.g.*, Cal. Lab. Code § 1198.5 (West Supp. 1995); Del. Code Ann. tit. 19, § 732 (Supp. 1994); Me. Rev. Stat. Ann. tit. 26, § 631 (West Supp. 1994); N.H. Rev. Stat. Ann. § 275:56 (1987); Bulkin v. Western Kraft E., Inc., 422 F. Supp. 437, 442-45 (E.D. Pa. 1976) (imposing common-law duty for employer to keep accurate personnel records).

153. *See* Richard D. Williams, Corporate Policies for Creation and Retention of Documents (PLI Litig. & Admin. Practice Course Handbook Series No. 332, 1987).

154. David F. Linowes & Ray C. Spencer, Privacy: The Workplace Issue of the '90s, 23 J. Marshall L. Rev. 591, 619 (1990).

155. *See* Linowes, supra note 147, at 30 (noting that IBM, for example, restricts access to personal information on a need-to-know basis for employment purposes, thus minimizing secondary use possibilities).

156. *See* Steven C. Kahn et al., Personnel Director's Legal Guide ¶¶ 2.04[3], 9.01 (2d ed. 1990).

157. Eighty-seven percent of U.S. companies were reported to provide access. Linowes & Spencer, supra note 154, at 594.

access or tampering.[158]

b. *Personnel records and transparency standards*

The benchmarks for transparency are not emphasized in the context of personnel record keeping. Legal rules create few obligations for companies to provide employees with notice and consent for the treatment of personal information.[159] Indirect standards from tort law, however, offer some transparency.[160] Defamation cases provided companies with an incentive to obtain employee consent before disseminating personnel records.[161] Yet, technical systems for personnel records are not configured to emphasize notice or consent.

Industry norms and business practice have not implemented the benchmark transparency standards. The majority of U.S. companies do not inform employees of the types of personal information that is collected, the purposes for the data collection, or the intended disclosures of personal information.[162] A significant minority of companies do, however, have policies to inform employees of personnel record practices.[163] These larger companies usually inform employees through general purpose employee handbooks that are part of a personnel department's new employee orientation program. Typically, companies will also request authorization from employees prior to disclosing personnel information to third parties.[164]

c. *Personnel records and standards for sensitive information*

Like the benchmark, standards for personnel records offer some special treatment for sensitive data. Labor laws and employment discrimination rules limit the types of sensitive information that employers may collect.[165] A tort against public disclosure of private facts, available

158. U.S. Council for Int'l Business, Statement on Examples of Privacy and Data Protection Codes of Conduct in Use in the United States 7 (1991) [hereinafter U.S. Council].

159. If an employer wishes to make an "investigative consumer report" on an employee or prospective employee, the person must be notified and, in the case of state law, may be required to consent. *See* 15 U.S.C. § 1681 (1988) (requiring notice); N.Y. Gen. Bus. Law § 380-c (McKinney 1984 & Supp. 1995) (requiring employee consent).

160. Tort damages such as those awarded in Sigal Constr. Corp. v. Stanbury, 586 A.2d 1204 (D.C. 1991), and O'Brien v. Papa Gino's of Am., Inc., 780 F.2d 1067 (1st Cir. 1986), have led to corporate fears of liability for the disclosure of personal information without consent. *See* Kahn et al., supra note 156, ¶ 7.03[4][c]; David Grant, Giving a Reference: Just Name, Rank, and Salary History?, Legal Times, Nov. 30, 1987, at 16.

161. Yet, even this protection is fading. *See* Richard C. Reuben, Employment Lawyers Rethink Advice, A.B.A. J., June 1994, at 32.

162. Linowes & Spencer, supra note 154, at 594.

163. *See* Linowes, supra note 147, at 41 (introducing results of a nationwide survey on the privacy policies of Fortune 500 companies).

164. Id. at 42.

165. *See* 42 U.S.C. § 12112(d) (Supp. II 1991) (prohibiting the collection of health data

under state common law, also affords special protection to sensitive data and has particular application in the workplace. Usually, the tort requires a wide dissemination of sensitive information;[166] however, courts have relaxed the requirement of broad public dissemination for disclosures in the workplace.[167]

Company practices frequently make secondary use of sensitive information for decisions related to an employee, and few companies inform employees of the practice.[168] Health information is particularly problematic. Corporate "wellness" programs often collect sensitive information about employees, ostensibly for the purpose of promoting good health and reducing company insurance costs, and then make secondary use of such information for decisions about the employees.[169] Some companies do set up contractual arrangements that better protect sensitive employee data. For example, IBM arranges claim submission to bypass corporate information systems in order to secure greater confidentiality.[170] Other companies, such as self-insured businesses, may not seek such special protection for employee health data.[171]

d. Personnel records and enforcement standards

Standards for the enforceability of fair information practices do exist, to some extent, for personnel records. Remedies are available for breaches of statutory rights. Tort law also offers some possibility for remedies benefiting aggrieved individuals. Business practices do not, however, afford individuals direct redress, though violations of company policies may result in the company sanctioning an offending agent.

Standards for supervision are more widespread. Federal and state

---

unrelated to job functions); Hanlon & Wilson, Co. v. NLRB, 738 F.2d 606, 613 (3d Cir. 1984) (interpreting 29 U.S.C. § 150(8)(a)(1) to prohibit employers from collecting information about the union activities of employees); 29 C.F.R. § 1630.14 (1994) (restricting use of medical information obtained as part of an entry physical). Compliance with affirmative action programs requires the collection of personal information about sex, race, ethnic classification, and handicaps; however, the use of such information is restricted. *See* 29 C.F.R. § 1602.7 (1994) (requiring reporting on Equal Employment Opportunity Comm'n, Standard Form 100).

166. *See* Restatement (Second) of Torts, § 652D cmt. a (1977); Prosser, supra note 35, at 393.

167. *See, e.g.*, Levias v. United Airlines, 500 N.E.2d 370, 373 (Ohio Ct. App. 1985) (holding employer was not allowed to disclose medical information without employee's consent); Sullivan v. Delta Airlines, supra note 135 (finding that employer invaded employee's privacy by placing his name on list of employees suspected of HIV infection).

168. Linowes & Spencer, supra note 154, at 594 (stating that the majority of corporations do not inform employees of the types of personal records that are maintained, how they are used, and corporate disclosure practices).

169. *See* Ellen E. Schultz, Open Secrets: Medical Data Gathered by Firms Can Prove Less Than Confidential, Wall St. J., May 18, 1994, at A1.

170. *See* Linowes & Spencer, supra note 154, at 612.

171. *See* Who's Reading Your Medical Records? Consumer Rep., Oct. 1994, at 628, 632.

agencies have oversight for labor practices and jurisdiction to consider the treatment of personnel records.[172] Industry norms and business practice impose standards for periodic company review of employment record systems.[173] Additionally, corporate policies may have a grievance procedure for employees to complain about the treatment of personnel records.[174]

C. *The Assessment of Standards in Key Contexts*

The search for standards in the United States that enshrine the commonly accepted benchmarks for treatment of personal information yields a surprising, and disappointing, result. Dispersed sources in a robust marketplace should, in theory, lead to the development of a complete and tailored set of standards for particular contexts. Instead, the sheer complexity of finding standards hinders both a clear understanding of private sector practice and the implementation of benchmarks. Citizens are at a loss to understand the treatment of personal information because of the multilayered approach to standards, and most corporate managers generally do not want to be innovators on fair information practice standards.[175]

The private sector reception of the benchmarks has been mixed. Data quality standards of access and correction are stronger than standards of data collection and secondary use. At the same time, transparency standards, sensitive data standards, and enforcement standards are weak. The greater focus on access and correction underlies a bias in American regulation to focus principally on the market process and to lose sight of the inherent substance or quality of the "marketplace of ideas."

The U.S. standards-setting approach also defies current industry practices. The narrow, dispersed approach assumes that the processing of personal information will be limited to one context within a particular industry or company. Today, companies' information practices challenge this sectoral thinking because there is widespread, cross-sectoral use of personal information.[176] For example, data collected to execute a

---

172. For example, the federal Department of Labor, Equal Employment Opportunity Commission, Occupational Safety and Health Administration, and their respective state counterparts each have supervisory roles with respect to specific aspects of personnel record keeping.

173. *See* Linowes & Spencer, supra note 154, at 596 (discussing corporate policies).

174. Sanctions may be available under grievance procedures to punish the offender within the corporate structure, but are generally not available to afford direct redress to the aggrieved employee.

175. *See* Louis Harris & Assocs., Inc., Privacy & American Business Survey of Interactive Services, Consumers, and Privacy, at xii (1994) [hereinafter Privacy & American Business Survey] (reporting that 78% of Americans believe they have lost control of how personal information is circulated and used by companies); Louis Harris & Assocs., Inc. & Alan F. Westin, The Equifax Report on Consumers in the Information Age 98 (1990) (reporting that few companies initiate privacy reviews); Smith, supra note 60, at 90-93.

176. *See* Joel R. Reidenberg, Information Flows on the Global *Infobahn*, *in* The New

payment transaction now has utility for marketing profiles and may be used by third parties outside the financial sector.

The search for U.S. standards ultimately reveals important shortcomings in the treatment of personal information in the American private sector. Specifically, there is a lack of transparency for the treatment of personal information, abundant secondary use of personal information, weak enforcement of fair information practice standards, and a misallocation of standard-setting responsibilities.

1. Opaque Transparency

The hallmark of fair information practices is the ability of individuals to participate meaningfully in society's information flows. The existence and extent of information processing must be public for individuals to have these opportunities. In key private sector contexts, notice to individuals and consent, if necessary, for the treatment of personal information are deficient.[177]

Private sector companies often display an unusual degree of hubris in justifying the failure to provide transparency. Companies believe that personal information should be open to the company, but that the concerned individuals have no right to know what the company is doing.[178] The private sector also takes the position that the use of personal information is in the best interests of consumers, yet companies simultaneously deny consumers the opportunity to judge this for themselves.

The lack of transparency has an even greater negative significance on the development of other standards through business practice. Nontransparency blocks the evolution of dispersed standards. Transparency forces companies to review their data quality and sensitive data practices. Similarly, transparency necessitates broader, internal company polices in order to inform individuals of the company practices. Transparency brings public pressure to promote better standards of data quality. Without the public scrutiny that transparency allows, companies do not feel compelled to justify their information practices. When unjustifiable information practices are transparent, public outrage can lead to prompt and appropriate legislative action.[179]

The lack of transparency further poses a fundamental challenge to interactive technologies. On an information highway, "lurkers," "slurpers," and "snoopers" abound. Lurkers monitor information flows over the

---

Information Infrastructure: Strategies for U.S. Policy (William J. Drake ed., forthcoming 1995).

177. *See* supra notes 124-31, 159-64 and accompanying text.

178. *See* Letter from Susan Coe Heitsch, supra note 122 (stating that treatment of personal information is proprietary to the company).

179. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710 (1988) (protection accorded to video rental records resulted from release of Judge Bork's viewing habits during his ill-fated nomination to the Supreme Court).

network hidden from public view. Slurpers assemble and collate information from multiple sources. Snoopers obtain information from unsuspecting sources. Transparency is necessary to make these players visible and distinguishable so that individuals or other suppliers of personal information can have effective participation in all aspects of network information flows.

2. *Secondary Use*

The benchmark standards for fair information practices place considerable value on "finality." This is the principle that information obtained for one purpose should not be used for other purposes without consent from the individual concerned. As seen in the direct marketing and employment contexts, secondary use is a problem in the U.S. private sector, particularly with respect to marketing applications.[180]

The problem of secondary use is accentuated for sensitive information.[181] An enormous commercial market exists, for example, in secondary use of health information.[182] Interactive technology now also allows isolated bits of personal information to be amassed and profiled to create "new" sensitive data. For example, it is easy to construct a list of married Catholics with small families who support abortion.[183]

The fragmented sources for American standards for the treatment of personal information invite a permanent problem for secondary use. Personal information gathered in one context has value for other uses. There will be unrelenting pressure for companies to re-use personal information in a secondary fashion.[184] Without effective transparency, companies have unfettered discretion to determine the uses for personal information. This inexorably leads to myopia in how companies characterize information use and how they use data in deviation from the original purposes.[185]

---

180. *See* supra notes 105-07, 112-20, 150, 168-71 and accompanying text.

181. *See* supra notes 112-20, 168-71 and accompanying text.

182. For example, one of the principal rationales offered for the merger between Merck, the large pharmaceutical company, and Medco, one of the nation's largest mail order pharmacies, was to utilize the individual prescription records and purchasing histories contained in Medco's database. *See* Joseph Weber & Rochelle Shoretz, Is This Rx Too Costly for Merck?, Bus. Wk, Aug. 9, 1993, at 28.

183. Planned Parenthood sells its list of donors, and demographic information is widely available to match the list by religion, age, family size, income, and marital status. *See* Craver, Mathews, Smith Awards 16 Files to ALC, DM News, Sept. 13, 1993, at 37 (including list of Planned Parenthood members and donors); Claritas Advertisement, DM News, May 23, 1994, at 26 (the PRIZM 4 offers matching according to family demographics); TRW Target Marketing Servs., supra note 139 (offering ethnic selections).

184. *See* Smith, supra note 60, at 74-80 (describing large databases of consumer information currently used for psychographic marketing).

185. *See* id. at 86-90 (discussing cognitive dissonance even among corporate information system managers).

3. Lightweight Enforcement

Fair information practices must be enforceable in an Information Society. Under the system of targeted standards in the United States, private enforcement is preferred to government sanction. Narrow, targeted standards and the corresponding reliance on self-regulation depend on the market for enforcement of fair information practices.[186] The scarcity of legal rules limits the option of private enforcement. Remedies for citizens and supervision of companies are lacking in key contexts.[187]

In the absence of legal rules, the emphasis on self-regulation poses a threshold obstacle to effective enforcement: companies have little incentive to police themselves. Bad practices can easily be hidden through nontransparency, and organized industry efforts are not serious about enforcement.[188] In addition, there are other formidable obstacles to private enforcement. The cost for an individual to pursue a claim for unfair information practices is prohibitive, and the real harm from unfair information practice is not monetary, but rather dignitary and societal.[189] These are often not covered by the liability provisions of relevant statutes or industry policies.

4. Misallocated Responsibility

The reliance on targeted standards in the U.S. private sector places a preponderant emphasis on voluntary industry norms and business practice. This allocates complete responsibility for standards to the business participants in private sector information exchanges. However, since transparency is missing in key contexts, individuals and society as a whole are ill-equipped to exercise any influence on standards setting. Responsibility for the existence and creation of standards, thus, rests fully on corporations. Yet, the business world shoulders this responsibility for information practice without accountability precisely because so many aspects of business practices are obscured from public view and there are few means of either public or private enforcement.

The haphazard and incomplete character of the existing standards in key contexts demonstrates that the allocation of responsibility to establish fair information practice from dispersed sources has not worked. The objective of tailored standards through an aggregation of dispersed sources cannot realistically be achieved.

---

186. For example, the United States has rejected until now the creation of any regulatory commission to enforce fair information practices.

187. *See* supra notes 145-46, 172-74 and accompanying text.

188. The significance of the DMA Ethics Committee is a good example of this. Despite the skewed treatment of personal information in the direct marketing industry, the Ethics Committee focuses on deceptive advertising and not on fair information practices.

189. An individual must budget at least $150-250 per hour for legal fees. *See* Judy Sarasohn, In Search of Alternatives: Client Pressure Holds Down Fees, Legal Times, Nov. 22, 1993, at 13.

III. THE SUBVERSIVE EFFECT OF TARGETED LEGAL STANDARDS

The evolution of standards for information practices in the private sector poses a paradox for the goals embodied in the pursuit of targeted standards. The noncomprehensive approach to standards seeks to preserve identity and liberty in American democracy.[190] The weak development of benchmark standards in key contexts means that the approach has instead fostered a concentration of economic and political power in American society and has diminished that very identity and liberty cherished by citizens.[191]

More than fifteen years ago, the U.S. Privacy Protection Study Commission identified a number of key sectors that had tremendous impact on the lives of citizens.[192] The Commission worried that treatment of personal information in these sectors corresponded to an obvious potential for the improper coercion of citizens by private sector actors.[193] Even in the most closely regulated of these sectors, namely financial services and telecommunications, the targeted legal protections emphasized minimal restraint on information flows; accuracy protections rather than collection and purpose limitations were predominant.[194]

Over the last decade, there has been a concentration of information power under private control.[195] The commonly accepted benchmarks for fair information practice to preserve citizen participation in the flows of personal information have not emerged through targeted standards. Contrary to the purposes of targeted standards, individuals have lost identity to computer profiles and models and have lost power in society. Targeted standards have created information flows that suffer from intractable inequities and frustrate the very objectives of the narrow and dispersed approach to standards setting in the United States.

A. Failures in the Information Market

The reliance on the marketplace to define standards faces formidable problems. The marketplace does not have a level playing field and contains destructive internal inconsistencies. In this "marketplace" of personal information, the system of targeted standards fails to assure citizens fair

---

190. Identity and liberty are intrinsically linked to the private sector treatment of personal information. *See generally* Fried, supra note 36 (arguing that the right to control the disclosure of personal information to others is part of political and social interchange); Herbert Maisl, État de la législation française et tendences de la jurisprudence relatives à la protection des données personnelles, 39 Revue internationale de droit comparé 559 (1987).

191. *See* infra text accompanying notes 212-35.

192. *See* Privacy Comm'n, supra note 8, at 37-39 (identifying, *inter alia*, the following as key sectors: financial services, direct marketing, employment, health care, government, and education).

193. *See generally* id.

194. *See* Reidenberg, supra note 11, at 210-16.

195. *See* Reidenberg, supra note 176.

participation and treats citizens inequitably.

1. *The Skewed "Marketplace"*

In the absence of the benchmark standards, political weight is greatly skewed in favor of the collectors and manipulators of personal information. At the same time, the reliance on targeted standards allocates to these actors the role of developing industry norms and business practices that require shared decision making with citizens. This presents an inherent conflict of interest. The only way to preserve some semblance of control over the disclosure of personal information in American society is to withdraw entirely and live a hermit's life.

The development of fair information practices through the marketplace faces profound structural problems. Posner has argued that absent any legal protections, the market will efficiently create fair "privacy" or information practice results.[196] This argument depends on the triviality of transaction costs, externalities, and imperfect information.[197] The absence of benchmark standards results, however, in precisely the reverse situation: a marketplace with high transaction costs, important externalities, and a significant level of imperfect information.

Dispersed standards allow transparency of information practices to be obscured. With obscured transparency, citizens face an extraordinary and often insurmountable burden if they even attempt to learn about information practices. Companies control the disclosure of their practices and suffer no penalties for refusing to disclose. In fact, companies may suffer harm if they do disclose their inappropriate practices as a result of negative backlashes.[198] Industry norms and practice preclude citizen involvement in the circulation of personal information. Without notice, consent, and access, it is impossible for an individual even to discover how, where, when, and why personal information is circulating. In economic terms, this obscured transparency raises transaction costs and allocates them to citizens.

There is also an external effect from the circulation of personal information without direct citizen participation. The failure to include citizens in the information decision-making process affects political and

196. *See generally* Richard A. Posner, The Right of Privacy, 12 Ga. L. Rev. 393 (1978) (arguing that individuals should not have protection for personal information because such protection would distort efficient market functions).

197. *See* George J. Stigler, The Citizen and the State: Essays on Regulation 104-07 (1975) (arguing that these points must be minimal for the market to function effectively). Posner assumed transaction costs would be low when individuals are assigned no rights by the state. Posner, supra note 196, at 398. He minimized the externalities, or social cost, of limited protection for individuals and bypassed the question of perfect or imperfect information. Id. at 412-13. Interestingly, Posner also argued for protection against eavesdropping and surveillance because the transaction costs for eavesdropping would be greater if the individual has no protection. Id. at 401. Fair information practice standards seek to provide exactly that: protection against surveillance.

198. *See* Smith, supra note 60, at 85-93.

social interchange.[199] Society as a whole is altered by the treatment of personal information without fair information practice standards. Distinctions between public and private activity disintegrate and social dynamics change as informational power shifts.

The weak standards for the accuracy of circulating personal information create a two-way condition of "imperfect information." The lack of participation by individuals in the market of circulating information prevents business from obtaining the best information for decision making.[200] Business is often unable to correct errors in circulating personal information because the problems may only be discovered by the concerned individuals.[201] Citizens also face imperfect information. Because customized products, services, and advertising are developed based upon information profiles, a citizen's vision of society is increasingly narrowed. The greater reliance citizens place on interactive services for daily life, including news, shopping, and household finance, the more citizens lose a broad view of the Information Society.[202]

2. *Self-Destructing Targets*

The system of targeted standards has become self-destructive for the U.S. private sector. The lack of fair information practices produces costly embarrassment to companies.[203] In rare instances of transparency, public pressure and congressional interest have forced companies to abandon or modify products after development.[204]

The narrow focus of targeted standards and the absence of benchmarks for fair information practice intensify internal conflicts for many large companies in their treatment of personal information.[205]

---

199. *See generally* Westin, supra note 5; Fried, supra note 36.

200. One recent audit of consumer profile lists in the direct marketing industry found surprising levels of inaccuracy. Ray Schultz, List Accuracy Rated in Leo Burnett Audit, DM News, Sept. 19, 1994, at 1 (noting that list accuracy ranged from 21% when profiling income to 95% when profiling home ownership).

201. Id.

202. To regain the broad view of society, citizens must deviate from the norm. Such deviations are likely to involve substantial effort and cost.

203. *See* Reidenberg, supra note 176.

204. *See* Domestic and International Data Protection Issues: Hearings Before the Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations, 102d Cong., 1st Sess. 6 (1991) (statement of John Baker, Senior Vice President, Equifax, discussing the abandoned Lotus-Equifax consumer database); Markey Widens Inquiry: AOL Defends its Privacy Policy on Mail Lists, Comm. Daily, Oct. 11, 1994, at 1 (referring to America Online's new notice policy following embarrassing publicity); Terry Brennan, CADM Releases Its Unanimous Objection to AT&T 800 Directory; Joins Other Industry Leaders, DM News, Oct. 7, 1991, at 1 (discussing the objections to distribution of an AT&T directory of 800 numbers).

205. Various departments within a single organization will have drastically different views on fair information practices for specific personal information. For example, in a financial institution, the marketing group will seek secondary use of account information, while the customer relations group may view transaction records as confidential for billing purposes

Products and product quality in an information economy depend increasingly on a complete set of standards for fair information practice. Incomplete standards and poor standards threaten the future of information-based businesses by jeopardizing the long-term vitality of their products and services.

For the long-term, business is beginning to grasp that better standards for fair information practice can be a competitive advantage and will be necessary for business survival.[206] Yet, companies are generally myopic and only see immediate revenue from the sale of personal information.[207] In the short-run, most companies still affirmatively resist developing standards.[208] Business reluctance to embrace setting standards preserves a destructive process for the development of the Information Society.[209]

B. Frustrating the Justification for Targeted Standards

The targeted standards approach to fair information practices enshrines inequities for citizens in the circulation of personal information. The approach also imposes structural hurdles that business must overcome to improve standards. Those results collectively challenge the underlying justification for the targeted standards approach.

To restrain abuses of power and attempts at thought control, the United States has long resisted government interference with personal

---

only.

206. *See* Dun & Bradstreet, supra note 65; Equifax 1991 Report, supra note 65; Privacy & Am. Bus., Sept./Oct. 1993, at 15 (setting forth Pacific Bell commitment to fair information practices). Two of these prominent examples stem from earlier instances of public embarrassment. Equifax developed a deep commitment to stronger fair information practices following the abandonment of the Lotus-Equifax consumer database. Pacific Bell similarly adopted a fair information practices code following a controversy over its plan to sell subscriber information.

207. Trans Union, for example, sells marketing profiles based upon information contained in its credit reporting databases. While credit reporting is regulated by the Fair Credit Reporting Act, 12 U.S.C. § 1681 (1988), Trans Union's secondary use of the information is inconsistent with benchmark standards of fair information practice. Trans Union's competitors, TRW and Equifax, no longer engage in the same practice. Trans Union, thus, has information products that face no competition. The Federal Trade Commission objects to Trans Union's practice under the Fair Credit Reporting Act and Trans Union is aggressively challenging an FTC order. *See* Trans Union Corp., 59 Fed. Reg. 55,669 (FTC 1994); Washington Regulatory Reporting Assocs., FTC: Watch, No. 426—Credit Reporting (Jan. 16, 1995), *available in* LEXIS, Trade Library, FTCWAT File (stating that United States Court of Appeals for the District of Columbia "stayed an FTC order requiring Trans Union to halt its direct-marketing lists business"). In the event that Trans Union wins its challenge, Congress has expressed interest in prohibiting Trans Union's practice. *See* H.R. 5178, 103d Cong., 2d Sess. (1994); H.R. 1015, 103d Cong., 1st Sess. (1993); S. 783, 103d Cong., 1st Sess. (1993). Despite such opposition, Trans Union makes money in the short run.

208. *See* Smith, supra note 60, at 85-86, 90.

209. *E.g.*, Privacy & American Business Survey, supra note 175 (finding that refusing to develop fair information standards will dissuade potential users of interactive services from participating in network transactions).

rights.[210] Freedom in the circulation of personal information, however, has neither prevented the manipulation of citizens nor supported citizen liberty and the accepted role of the state in economic affairs.[211]

1. Manipulation of Citizens

One of the earliest government studies of computers and society made the profound insight that the concentration of information techniques leads to an imbalance of political power.[212] The ubiquitous availability of extensive information risks the manipulation, molding, and adjustment of individual conduct. The citizen loses power to other actors in society when computer models define individual conduct and when deviations from predicted behavior are questioned.[213] Information traces of individual conduct, such as transaction records from interactive communications, lead to the manipulation of social engagement. Services and products will be offered to the individual based on predictions from these interactive patterns. This has the positive effect of offering consumers information about goods and services that they are likely to find interesting or appealing. At the same time, these selective offerings have the more nefarious consequence of limiting an individual's "information horizon" and stereotyping citizens.

The private sector has precisely the type of dossiers that the public has long feared government would abuse.[214] In many ways, private data files substitute for the lack of state data bases.[215] It is particularly telling that the FBI, with all its surveillance resources, still went to the direct marketing industry to obtain personal information.[216]

At the present time, one important result of the existing limited set of standards is that large corporate interests structure decision making through their hidden control of information flows. Companies both create and enforce information standards without public scrutiny. The effect is subtle, but significant. As interactive communications become ever more crucial to everyday life, goods and services will be offered primarily on the basis of transaction data profiles. What a subscriber has done in the past will dictate what is offered in the future. Such behavioral stereotyping censors the information delivered to the citizen.[217] In addition, the

---

210. *See* supra note 18-54 and accompanying text.

211. Professor Sunstein has argued a similar point. Sunstein, supra note 31, at 197-256.

212. Rapport de la Commission Informatique et Libertés 77 (1975) (report of a French government commission established to consider the impact of computers on freedom and society and to make recommendations for government action).

213. *See* Simitis, supra note 3, at 710-12, 720-24; Hearings, supra note 7, at 61, 69 (statement of Joel R. Reidenberg, Associate Professor, Fordham Univ. School of Law).

214. *See* Linowes, supra note 147, at 156-67.

215. *See* Simitis, supra note 3, at 725.

216. Ray Schultz, FBI Said to Seek Compiled Lists for Use in Its Field Investigations, DM News, Apr. 20, 1992, at 1. Ironically, the marketing industry declined to provide information to the FBI. Ray Schultz, Big Compilers Say No to the FBI, DM News, May 4, 1992, at 1.

217. For example, on the Prodigy network, interactions are profiled and each subscriber

control of these information resources without citizen knowledge empowers corporations to engage in thought control. Without knowledge of the specific commercial sources of personal information or the basis for particular profiles, citizens cannot effectively evaluate alternatives.[218]

Critiques of recent Supreme Court privacy jurisprudence highlight an important shift and a growing concern for protection against the manipulation of citizens.[219] The "old privacy" doctrine sought to protect against government surveillance of citizens such as the intrusion of the police into "marital bedrooms for telltale signs of the use of contraceptives."[220] The "new privacy" doctrine seeks to protect citizens from coercive choices about how to live their lives, such as a state ban on a woman's right to choose.[221] This evolution shifts the conception of abuse of power from fear of surveillance to fear of control of thought and social interaction. A similar potential abuse now emanates from private use of personal information.

The concept that private control of information flows risks significant potential for citizen manipulation is not new. There is a unique strand in U.S. telecommunications policy that seeks to harness private sector control of information flows as a means to manipulate citizens. For example, the fairness doctrine requires private broadcast stations to air opposing points of view,[222] and the "must carry" doctrine requires private cable television companies to offer public service channels.[223] In *Red Lion Broadcasting v. FCC*,[224] the Supreme Court upheld the fairness rule in order to protect the public's right of access to free thought. The Court said: "It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail, rather than to countenance monopolization of that market, whether it be by the Government itself or a private licensee."[225] More recently, in *Turner Broadcasting v. FCC*,[226] the Supreme Court similarly upheld the "must carry" rule because the "basic tenet of national communications policy that 'the widest possible

---

sees a customized set of product advertisements based on the profile. The subscriber is thus cut off from other product information.

218. *See generally* C. Edwin Baker, Advertising a Democratic Press, 140 U. Pa. L. Rev. 2097 (1992) (discussing manipulative effects of advertising).

219. *See* Sandel, supra note 21, at 525 (arguing that "old" privacy rhetoric emphasizes protection from surveillance and "new" privacy rests on protection for particular forms of conduct). *See generally* Rubenfeld, supra note 22 (arguing that privacy rights must restrain the government from dictating choices about citizen conduct that are fundamental to individuality).

220. Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965).

221. Roe v. Wade, 410 U.S. 113 (1973).

222. Communications Act of 1934, 47 U.S.C. §§ 151-613 (1988 & Supp. V 1993).

223. Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521-559 (1988 & Supp. V 1993).

224. 395 U.S. 367 (1969).

225. Id. at 390.

226. 114 S. Ct. 2445 (1994).

dissemination of information from diverse and antagonistic sources is essential to the welfare of the public.'"[227] Under this jurisprudence, standards for public participation in information flows are critical to avoiding citizen manipulation. The lack of standards for fair information practice in the private sector prevents precisely the type of participation that the Court deems essential to the welfare of the public.

2. *The Reversal of Liberty*

The market failure and the shift in information power reverses the evolution of the concept of liberty and the role of the state that took place in the United States between the nineteenth and twentieth centuries. Modern liberty for citizens requires an ability to participate in flows of personal information, if not the ability to exercise control over those flows.[228] Early America viewed personal information as private, and significant efforts were made to limit the amount of personal information in the public realm.[229] The more colonialists adapted to New World conditions and found open space, the more protective they became of solitude and isolation from others.[230] In the congested urban centers of the industrial age, the same sense of isolation or solitude could be found in "protective anonymity."[231] An individual could be in a public place, yet still seek or assume freedom from personal identification.[232]

The search for solitude and protective anonymity meant that citizens had full participatory power in the circulation of personal information. Citizens acquired an important liberty through the exercise of control over flows of personal information. Nineteenth century U.S. courts gradually enshrined the notion of inviolable physical and mental space.[233] The state, through the increase of citizen rights, promoted such liberty. The First Amendment grew to secure information flows in support of the process for democratic political judgments and the respect for polity.[234] The First Amendment promoted liberty for individuals as participants in a

227. Id. at 2470 (citations omitted).

228. *See* Glendon, supra note 17, at 52-54 (noting the American development of privacy as an extension of liberty); Westin, supra note 5, at 7 (stating that privacy is the complete control by individuals in determining the disclosure of personal information to others); Fried, supra note 36, at 493 (stating that privacy consists of the right of individuals to define themselves for others); Miller, supra note 10, at 1107 (stating that privacy entails the control of the flow of information about individuals); Simitis, supra note 3, at 232-37 (arguing that data protection is necessary for citizens to participate in democracy).

229. *See* Note, The Right to Privacy in Nineteenth Century America, 94 Harv. L. Rev. 1892, 1895-96, 1900-01 (1981) (discussing emergence of right to exclude others from private property and the right to control the disclosure of private communications).

230. *See* David Flaherty, Privacy in Colonial New England, 26 (1972).

231. Richard F. Hixson, Privacy in a Public Society 9 (1987).

232. *See* Westin, supra note 5, at 31-32.

233. *See* Note, supra note 229, at 1895-96, 1900-01.

234. *See* Sunstein, supra note 31, at 220; *see also* Mark Tushnet, An Essay on Rights, 62 Tex. L. Rev. 1387 (1984).

democratic society as distinct from the notion of liberty for individuals to make private consumption choices.[235]

Today, with targeted standards and the corresponding treatment of personal information, citizen liberty resembles the early colonial experience without any of the developments over the centuries. The combination of current technology and existing targeted standards erode protective anonymity. "Information traces" destroy anonymity. Individuals perceive transactions in public places, such as the purchase of groceries at the supermarket or books at the bookstore, as anonymous activities, yet information records collected and maintained by store computer systems enable these activities to be personalized. Stores and other third parties can link specific transactions to individuals. Citizens no longer have the freedom to choose the terms of personal information disclosure and consequently have lost the capacity to participate in decisions about societal information flows. This denial of participation inherently manipulates citizens; liberty for the control of personal information reverts back in time.

3. Usurping the State

The transfer to business of control of personal information flows, coupled with continued dispersion of standards for fair information practice, usurps the role of the modern American state. After the New Deal, the state became a more active participant in economic affairs, and the courts sought to give greater protection to personal liberties. Following *West Coast Hotel v. Parrish*[236] and *United States v. Carolene Products*,[237] the Supreme Court upheld economic regulation more readily than restrictions on certain fundamental personal freedoms, such as freedom of communication.[238] Ironically, the underpinning of dispersed standards is to preserve personal rights—the freedom from manipulation and abuse of power. Yet, the combination of minimal restraints to protect personal information and of dispersed standards creates broader protection for commercial interests than for individual interests. Business has unchecked discretion to determine the terms and conditions of the circulation of vast amounts of personal information.

The treatment of personal information is actually confused between the two ideologies of economic and personal freedoms. Flows of personal information raise significant commercial stakes while at the same time implicating personal freedoms. Personal information is an economic asset. Accordingly, like other economic assets, the Supreme Court's jurispru-

235. Sunstein, supra note 31, at 220.

236. 300 U.S. 379, 393-94 (1937) (upholding a state minimum wage law).

237. 304 U.S. 144, 152 n. 4 (1938) (suggesting that legislation impinging on personal liberties may be subject to more exacting scrutiny than economic regulations).

238. *See* Glendon, supra note 17, at 4-5; Harry N. Scheiber, Economic Liberty and the Constitution, *in* Essays in the History of Liberty: Seaver Institute Lectures at the Huntington Library 75, 84-86 (1988).

dence on economic regulation should apply. However, because personal information implicates individual rights, courts and society tend to scrutinize regulation and restrictions on the flow of personal information as a limitation on cherished First Amendment freedoms.[239] While the courts give less protection to commercial speech, advertising and commercial messages do enjoy some protection.[240]

The circulation of personal information, however, is not like the traditional commercial speech cases involving advertising or the communication of a commercial message. Restraints on the circulation of personal information would not damage the communication of a message. Rather, the regulation of the treatment of personal information would secure participation by citizens in the communications process. Moreover, in commercial speech cases, courts are willing to uphold regulations if the government can regulate the underlying economic activity.[241]

The continued pursuit of target standards in the face of market failure and frustrated goals abdicates the proper role of the post-New Deal state.[242] The Constitution is not inconsistent with the government securing a more balanced market in information.[243] At the same time, the targeted standards present a classic case for justified economic regulation. Society cannot expect the private sector to self-regulate when the short-term costs of setting high standards is considerable and the significant transaction costs for citizens limits countervailing pressure on companies. Furthermore, citizen manipulation and reductions of liberty cry out for intervention.

IV. THE FOREIGN AID TO A REVIVAL OF DEMOCRATIC VALUES

The U.S. private sector faces serious pressure to rebalance information practices and to restore the values underlying the targeted standards approach. In addition to growing discord within the United

239. *See, e.g.*, Lovgren v. Citizens First Nat'l Bank, 534 N.E.2d 987, 988-91 (Ill. 1989) (suggesting that privacy tort has similar concerns to defamation and First Amendment); Arrington v. New York Times Co., 434 N.E.2d 1319, 1321 (N.Y. 1982) (interpreting New York statute codifying the privacy misappropriation tort to exclude newspaper publication from commercial use under First Amendment reasoning).

240. *See* SEC v. Wall St. Publishing Inst., Inc., 851 F.2d 365, 366 (D.C. Cir. 1988) (explaining that injunction against publication of monthly stock market magazine not prohibited by First Amendment); Towers Fin. Corp. v. Dun & Bradstreet, Inc., 803 F. Supp. 820, 824 (S.D.N.Y. 1992) (allowing a restraining order against the publication of commercial speech); Ohio State Bar Ass'n v. Ohralik, 357 N.E.2d 1097, 1099 (Ohio 1976) (rejecting First Amendment defense by defendant attorney suspended from practice for improper client solicitation).

241. Posadas de P.R. Assocs. v. Tourism Co. of P.R., 478 U.S. 328 (1986) (holding that advertising for gambling could be regulated because the government had the power to regulate gambling itself).

242. *See* Sunstein, supra note 31, at 230 (arguing that the New Deal for speech means regulation to further democratic deliberation and diversity of participation).

243. *See* id. at 256.

States, foreign interest in and concern over U.S. standards is an unusual, but important, force driving a return to the democratic value of protecting citizens against thought manipulation and abuses of power. Unlike the ad hoc, narrowly tailored standards of the United States, foreign standards often offer comprehensive legal norms for the treatment of personal information. Divergent norms among various countries in a global information economy are problematic. Global information processing, thus, requires the U.S. private sector to consider trends in foreign standards of fair information practice.

The original European data protection proposal[244] has served as a wake-up call for information practice standards in the U.S. private sector. The initial business reaction to the proposed directive was loud and negative, but the need to respond galvanized American companies to evaluate their information practice policies.[245] Trade associations began or reinvigorated the process of drafting codes of conduct.[246] Similarly, European interest stimulated scrutiny in U.S. policy-making circles of fair information practice norms. Both legislative and executive branch officials began to evaluate U.S. standards in light of the more comprehensive European principles.[247]

Existing and emerging foreign standards lead to scrutiny of industry norms and business practice.[248] Because offshore data processing may compromise the treatment of personal information, the evaluation of nonlocal standards becomes a regulatory problem. Foreign regulators have expressed specific interest in U.S. private sector standards. The Commission of the European Communities has, for example, sponsored a comparative-law study of U.S. and European data protection.[249] Foreign privacy commissioners have voiced concerns about American standards.[250] Other commissions have prohibited data flows to the United States on the ground of unfair information practices in the United States.[251]

---

244. *See* Original Proposal, supra note 75.

245. *See, e.g.*, U.S. Council, supra note 158.

246. *See, e.g.*, Information Industry Ass'n, supra note 62 (stating that guidelines were developed "to assist companies in their development of policies and practices" following adoption of a 1990 policy statement on privacy).

247. *See, e.g.*, Working Group on Privacy, Information Infrastructure Task Force, Draft Principles for Providing and Using Personal Information, 59 Fed. Reg. 27,206 (1994), *revised by* Working Group on Privacy, Information Infrastructure Task Force, National Information Infrastructure—Draft Principles for Providing and Using Personal Information and Commentary, 60 Fed. Reg. 4362 (1995) (containing an executive branch review of fair information practices and attempt to articulate norms that satisfy international standards); Hearings, supra note 7 (discussing the integrity of telecommunications transmissions and networks and encryption and telecommunications network security).

248. *See* Reidenberg, supra note 56, at 294-96.

249. *See* Paul M. Schwartz & Joel R. Reidenberg, A Study of American Data Protection Law & Practice: Report to the Commission of the European Communities (forthcoming).

250. Private discussions with data protection officials at international meetings, such as the annual Privacy Laws & Business conference at Cambridge University, reveal this concern.

251. *See* U.K. Office of the Data Protection Registrar, Seventh Annual Report 33-34 (1990)

With the disappointing aggregation of standards under the U.S. targeted approach, this scrutiny raises challenges for global information flows. In particular, foreign data protection commissioners can and do seek to assure fair treatment of exported personal information. The weakness in U.S. targeted standards poses an important obstacle for global private sector activities and undermines the U.S. approach to information practice standards. The very search to accommodate global information flows pressures the United States to restore the underlying objectives subverted by the disappointing and unsuccessful targeted standards. American information practices can be connected to foreign standards through narrow comparisons and a reallocation of responsibility for international data flows. A key consequence of any such solution to the problem of international data flows is an increase in citizen participation in the treatment of personal information through reallocation of responsibility and the creation of corporate incentives to support general, rather than targeted, standards. This international influence pushes a reconceptualization of the philosophy of minimal restraints on information flows.

A. Foreign Pressure on U.S Targeted Standards

The foreign pressure to reform U.S. standards has two distinct features. First, foreign legal rules authorize data protection agencies to prohibit the flow of personal information to countries perceived as having insufficient standards of fair information practice.[252] Second, these foreign restraints on transborder data flows undermine the U.S. targeted approach by raising the stakes for U.S. businesses of unsuccessful self-regulation.

1. Precise Restraints on Transborder Data Flows

National laws in many countries already authorize government data protection agencies to prohibit the transfer of personal information if the destination has insufficient privacy standards.[253] In light of these existing provisions, the proposed European directive on data protection was a catalyst for renewed fear regarding restrictions on international data flows. The first version of the proposal contemplated a blacklist of countries with inadequate standards for the fair treatment of personal information.[254] With the targeted standards in the United States, American business

---

[hereinafter Data Protection Registrar] (prohibiting data export to the United States); *see also* Reidenberg, supra note 69, at S162-65 (discussing data export prohibitions).

252. *See* Reidenberg, supra note 69, at S160-65.

253. *See generally* Loi no. 78-17 du 25 janvier 1978, art. 24 (Fr.); Data Protection Act, 1984, § 12(2) (U.K.); Martine Briat, Personal Data and the Free Flow of Information, *in* Freedom of Data Flows and EEC Law (1988); Nugter, supra note 13; Peter Blume, An EEC Policy for Data Protection, 11 Computer L.J. 399 (1992); Michael Kirby, Legal Aspects of Transborder Data Flow, 11 Computer L.J. 233 (1991); Reidenberg, supra note 69, at S137, S160-65 (1992).

254. Original Proposal, supra note 75, art. 24.

thought the European Commission would be obliged to blacklist the United States. The high stakes and inappropriate nature of a general assessment of non-European standards led to a more permissive provision in a revision of the proposal.[255] Following the revised proposal, the Council of Ministers adopted a common position on a new text that compromises between the European Commission's first and second versions. The Council's draft contains an important clause that requires the examination of data transfers outside the European Union and mandates that member states block data flows to countries that the European Commission identifies as "inadequate," yet permits transfers to blacklisted destinations if a case-by-case review can demonstrate that satisfactory standards will be applied in the particular case.[256]

Outside Europe, the proposal has also had a spill-over effect on precise restraints. For example, in Canada, the provincial legislature of Québec enacted a provision that enables the Québec privacy commission to scrutinize private sector data transfers.[257] Similarly, Hong Kong undertook a review of its fair information practices standards through the Law Reform Commission.[258]

In many ways, the proposal masks the real action likely to occur at the national level in Europe. The debate over the course of the proposal seems to have harnessed national authorities. Shortly before the release of the first draft of the proposal, both France and the United Kingdom issued public prohibitions of the export of personal information.[259] Since then, data protection authorities have voiced grave concerns about international data transfers, but have refrained from taking public actions.[260] Once the proposal is finalized, the push toward greater scrutiny of international data transfers is likely to stimulate national data protection agencies with a new European-wide mandate to consider international data flows.

---

255. *See* Amended Proposal, supra note 75, art. 26; Reidenberg, supra note 56, at 293 (arguing that the Original Proposal was actually less likely to result in transfer prohibitions than the Amended Proposal).

256. *See* Common Position, supra note 75, arts. 25-26.

257. *See* An Act respecting the protection of personal information in the private sector, ch. 17, 1993 S.Q. 503 (Can.) (to be codified at R.S.Q. ch. P-39.1) (requiring that the collection, storage, use, or communication of personal information on behalf of another party must conform to the standards established in the law); Paul-André Comeau & André Ouimet, Freedom of Information and Privacy: Québec's Innovative Role in North America, 80 Iowa L. Rev. 651 (1995).

The Québec law also reflects a new commitment to fair information practices found growing around the world. The Québec legislature enacted this most recent data protection law unanimously.

258. Law Reform Comm'n of H.K., Report on Reform of the Law Relating to the Protection of Personal Data (1994).

259. Déliberation no. 89-78 du 11 juillet 1989, *reprinted in* Commission nationale de l'informatique et des libertés, 10e Rapport au president de la République et au Parlement 1989, at 32-34 (1990) [hereinafter CNIL]; Data Protection Registrar, supra note 251, at 33-34.

260. Paul Waterschoot, EC Directive Update, *in* Proceedings of the XVth International Conference of Data Protection & Privacy Commissioners 160 (1993).

2. *Raising the Stakes for Global Business*

Foreign rules that allow data protection agencies to block transfers of personal information to the United States and the growing concern over international data flows raise the stakes for American business and undermine the targeted approach. Foreign data protection regulators will search to make determinations about the sufficiency of U.S. standards. Just as the U.S. standards derive from accepted American beliefs in certain political principles, foreign standards embody the particular democratic values of foreign societies.[261] The scrutiny of U.S. targeted standards requires a way to compare divergent legal rules and to accommodate global information flows without diminishing fair information practices.[262]

Without a full set of legal rules to establish the benchmark standards for fair information practice, context becomes vital to determine the actual standards of practice applied to the treatment of personal information. Because standards arise from dispersed sources in the United States, the actual implementation of fair information practices offers the only appropriate basis to compare U.S. standards to foreign standards. For the comparison to be meaningful, the examination of standards must search for "functional similarity" in specific contexts. If the totality of standards resulting from divergent sources in the United States is functionally similar to the foreign standards for a particular situation, then any restraint on information flows would be entirely unwarranted. This inquiry focuses on the aggregate, substantive standards that are applied to personal information, rather than on the means or sources of norms. Functional similarity allows a comparison of divergent approaches to fair information practice without imposing values from either legal system on the other.[263]

Although narrow comparisons support freer flows of information, the contextual analysis offers precision for the identification of the inconsistencies between actual U.S. standards and the underlying American policy goals. While there are major U.S. businesses that adhere to high standards of fair information practice, the U.S. private sector bears an important and significant burden. Particular companies must define an appropriate evaluation context for foreign regulators and demonstrate that the aggregation of targeted standards in the relevant context is satisfactory. The inconsistency between American standards and underlying values foreshadows significant difficulties for the U.S. private sector in meeting this burden.

The proposal for a European data protection directive reiterates the increased stakes for global businesses. As compared to the original draft of

---

261. *See* Bennett, supra note 4, at 217-19 (discussing the political grounding for differences in privacy regulation).

262. *See* Reidenberg, supra note 69, at S142.

263. *See* Konrad Zweigert & Hein Kotz, 1 Introduction to Comparative Law 30-31 (Tony Weis trans., 2d rev. ed. 1987).

the proposal, the revised version emphasizes context evaluations, rather than overall country assessments.[264] By doing this, the revised draft decreases the political power of lobby groups and reduces political pressure that might have promoted unrestricted information flows despite a lack of relevant standards.[265] As a result, scrutiny of data flows to the United States will need to take place on an ever-increasing micro-level in each of the European member states by the separate national data protection authorities. Because key standards of transparency, finality, and enforcement are often ignored by targeted standards in the United States, the scrutiny on a micro-level of international data processing increases the prospect that European regulators will restrict more data flows if the U.S. private sector does not augment existing standards.

With the lack of key standards in many contexts, U.S. businesses become forced to justify the legitimacy of data flows to the United States. The lack of observable benchmark standards creates a presumption of insufficient privacy. Foreign regulators must insist that all U.S. companies show adequate protection for personal information. American companies that implement serious standards of fair information practice are, in effect, penalized by the absence of general legal rules. For these companies, the targeted standards may supply adequate levels of fair information practice, but because of the disappointing aggregation under the U.S. approach, these companies must justify their practices to a variety of separate national regulators. In effect, the companies that have actually implemented the set of benchmark standards for fair information practices lose under the targeted approach and those that do not implement fair practices will be prevented from doing global business until they develop appropriate standards.

B. Connecting U.S. Standards to the Global Information Infrastructure

Since few, if any, European data protection officials seek to "pull the plug" on global networks, regulators and companies have engaged in an active search to customize standards for transborder data flows. The customization solution ironically reinvigorates the desire to minimize restrictions on information flows and reliance on dispersed standards. A reconceived contractual approach to bridging divergent standards of fair information practices injects citizen participation and societal restraint on the abuses of information power back into U.S. standards setting through a new mix of both legal rules and industry norms and business practices.

1. A New Approach to the Contractual Solution

Academics, international organizations, and European government agencies have proposed contractual solutions as a potential aid to the transborder data-flow problem.[266] Under this model, a company that

264. *See* Reidenberg, supra note 56, at 294.

265. Id.

266. *See* G. Michael Epperson, Note, Contracts for Transnational Information Services:

wishes to transfer personal information to a country without an omnibus data protection law, like the United States, must first enter into a contract with the recipient to protect the data protection rights of the individuals concerned once the data is at the destination.[267]

The contractual model, as presently conceived, however, suffers a number of weaknesses. Because of the traditional contract doctrine of privity in some European common- and civil-law jurisdictions, individuals may not have any right against the recipient of personal information to enforce fair information practices.[268] If the contract is governed by American law, the individuals may have a third party beneficiary claim.[269] The model, though, also contemplates discrete information transfers, rather than the complex network information processing arrangements that may be the primary source of concern. Additionally, this contractual model is not an adequate substitute for an effective managerial policy toward personal information that implements fair information practices in transnational contexts.[270]

The existing contractual solution seeks to give the individual "primary" rights with respect to the data recipient. The contract itself is the source of protection for individuals against the data recipient. This situation suffers important substantive and instrumental weaknesses. Individuals may be unable to enforce effectively their protections for the treatment of personal information due to a lack of privity, the need to obtain jurisdiction in a foreign country, or the difficulty establishing foreign law in the local forum. In addition, the terms of the contract are

---

Securing Equivalency of Data Protection, 22 Harv. Int'l L.J. 157, 171-75 (1981); B.W. Napier, Contractual Solutions to the Problem of Equivalent Data Protection in Transborder Data Flows (paper presented at conference on "Legal Challenges and Opportunities Created by the Prolific Growth of Electronic Information Services," organized jointly by the Council of Europe and the Commission of the European Communities, Luxembourg, March 27-28, 1990) (on file with the University of Iowa College of Law library); Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows with Explanatory Memorandum, Council of Eur. Doc. T-PD (92) 7 revised (Nov. 2, 1992) [hereinafter Council Model Contract] (on file with the University of Iowa College of Law library).

267. *See* Déliberation No. 89-78, *reprinted in* CNIL., supra note 259; Council Model Contract, supra note 266.

268. *See* Napier, supra note 266, at 24 (discussing the problem of privity in English law). Other jurisdictions may not have the same privity problem, but conflict of law principles may present an issue if parties go forum shopping. Furthermore, the typical contractual solution contemplates very discrete transfers that are often atypical for information systems. *See* Reidenberg, supra note 69, at S175. In addition, scope and enforceability issues remain. *See* Ulrich Lepper, XIII Conference of Data Protection Commissioners 50-51 (1991) (paper available from the Council of Europe).

269. *See* Joel R. Reidenberg, An American Solution to TBDF Personal Data Contractual Problems, Privacy L. & Bus., Dec. 1991, at 12-14.

270. *See* William R. Whitehurst, Director of Data Security Programs, IBM, Remarks at the Symposium on Model Contract Clauses and Their Use in Transborder Data Flows (May 6, 1993) (symposium organized by the International Chamber of Commerce, the Council of Europe, and the Commission of the European Communities) (on file with the University of Iowa College of Law library).

negotiated by the companies themselves with the input of data protection authorities.[271] The exporting company acts, in effect, as the agent for the individual, though the individuals have no direct representation during the contract negotiations.

The reconception of the contractual model can avoid these inherent problems. The reconceived model looks to contract as a by-product of protection for individuals rather than a source of protection itself. This reconception starts with an exporter's direct obligation to the individual to adhere to the local standards[272] of fair information practice no matter where the personal information goes.[273] The exporter remains responsible to the individual for the foreign treatment of any personal information the company transfers. The foreign recipient becomes, in effect, the agent of the exporter.[274] This places the burden on exporters to demonstrate to individuals, and to the local data protection authority, that the standards actually being applied by the foreign recipient conform to the requirements of the exporting jurisdiction. The exporter has a form of strict liability for the foreign treatment of any exported personal information. Under this reconceived model, individuals can seek redress in their local jurisdiction against the exporting company for the recipient's nonconforming treatment of personal information. The individual's claim is based directly on existing local data protection law and the export authority.

Under this reconceptualization, the implementation of standards for foreign treatment of personal information becomes a private contractual matter between the exporter and the recipient. Yet, because the exporter's obligations depend upon the standards at the place of exporting, the recipient must disclose its foreign practices and must commit to adhere to appropriate practices. Unless the exporter knows what standards the recipient will apply, and knows that the standards meet local requirements, the exporter cannot meet its local obligations.

Once the recipient commits to appropriate standards, the exporter will still need to supervise compliance. To this end, an exporter needs some form of regular certification mechanism included in the contract to assure that the recipient's processing conforms to the contractual standards. Without some form of periodic audit, the exporter would fail to conform to its own local obligations. Since the foreign recipient is not

---

271. Since the data protection authorities may block information transfers if they are not satisfied with the arrangements, companies must consult with them on any contractual arrangements.

272. Throughout this discussion, "local" refers to the jurisdiction where the data export originates.

273. This parallels the new Québec law that requires exporters to take reasonable measures to assure the fair treatment abroad of any transferred data. An Act respecting the protection of personal information in the private sector, ch. 17, 1993 S.Q. 503 (Can.) (to be codified at R.S.Q. ch. P-39.1).

274. This reverses the assumption under the present view of contractual solutions that the transferor is acting as an agent of the iiidividual concerned. *See* Napier, supra note 266.

subject to similar legal standards where it operates, the presumption is that the recipient's practices do not conform to the exporter's local obligations. Audit and certification is the only way for the exporter to show the recipient's compliance with proper standards. Certification by an independent outside audit could confirm compliance with the appropriate standards to individuals and data protection authorities,[275] though for particular cases, the exporter would need to show that the standards were followed in the specific instance.

There are precedents emerging in U.S. domestic practice that show the viability of this approach. Several companies have recently established "privacy audit" mechanisms.[276] Others are improving transparency of their business practices through corporate privacy advisory boards.[277] Intercorporate arrangements are now starting to include greater disclosure.[278]

Under this new contractual approach, the local data protection authority preserves its ability to protect the treatment of personal information while decreasing disruption of international data flows. The data protection authority retains supervisory power over the exporter and leaves the question of the adequacy of foreign standards to the private sector itself. Data protection authorities could also develop a useful role serving as a consultative agency to determine foreign disclosure needs and validate the quality of any outside auditor.[279]

---

275. In Canada, the Canadian Standards Association is developing a mechanism for privacy auditing. At least one large accounting firm has conducted a company privacy audit and other experts have performed privacy audits for large companies.

276. For example, IBM has had a long-standing audit policy for personnel records. Within the last five years, Equifax has hired an outside consultant to assess the privacy implications of various company activities. TRW has instituted a rating mechanism to determine the privacy sensitivity of new information uses. TRW/REDI, likewise, engages in regular privacy audits and assigns internal officers to the task. Other companies, such as LEXIS/NEXIS have more informal privacy vetting procedures, usually centered on reviews of information products or systems by key personnel.

277. These have three varieties. External boards involve outside consultants to advise on fair information practices. TRW and Equifax have followed this model. Internal boards consist of formal management committees of key personnel charged with considering privacy policy. AT&T is an example of this approach. Finally, informal consultations consist of a group of key personnel that considers a particular new problem or product on an ad hoc basis. U.S. West and LEXIS/NEXIS have followed this process.

278. Aetna Insurance Company, for example, processes claims for many private insurance plans. When Aetna acts as a third party claims processor, it requests that the client specify the purposes for the claims information in writing, and the purpose must be related to the relevant insurance plan. *See* Who's Reading Your Medical Records?, supra note 171, at 628; *see e.g.*, U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, 33-35 (Sept. 1993).

279. The Canadian Standards Association is presently studying models of fair information practice auditing.

2. *Restoring Citizen Participation in the U.S. Private Sector with Limited Government*

The reconception of the contractual model ensures greater citizen participation in foreign data processing. Individuals could directly challenge an exporter in the individual's home country over the treatment of personal information by foreign recipients. Because of the absence of comparable legal rules at the information destination, foreign treatment of personal information without clearly articulated standards cannot satisfy the local requirements. The individual need not show noncompliance with local standards; rather, the exporter must show that it has taken steps to assure protection and that the recipient has implemented those steps. A data protection authority could, likewise, require the exporter to demonstrate that the standards of the exporting country are respected by the foreign recipient.[280] In each case, the burden falls on the exporter to justify that foreign data processing meets the local standards. Absent sufficient proof, the exporter fails to meet the local standards. Under this structure, only a foolish exporter would fail to enter into a contract with the recipient that allows the exporter to audit and control the processing of the transferred personal information.

An important aspect to this reconceptualization is that the contract remains a decision between the exporting and importing companies. The implementation of data protection requirements at the destination is a business deal. This is consistent with the American desire for minimal government involvement. Self-interest forces the exporter to take data protection provisions seriously. Similarly, the solution injects a data protection authority into the calculus; any cautious exporter will necessarily engage in consultations with the relevant data protection authority. Even absent a notification requirement for foreign data transfers, an exporter has much to gain by seeking assurances that the measures it envisions are satisfactory. Few exporters would want the risk of liability in the exporting jurisdiction.

The reconceived contractual model has an important transparency effect in the United States. Foreign companies will require that U.S. trading partners disclose their U.S. information practices. Under the foreign standards, the disclosure would be available to the concerned individuals in the exporting jurisdiction. This reduces the possibility for hidden manipulation of citizens. Although the direct beneficiaries of this transparency are individuals with foreign-sourced personal information,[281] double standards are frequently problematic for corporate management. The required disclosures are likely to prompt commitments by U.S. companies to refrain from secondary use of transferred personal

280. This power may only be available where national data protection law requires protection in the case of international transfers.

281. Many of these individuals are unlikely to be U.S. citizens or residents.

information.

The commitments made by U.S companies to satisfy their foreign counterparts are likely to have an important spill-over effect on U.S. practice. Companies will be reluctant to provide fairer treatment for foreign-sourced personal information than to U.S.-based information. The pressure for good corporate citizenship makes it hard for a U.S. company to justify treating foreign personal information with higher standards than personal information of U.S. origin. Since information processing systems are global systems, transparency and commitments in one part of the network can circle back to other areas in the network.

The new contractual solution also introduces enforcement possibilities. Individuals could pursue remedies against data exporters according to the local data protection law. While individuals may not be able to stop unfair foreign practices directly, the civil and criminal penalties available under many national data protection laws provide a powerful incentive for the exporter with potential liability to include contractual controls over the information recipient, the exporter's "agent." This supervision, however, preserves the philosophy of limited government. The allocation of responsibility to the data exporter places the burden on the exporter to assure compliance at the destination. If the exporter fails to obtain sufficient disclosure, adequate commitments, and satisfactory compliance certifications, the exporter would face liability for directly violating the data protection law in the jurisdiction of export.

This arrangement establishes private contract rather than government regulation as the prime source of standards between parties to international data transfers; the local data protection law provides the motivation. Yet, the role of the data protection authority would be significant. As a matter of prudence, data exporters would consult with data protection agencies to assure that contemplated arrangements are satisfactory. For example, a data exporter would need to seek guidance from the data protection authority to confirm that the disclosure is adequate and that the audit mechanism is strong enough.

With enforcement in place for international data transfers, pressure should build to establish U.S. standards that treat domestic data in the same fair fashion. International data transfers will force exposure of U.S. industry norms and business practices and give transparency to U.S. companies' treatment of foreign-sourced personal information. Companies will have to implement standards of fair information practice for at least some personal information, and their partners will be able to penalize them for failure to treat personal information properly. Without similar standards of fair information practice in the United States, companies will find it difficult to justify a double standard to the American public. At the same time, the adoption of standards of fair information practice by companies for their foreign information will make it easier to accommodate the extension of similar treatment to domestic data.

CONCLUSION

Business and citizen confidence in the "Information Superhighway" will depend on their perception that there is fair treatment of personal information. The minimal restrictions on information through targeted standards in the United States have not fulfilled the underlying goals nor have they provided benchmark standards of fair information practice. Foreign pressure will set the stage for new standards in the U.S. private sector.

The call for standards of fair information practice is not a call for interventionist or intrusive government regulation. The values of minimal government and the possibilities of state abuses of power are ever-valid policies. Instead, the call for standards is a call to equalize the playing field. In an Information Society, the private sector has not satisfactorily handled the making of norms through technical or corporate sources. Industry trade groups are hampered in their ability to promote the implementation of standards by their members. Individuals lack representation in these groups, and the cross-industry and context-specific uses of personal information defy a single point of view. Legal benchmark standards are needed to force private sector companies to develop appropriate information practices.

At the same time, the implementation and interpretation of any standards must remain a flexible and private sector-driven exercise. The significance of contextual evaluations for both domestic and international analyses is that any given treatment of personal information has unique characteristics that defy a generic assessment of "right and wrong."

The mix of conditions vigorously renews repeated calls for the creation of a federal privacy commission in the United States. A commission is now in the interests of the U.S. private sector and the public. The development of a consensus on new standards with the participation of government, citizens, and business will, in the long run, directly benefit corporate America. The commission could provide a forum for resolving the struggles between different internal corporate divisions and society over the treatment of personal information.[282] For the Global Information Infrastructure, a U.S. privacy commission could also provide valuable assistance to companies dealing with foreign data protection authorities. Such a commission could also restore the United States to a position of agenda setting for the treatment of personal information on global networks; today, foreign data protection authorities monopolize the agenda.[283]

---

282. For example, tensions among marketing, security, and customer relations departments will highlight different views of the treatment of personal information.

283. *See* Paul M. Schwartz, European Data Protection Law and Restrictions on International Data Flows, 80 Iowa L. Rev. 471 (1995).