1995

The Fundamental Role of Privacy and Confidence in the Network

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

THE FUNDAMENTAL ROLE OF PRIVACY AND CONFIDENCE IN THE NETWORK*

*Joel R. Reidenberg***
*Françoise Gamet-Pol****

In this article, Professors Reidenberg and Gamet-Pol address privacy issues created by the expanding information infrastructure. Due to the historical trend of self-regulation in the private sector, they concentrate their attention on this area, where the possibilities for abuse are great and are detrimental to individual privacy interests. They begin by identifying key values for the treatment of personal information in a networked society: confidence of citizens and businesses, availability and accessibility of information, quality of information, and interoperability with the Global Information Infrastructure. The analysis then focuses on the relationship between these values, the characteristics of the emerging information networks, and the existing legal rules for private sector regulation. From this analysis, it becomes clear that new incentives must emerge to promote new rules in the private sector if we wish to maintain our commitment to the key values in the networks.

TABLE OF CONTENTS

** Associate Professor, Fordham University School of Law. A.B., Dartmouth 1983; J.D., Columbia 1986; D.E.A., Univ. de Paris I (Panthéon-Sorbonne) 1987.

*** Member of the Bars of New York and Marseille, France. Lic. en droit, Univ. de droit d'Aix-Marseille 1979; Maitrise en droit, Univ. de droit d'Aix-Marseille 1980; C.A.P.A., Institut des Etudes Judiciaire d'Aix-en-Provence 1980; LL.M., Fordham Univ. School of Law 1992.

INTRODUCTION

The emerging information infrastructure places standards for the fair treatment of personal information at a critical juncture. Information technology and information flows on expanding networks have restructured economic, political, and social organization. In essence, the "Information Society" is both a reality and a global enterprise. The capabilities of information technology linked to seamless networks offer revolutionary advances for "life, liberty and the pursuit of happiness."[1] Telemedicine will bring the best international expertise to rural doctors in North Carolina, Internet forums will open opportunities for "town meetings" across the country, and mobile communications will expand personal horizons exponentially. At the same time, however, these very seamless networks raise the fear of an Orwellian "Big Brother." Digital communications leave traces and portraits of every interaction with the network, and these traces may be put to a variety of unwanted secondary uses. Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens.[2]

This article explores some of the implications of an information infrastructure on privacy and confidence in the emerging networks. As part of this exploration, this article searches the contours of society's interest

1. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

2. *See, e.g.*, The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025-49,035 (1993); Europe and the Global Information Society, Recommendations to the European Council 18 (Brussels, May 26, 1994) [also known widely as the Bangemann Report] *available on* Internet, http://www.earn.net.

in the treatment of personal information and explores the new landscape of legal and policy values. Part I articulates some of the key values for the treatment of personal information in a networked, information society. It argues that public and private confidence is indispensable for robust networks to flourish, and such confidence, in turn, depends on the fair treatment of personal information. This part also stresses the social value of the available and accessible information with a concomitant dedication to the quality of information. This section further argues that quality requires participation by citizens and businesses in decisions about the circulation of personal information. Finally, part I expresses the value of interoperability of information networks across borders.

Part II analyzes some characteristics of emerging networks and demonstrates new challenges posed by the Global Information Infrastructure. In particular, this part examines decentralized information processing, multiple uses of information, and cross-sectoral uses. The section also describes the beneficial characteristics of network globalization.

In part III, this article examines the links between network values, characteristics, and existing legal rules. This part provides an overview of the treatment of personal information in the United States with particular emphasis on telecommunications. Finally, this section argues that some of the network values are advanced by existing rules, while others, such as confidence and data quality, are distorted.

Part IV concludes this article with an analysis of the incentives that push for greater congruence between network values and legal rules. This part determines that governmental pressure, both domestic and international, combined with greater citizen pressure on businesses is required to set this evolution in motion.

I. Key Values for the Treatment of Personal Information in a Networked Society

The effective penetration of information technology in society and the advancement of a network infrastructure depend upon the fulfillment of key values for the treatment of personal information. While networks may bring great benefits to society, they also may give rise to social costs associated with the use of personal information. This is especially true due to the fact that a number of essential values relate to the treatment of personal information.

A. Creating and Preserving Confidence of Citizens and Business in Information

One of the most striking findings of a recent opinion poll was that confidence in the fair treatment of personal information is an important factor to citizens in deciding whether to participate in the "National Information Infrastructure."[3] Similarly, the integrity of networks is a criti-

3. Louis Harris & Assoc., Inc., *Interactive Services, Consumers, and Privacy: A Na-*

cal factor for the growth of business opportunities on an information infrastructure.[4]

At present, both citizens and businesses in the United States lack confidence in our information-based society. A majority of Americans believe that they have lost control of their personal information. A growing number of individuals decline to engage in some form of commercial relationship, such as applying for jobs, credit, or insurance, and refrain from economic participation in society to avoid disclosing personal information.[5] While industry had promoted self-regulatory policies for almost twenty years,[6] public opinion has recently ceased to view industry treatment of personal information as benign.[7]

Businesses too have an increasingly common stake in the treatment of information on networks. Traditionally, the issue of confidence from the business side has not received much attention. Businesses often appeared to be potential abusers rather than potential victims since they were "users" of personal information rather than "producers." The expansion of information networks gives the business sector commercial reasons to desire a fair treatment of information. With heightened public concern for privacy, businesses will receive less information from individuals, thereby reducing commercial activity, if fair treatment is not perceived to exist widely.

Further, despite the more popular image of businesses using the personal information of consumers, businesses also produce identifying information themselves. As producers, businesses must be able to rely on the fair treatment of their own information. For example, when a communications company planned to profile the calling patterns of households in order to send them a directory of businesses with 800 numbers for services those households used, the key opponents turned out to be the business clients of the communications company.[8] The business clients

---

tional Survey xvii (1994) (a survey conducted for Privacy & American Business) [hereinafter *Interactive Services*].

4. *See* OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN A NETWORKED ENVIRONMENT 3 (1994) [hereinafter OTA, INFORMATION SECURITY].

5. *Interactive Services*, *supra* note 3, at xiii. A 1990 report showed that only 42% of Americans had "ever refused to give information to a business or company because they thought it was not really needed or was too personal." Louis Harris & Assocs. & Alan F. Westin, Equifax, Inc., *The Equifax Report on Consumers in the Information Age*, VI (1990), *in 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. 298 (1991) [hereinafter *The 1990 Equifax Report*]. The 1994 survey shows that this figure has risen to 70%, that is to say an increase of 28% in four years. *Interactive Services*, *supra* note 3, at xiii (quoting *The 1990 Equifax Report*, *supra*).

6. *See, e.g.*, S. REP. No. 1183, 93d Cong., 2d Sess. 14 (1974) *reprinted in* 1974 U.S.C.C.A.N. 6916, 6929-31 (explaining why the Privacy Act of 1974 was not extended to the private sector); PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) 34-35 [hereinafter PRIVACY STUDY REPORT].

7. Surveys show that the public believes the excessive collection of personal information by industry is a major problem. *See Interactive Services*, *supra* note 3, at xii.

8. Terry Brennan, *CADM Releases Its Unanimous Objection to AT&T 800 Directory;*

objected to telephone subscribers receiving a directory of competitors' toll free numbers.[9]

The critical importance of confidence is also well demonstrated by a recent United States governmental encryption proposal. The executive branch proposed a key escrow system using technology called the "Clipper Chip" in an effort to balance confidentiality of communications on digital networks with the government's capability to conduct wiretaps.[10] Privacy advocates and business lobbies were united in their opposition to the proposal. For privacy advocates, the proposal conjured up fears of massive governmental snooping on communications. For business, the proposal jeopardized the ability to use higher levels of security to preserve data integrity traveling on public information highways.[11]

For networks to develop and sustain the confidence of their participants, citizens and businesses must both be afforded a high degree of involvement in the decisions about the circulation of identifying data. This requires openness of policies and practices for the treatment of information. Citizens, businesses, and governments, when confronted with network issues, have each demonstrated a distrust of information practices that grew from decisions made on a non-inclusive basis. Citizens feel they have lost control of personal information. Businesses feel threatened by externally imposed security standards. Governments feel handicapped in law enforcement capabilities. To overcome these obstacles and to bolster confidence, each interested side must be involved in setting rules for fair treatment of information on an information infrastructure.

B. Promoting Information Availability and Accessibility

If personal information is available and accessible, the Global Information Infrastructure can make significant contributions to the quality of life in the Information Society.[12] Businesses can customize products and services, and managers can improve productivity while operating businesses from remote locations.[13]

In these ways and others, a wide array of data permits greater flexibility and value to an Information Society. Rules and safeguards for legitimate access and use of personal information should therefore set minimal barriers for healthy information sharing arrangements.[14]

Joins Other Industry Leaders, DM NEWS, Oct. 7, 1991 at 1.

9. *Id.*

10. *Telecommunications Network Security: Hearings Before the Subcomm. on Telecomm. and Finance of the House Comm. on Energy and Commerce*, 103d Cong., 1st Sess. 38-40 (1993) (statement of Raymond Kammer, Acting Director, NIST).

11. *See* OTA, INFORMATION SECURITY, *supra* note 4, at 170-72.

12. For example, Levis jeans can now be made to order through a networked information processing system linked to an automated sewing factory. Glen Rifkin, *Digital Blue Jeans Pour Data and Legs into Customized Fit*, N.Y. TIMES, Nov. 8, 1994, at A1.

13. Nearly one in five Americans (17%) either operates a business from his or her home or does considerable amounts of office work at home. *Interactive Services*, *supra* note 3, at xi.

14. *See id.* at xv-xvii.

C. *Assuring Quality Information*

A robustly networked society depends upon quality information. Because of the intangible nature of information, quality derives from the conditions surrounding the data. Only the fair treatment of personal information gives maximum value. Quality information reconciles the values of all interested parties—citizens, business, and society. Participation on an equal footing in a networked society gives value to personal information. Private citizens must be able to take part in the use of their personal information. Indeed, easy access to personal information will improve the accuracy of information since individuals will have the opportunity to check and correct their personal information. Similarly, this right of access will ensure the validity of information. The business community needs to develop a broad consensus on fair information practice standards. Above all, it must be remembered that quality requires fair and permissible uses,[15] relevancy,[16] timeliness,[17] accuracy,[18] and reliability.[19]

D. *Ensuring "Interoperability" on the Global Information Infrastructure*

Networks and information transmissions are global in nature, and few would deny that divergent norms in a global information economy pose problems.[20] Consequently, information standards cannot be developed solely on a national level. Indeed, the European Commission has noted that if countries were to adopt varying standards, "efforts to guar-

---

15. Information should be collected lawfully for specific purposes. 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, art. 6(1)(b) (Oct. 15, 1992) [hereinafter Amended Proposal]; The Organization for Economic Co-operation & Dev., Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, O.E.C.D. Doc. C(80)58, final (Oct. 1, 1980), pt. 2, §§ 7-8, *reprinted in* 20 I.L.M. 422 (1981) [hereinafter O.E.C.D. Guidelines]; Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 5, *opened for signature* Jan. 28, 1981, Eur. T.S. No. 108, *reprinted in* 20 I.L.M. 317 (1981) [hereinafter Council of Europe Convention]. Likewise, secondary uses must be limited. Amended Proposal, *supra*, art. 6(1) (b); the O.E.C.D. Guidelines, *supra*, pt. 2, §§ 9-10; Council of Europe Convention, *supra*, art. 5b.

16. The collection of extraneous information is proscribed by a commonly accepted standard that can be found in Amended Proposal, *supra* note 15, art. 6(1)(c); O.E.C.D. Guidelines, *supra* note 15, pt. 2, § 8; Council of Europe Convention, *supra* note 15, art. 5c.

17. Amended Proposal, *supra* note 15, art. 6(e); O.E.C.D. Guidelines, *supra* note 15, pt. 2, § 8; Council of Europe Convention, *supra* note 15, art. 5e.

18. Amended Proposal, *supra* note 15, arts. 6(1)(d), 13; O.E.C.D. Guidelines, *supra* note 15, pt. 2, §§ 8, 12-13; Council of Europe Convention, *supra* note 15, art. 8c.

19. *See* Amended Proposal, *supra* note 15, art. 17; O.E.C.D. Guidelines, *supra* note 15, pt. 2, § 11; Council of Europe Convention, *supra* note 15, art. 7.

20. *See* Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137 (1992) [hereinafter Reidenberg, *Privacy Obstacle Course*].

antee a high level of protection could be nullified by transfers [of personal information] to other countries in which the protection provided is inadequate."[21] To accomplish true data protection then, American standards of fair information practice must be "interoperable" with worldwide trends in data privacy. Only in this way can we maintain the competitive position of American business on the Global Information Infrastructure.

II. Some Emerging Characteristics of the Network[22]

The Global Information Infrastructure transforms American society both economically and politically. From a domestic point of view, it offers numerous multimedia services, thereby bringing a major shift in information processing and enabling the decentralization of information processing, the multiplication of uses, and the increase of cross-sectoral uses. From an international point of view, it allows real-time access to data and information services across borders.

A. Major Shift in Information Processing Systems

In the 1960s and early 1970s, computing and telecommunications were generally controlled by the federal government and large corporations.[23] The emergence of personal computers and networking in the mid-1980s, however, contributed to a shift in power to the commercial sector. Smaller private-sector organizations gained access to sophisticated information-processing capabilities through inexpensive equipment. Individuals and small, private organizations obtained access to vast information resources through services such as Prodigy, Compuserve, and America Online. In essence, the Internet and private networks gave globalized access to information to both individuals and small organizations. Globalized access to information and real-time interactivity multiply the options available to users of information, both individuals and businesses. Interactive communications produce numerous transaction records, thereby multiplying choices regarding the use of information as well.

At the beginning of the 1990s, information processing was decentralizing even within large corporations as networks replaced mainframe computers. Today, in the mid-1990s, the decentralization of information processing has made omnipresent surveillance possible by organizations and even individuals. This decentralization enables any network participant to centralize data, for although bits of information are scattered throughout the network, they are accessible from any place on the network. This, however, is not the extent of decentralization's effects. Sophisticated information providers and intelligent networks already enable combinations of audiovisual images and sounds with other interactive ser-

---

21. Amended Proposal, *supra* note 15, Explanatory Memorandum.

22. *See generally* Joel R. Reidenberg, *Information Flows on the Global Infobahn, in* The New Information Infrastructure: Strategies for U.S. Policy (Wm. J. Drake ed., forthcoming May 1995).

23. *See generally* Privacy Study Report, *supra* note 6.

vices. Further, decentralization of information processing in the United States dramatically broadened the role of private-sector data processing and shifted power from the federal government to private-sector organizations. These private organizations now have exclusive control over the decisions regarding the collection and use of personal information.

B. Blurring Boundaries

As interactive communications proliferate, transaction information or "information about information" is commonly generated in the context of service provision. Transaction generated information occurs in fields ranging from the obvious, like interactive media, to the unsuspecting, like employment.

Because of easy access to multiple sources of data and because there are few existing legal restrictions on the use of information, secondary use of collected information is significant.[24] Personal information is often collected in one context for a particular purpose and used in another context for a different purpose. For example, telephone billing requires the processing of information relating to the caller, the number called, the duration of the call, the time of the call, and the billing rate. Similarly, caller identification services disclose the originator of incoming calls. Yet, this information, when stored, is used to develop profiles of individuals for other uses, such as direct marketing. The network not only generates personal information in similar fashion across industries, but it also takes information generated in one industrial sector and enables its use in another.

The network itself also amplifies this tendency and decreases confidence in privacy by giving numerous private actors easy access to personal transaction information. For example, caller identification technology, combined with data capture equipment and information service offerings, allows even small companies to build profiles of individuals in previously unimaginable detail.[25]

In addition to their diminishing effect on sectoral boundaries, networks also blur national borders. The Global Information Infrastructure, through network activity, links great distances and traditional boundaries. At the international level, networks allow real-time access to data and information across long and short distances. Miles are traversed in seconds and international boundaries become little more than imaginary lines on maps, as borders become defined in terms of networks rather than countries.[26]

---

24. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 200-08 (1992) [hereinafter Reidenberg, *Privacy in the Information Economy*].

25. For a further discussion of the types of profiles created with transaction information, see *infra* notes 77-78 and accompanying text.

26. *See* Joel R. Reidenberg, *Symposium: Electronic Communications and Local*

III. Forging Links Between Values and Characteristics

The Global Information Infrastructure's characteristics pose challenges to fundamental values for an information society. Present legal rules and standards for electronic communications offer disjointed links between the values and characteristics. While some values may be advanced by the match between net characteristics and existing rules, others are not.

A. *The Legal Landscape and Setting Standards*

The treatment of personal information in the private-sector is addressed in a reactive, ad hoc manner. Specific laws answer particular concerns. Until recently, most issues were addressed by self-regulation, an ideology having great symbolic meaning in the United States. With the American legal system's preference for drawing fair information practice standards from varied and diverse sources, it comes as no great surprise that the United States legal system tends to disregard present international trends.

1. *U.S. standards: ad hoc, targeted, and confused*

Despite the development of the multi-layered information society, the United States develops legal rules for standards of fair information practice in an ad hoc, targeted fashion.[27] This specificity is due, in part, to American business lobbying, which has managed to maintain narrow privacy protection for individuals in spite of the decentralization and the growing role of private sector data processing. Industry, to some extent, proposes voluntary standards for particular problems.[28] As a result, targeted standards and specific restrictions govern the treatment of personal information. Decentralization of information processing and wider information use have not altered the narrow focus of U.S. regulatory policy.

2. *The religion of self-regulation*

This ad hoc, issue-by-issue conception of governance has two consequences in the area of information. First, there is the recognition of the principle of the free flow of information. As Justice Brandeis wrote, the

---

Changes: Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms, 6 Harv. J.L. & Tech. 287, 303 (1993) [hereinafter Reidenberg, *Rules of the Road*].

27. *See* Reidenberg, *Privacy in the Information Economy*, *supra* note 24, at 195.

28. *See, e.g.*, Direct Mktg. Ass'n, Direct Marketing: Opening the Door to Opportunity: A Simple Guide to Understanding How Direct Marketers Use Information 9-10 (discussing how Direct Marketing Association Mail Preference Service allows consumers to have their names and addresses suppressed from mailing lists for junk mail solicitations); Privacy Study Report, *supra* note 6, 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.").

First Amendment—itself closely linked to the concept of protection of the citizen against the state—secures the "freedom to think as you will and to speak as you think."[29] Liberty of thought presupposes that information be freely available, and thus is usually believed to conflict with government-imposed restrictions.[30] Second, sectoral restrictions, if any, are preferred over comprehensive rules on the treatment of personal information. Following the principle of free flow of information, legislatures respond only to specific issues.[31] Legal standards are justified only where targeted for a particular problem: therefore, standards often develop on an ad hoc basis, by reaction to public scandals. Examples include the protection of video rental records following the disclosure of records for a nominee to the U.S. Supreme Court[32] and the Fair Credit Reporting Act, which was enacted in response to consumer horror stories about dealing with credit reporting agencies.[33]

Traditionally, the business community opposes the establishment of legal standards: it prefers to resort to self-regulation to assure fair standards for treatment of personal information in American society. Yet, the experiences resulting in legislation and the discomfort of prominent businesses with industry practices show that the sectoral restrictions on the treatment of information have not been sufficient.

3. A few particular rules for telecommunications

In a digital environment, the treatment of message content and transaction information are critical for the promotion of key values. The net makes the distinction artificial. Message content is just as searchable and malleable as transaction profile data. Despite this similarity in accessibility and options, however, current law differentiates between the two.

a. The Electronic Communications Privacy Act. The Electronic Communications Privacy Act,[34] along with a number of similar state laws,

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

30. This conflict is a traditional view that Professor Sunstein persuasively criticizes. CASS R. SUNSTEIN, THE PARTIAL CONSTITUTION 197-256 (1993).

31. *See, e.g.*, The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1988 & Supp. V 1993); The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2711 (1988 & Supp. V 1993); The Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1988 & Supp. V 1993); The Cable Communications Policy Act, 47 U.S.C. § 551(a) (1988); PRIVACY STUDY REPORT, *supra* note 6, at 34. *See generally* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993) (explaining the results of legislative attempts to codify standards of fair information practices); Reidenberg, *Privacy in the Information Economy*, *supra* note 24 (arguing state legislation is narrowly focussed). In the public sector, however, legislatures have sought broader regulation. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1988 & Supp. V 1993); Paul Schwartz, *Data Protection and Participation*, Symposium, 80 IOWA L. REV. _ (forthcoming March 1995).

32. *See* The Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1988 & Supp. V 1993).

33. The Fair Credit Reporting Act, 15 U.S.C. § 1681a (1988 & Supp. V 1993).

34. 18 U.S.C. §§ 2510-2711 (1988 & Supp. V 1993).

offers a variety of standards for the handling of message content. In essence, legal rights offer protection from unauthorized collection and recording.[35] Yet, the legal rights emphasize protection against governmental intrusions in the private lives of citizens.[36] The government can only access private communications with a court order and for a specified law enforcement purpose.[37] As for the provider of a public telecommunications service, it may not disclose the contents of an electronic mail message without the consent of at least one of the parties.[38] Legal rights also prevent third parties from accessing electronic mail messages without authorization.[39] In addition, computer crime legislation prohibits individuals from accessing computer systems, including electronic mail files, without authorization.[40]

Once the network records message content, senders or recipients may generally make multiple use of the recording even for secondary purposes.[41] In the case of private networks, the network operator may also use electronic mail message content for secondary purposes.[42] This issue arises in the context of employee monitoring.

Unlike the protection afforded to content, however, U.S. telecommunications laws generally do not require the identification of purposes for the collection of transaction generated information. There is no specific restriction against overextensive collections of personal information for transaction data. Nor is there any restriction on the duration of storage for transaction generated information. Few obligations exist for openness or transparency with respect to the treatment of transaction generated information. Networks now provide caller identification automatically and even household recipients have the same data capture ability as large companies operating toll free services. Significantly, the law provides few restraints on secondary use of traffic data. While it is true that transaction information is a valuable tool for surveillance, lifestyle profiling, and product marketing, these uses can be both beneficial and nefarious.

b. The Telephone Consumer Protection Act of 1991. The recent Telephone Consumer Protection Act,[43] which restricts the use of auto-

35. *Id.* § 2702.

36. The law prohibits the federal government from obtaining personal information without a specified law enforcement purpose. In addition, the recent Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279, 4292 (1994), created stricter requirements for the federal government in obtaining a court order to access transaction information.

37. 18 U.S.C. § 2703.

38. *Id.* §§ 2511(3)(b), 2702(b).

39. *Id.* § 2511(1).

40. *Id.* § 2701 (1993).

41. This is not the case in the few states that have "two party consent" rules. *See* Maryland Wiretap and Electronic Surveillance Act, MD. CODE ANN., §§ 10-401 to 10-414 (1989).

42. *See* 18 U.S.C. § 2701(c).

43. Pub. L. No. 102-243, 105 Stat. 2394 and Pub. L. No. 102-556, 106 Stat. 4185 (codified in scattered sections of 47 U.S.C.).

matic dialing equipment, was cast as an important piece of privacy legislation.[44] In reality, this act was meant to address nuisance telephone calls to households.[45] In implementing the act, the Federal Communications Commission originally contemplated a national "do not call" database of individuals who wanted to opt out of telemarketing calls.[46] Marketers did not favor the concept of losing control of the database and the final regulations took an approach more oriented toward the private sector. Telemarketing companies were allowed to make the first unwanted call and then had to maintain their own "do not call" lists from individuals who requested to opt-out.[47] While the law is primarily directed at nuisance problems, the statute provides a measure of fair information practice for the use of household telephone numbers.

4. Other normative sources[48]

The American system values a diversity of sources for fair information practice standards to prevent any single actor from controlling information flows. Specific standards for fair information practices come from various sources. First, there are legal rules, including specific pieces of legislation, such as the Fair Credit Reporting Act[49] or the Video Privacy Protection Act,[50] as well as more general statutes with some bearing on the treatment of information like the Equal Employment Opportunity Act.[51] Second, there is technology, which may structure the treatment of personal information through technological choices and technical decisions. Third, there are industry norms and business practices, in particular, industry codes of conduct which may establish an ethos for an industrial sector,[52] company policies and their implementation,[53] contrac-

---

44. While the law has been held unconstitutional by a federal court, the grounds did not relate to fair information practices. *See* Moser v. FCC, 826 F. Supp. 360 (D. Or. 1993) (holding act's ban on use of artificial or pre-recorded voices to deliver commercial messages to residential telephones without consent of recipient placed unconstitutional content-based restriction on protected commercial speech in violation of First Amendment). *See generally* Rita Marie Cain, *Call Up Someone and Just Say 'Buy'—Telemarketing and the Regulatory Environment*, 31 AM. BUS. L.J. 641, 649-55 (1994) (discussing telemarketing regulation, including Telephone Consumer Protection Act and *Moser* decision).

45. *See In re Rules and Regulations Implementing the Telephone Consumer Protection Act*, 7 F.C.C.R. 8752, 8753 (1992).

46. *Id.* at 8754-55.

47. 47 C.F.R. § 64.1200(e)(2) (1993).

48. For a further discussion of the three main sources of fair information norms, see Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. _ (forthcoming March 1995) [hereinafter Reidenberg, *Setting Standards*].

49. 15 U.S.C. §§ 1681-1681t (1988 & Supp. IV 1992).

50. 18 U.S.C. §§ 2710-2711 (1988).

51. 42 U.S.C. §§ 2000e-2000e17.

52. *See, e.g.*, DIRECT MKTG. ASS'N, GUIDELINES FOR PERSONAL INFORMATION PROTECTION (1992) [hereinafter DMA GUIDELINES]; INFORMATION INDUS. ASS'N, FAIR INFORMATION PRACTICES GUIDELINES, POLICY STATEMENT (1994).

53. *See, e.g.*, American Express, Cardmember Privacy, Mailing and Telemarketing Options (1994); Citibank Visa & Mastercard, Privacy Policy (1993).

tual arrangements between companies and individuals or business customers and, lastly, good corporate citizenship resulting from pressures of public opinion, academia, advocacy groups, and governmental officials.

Industry codes are generally weak sources of information practice standards because the fairness of practices remains at the level of company activity. Likewise, company policies are not legally binding. Finally, corporate citizenship, though not mandatory, may prove more efficient for stimulating business practices because of the potential public relations embarrassments associated with poor practices. A number of private companies are now implementing new standards in order to promote good corporate citizenship.[54]

This justification for decentralized sources is the anticipated flexibility of such a resulting system to adapt to specific conditions. This rationale draws on the same thinking as the federalist goal of making the states "laboratories" for appropriate kinds of regulation.[55]

Since varied sources offer overlapping and distinct standards of treatment, this argument is not convincing. The standards applicable to the private sector derive from the combination of standards implemented through each source. Rather than flexibility, this brings excessive complexity, especially when associated with the pursuit of targeted standards. Targeted standards from diverse sources make an accurate assessment of the treatment of personal information in the private sector elusive.

The narrow and complex nature of American standards for fair information practices encourages parochialism. This situation brings about a disregard for international trends and standards regarding the treatment of personal information and the protection of privacy.

5. *The American disregard for international trends and standards*

Other countries, particularly European countries, have approached the treatment of personal information in a comprehensive manner and have adopted broad legislation which seeks to balance freedom of information against privacy rights. Such legislation, called "data protection laws," usually covers both the public and private sectors and sets out principles for the fair collection, storage, use, and dissemination of per-

---

54. Equifax and Dun & Bradstreet have recently included commitments to privacy in their annual reports. *See* DUN & BRADSTREET, 1993 ANNUAL REPORT (1993), *available in* LEXIS, Naars library, 93 file; EQUIFAX, INC., 1992 ANNUAL REPORT (1992), *available in* LEXIS, Naars library, 92 file. American Express also provides a detailed privacy notice to cardholders on an annual basis. The exact wording of this notice was prescribed by the New York Attorney General's Office. *See* American Express Travel Related Services, Inc., Agreement of Voluntary Assurances, May 8, 1992 (on file with the Attorney General of the State of New York, Bureau of Consumer Frauds and Protection).

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). *See* Reidenberg, *Setting Standards*, *supra* note 48.

sonal information.[56]

This world-wide trend toward broader, more comprehensive legislation is reflected particularly in the proposed European data privacy directive,[57] currently under active deliberation. This proposal, as well as existing national laws in many European countries such as Belgium, France, Germany, the Netherlands, and the United Kingdom, allows the prohibition of data transfers to countries perceived to lack sufficient privacy protection. Governments in other places, such as Quebec,[58] have adopted novel legislation, while elsewhere, in Japan for example,[59] governments are also examining their present fair information practice policies. According to one source, more than thirty countries around the world are focussing on new fair information practice rules.[60]

Thus far, the United States has either sought to avoid the trend or to ignore international standards.[61] In the late 1970s, the Organization for Economic Cooperation and Development (O.E.C.D.)[62] and the Council of Europe[63] began developing comprehensive principles for fair information practices.[64] The O.E.C.D. emphasized the free flow of information,[65] while the Council of Europe favored a stronger emphasis on the protection of human rights.[66] The United States participated only in the O.E.C.D. efforts and succeeded in having the final document considered only a set of voluntary standards, rather than mandatory rules. The Council of Europe instrument, however, became a binding international treaty and many countries enacted comprehensive national laws in response to it. Conspicuously, the United States did not become a signatory to the treaty. Consequently, there is no formal United States representation at multilateral meetings of foreign Privacy Commissioners to discuss standards.

More recently, during the Uruguay Round of the General Agreement on Tariffs and Trade (GATT)[67] and the negotiations of the North Ameri-

---

56. *See* Reidenberg, *Privacy Obstacle Course*, *supra* note 20, at S137-S177 (describing such statutes).

57. *See generally* Amended Proposal, *supra* note 15; Robert G. Boehmer & Todd S. Palmer, *The 1992 EC Data Protection Proposal: An Examination of its Implications for U.S. Business and U.S. Privacy Law*, 31 AM. BUS. L.J. 265, 265-311 (1993) (comparing Amended Proposal with previous 1990 version).

58. *See* Loi No. 68 sur la protection des renseignements personnels dans le secteur privé, Assemblée Nationale, Deuxième Session, Trente-quatrième Législature (1992).

59. *See* Reidenberg, *Privacy Obstacle Course*, *supra* note 20, at S170-S171.

60. *See* Bojana Bellamy, *Data Protection Roundup*, PRIVACY LAWS & BUS., Oct. 1992, at 2.

61. *See* Fred H. Cate, *The Future of Communications Policy Making*, 3 WM. & MARY BILL RTS. J. 1, 10 (1994) (stating that "the United States . . . has often resisted participation in multinational policy level agreements" regarding information regulation).

62. The O.E.C.D. was founded in 1960 by 20 states, including the United States, to foster economic cooperation among industrialized nations.

63. The Council of Europe is an intergovernmental association organized to promote human rights issues.

64. O.E.C.D. Guidelines, *supra* note 15; Council of Europe Convention, *supra* note 15.

65. *See* O.E.C.D. Guidelines, *supra* note 15, Appendix § 25.

66. *See* Council of Europe Convention, *supra* note 15, Preamble.

67. General Agreement on Tariffs and Trade, *opened for signature* Oct. 30, 1947, 61

can Free Trade Agreement (NAFTA),[68] privacy was discussed as a possible barrier to trade.[69] The United States rejected proposals for a fair information practices code due to the strong opposition of American business lobbies.[70] Each instrument provides only for minimal restrictions on information flows: in the case of GATT, only for security and confidentiality purposes; in the case of NAFTA, only for the protection of subscriber privacy.[71]

Because of this history and its ongoing repetition, the United States' treatment of personal information is under great scrutiny. The European Union, in particular, is taking an active interest in American privacy law and practice. With passage of the European data privacy directive almost assured, the United States is taking greater notice of global issues and the importance of working in tandem with foreign trends rather than against them.

B. The Key Values Advanced by the Existing Landscape

1. Widely available and accessible information

Networks and the existing narrow regulations of information flows offer broad access to information. This has been the case since the mid-1980s with the emergence and development of personal computers and private networks. Information technology is becoming ever less expensive. Both individuals and small businesses have access to vast information resources, such as those available through the Internet and private networks like Prodigy or America On Line. The existing landscape erects few barriers to access to information.

This widely available information leads to improvements in daily life and in an increase of options: a growing number of Americans operate businesses from their homes; many students work from their homes through the use of personal computers and have access to a huge volume

---

Stat. pts. 5, 6, T.I.A.S. No. 1700, 55 U.N.T.S. 187 [hereinafter GATT].

68. North American Free Trade Agreement, Dec. 17, 1992, U.S.-Canada-Mexico, *reprinted in* 32 I.L.M. 289 (1993) (implemented in United States by North American Free Trade Agreement Implementation Act, Pub. L. No. 103-182, 107 Stat. 2057 (1993)) [hereinafter NAFTA].

69. *See* Reidenberg, *Rules of the Road*, *supra* note 26, at 294-95.

70. *See* Communications from the United States, Annex, Annex to and use of Services of Public Telecommunications Transport Services, GATT Doc. MTN.GNS/2/97 (Mar. 23, 1990) (outlining U.S. position during telecommunications annex negotiations).

71. *See* GATT, Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Annex on Telecommunications (Apr. 15, 1994), *available in* WESTLAW, IEL Database, I.E.L. I-B-64, at *741-50, art. 5(d) ("[A] Member may take such measures as are necessary to ensure the security and confidentiality of messages, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustified discrimination or a disguised restriction on trade in services."); NAFTA ch. 13, *available in* WESTLAW, NAFTA Database, 1993 WL 574438, at *2, art. 1302(5) (stating that parties may take necessary measures "to ensure the security and confidentiality of messages" and to "protect the privacy of subscribers to public telecommunications transport networks or services").

of data. This broad access also allows providers of goods and services to develop profile information on potential consumers, and thus to customize their offerings to those consumers. With fair information practices, the customization will match consumer needs and desires.

Information may not be available and accessible to all, however. In particular, access barriers are not low when citizens seek access to their own personal information. This aspect is problematic because any information can be included in some compiled profiles, and often companies do not permit the concerned individuals to access their own personal information. For example, Metromail, one of the largest sellers of personal information about consumers in the United States, ignores requests for access.[72] Hypocritically, Metromail purports to follow the Direct Marketing Association's privacy guidelines and serves on the DMA Privacy Task Force which is dedicated to promoting fair information practices within the trade association.

2. *Limited quality information*

Though the quantity of information is unquestionably promoted by the existing landscape, the quality of information may be less advanced. As previously argued, the quality depends on standards for permissible uses, relevance, timeliness, accuracy, and reliability.[73]

Since no set of general and comprehensive rules establish these quality standards and specific, targeted statutes rarely offer the range of standards,[74] society relies on business practices and self-regulation. While some companies may make a commitment to standards, self-regulation raises several inherent problems. First, many companies do not wish to implement any forceful standards. On a short-term basis, the exploitation of transaction information collected without such restrictions has tremendous value for marketing purposes. Second, even if companies do have such policies, the policies are often invisible: because of the lack of publicity and the absence of any obligation to disclose those company policies, citizens are not aware of them and cannot use them to access, check,

---

72. The DMA Guidelines call for access to personal information held by direct marketers. DMA GUIDELINES, *supra* note 52 at arts. 4-5. *Compare* Letter from Mary Doher, Metromail, to Joel R. Reidenberg (Aug. 10, 1994) (providing extremely limited and misleading information in response to request for all personal information contained in company databases) (on file with author) *with* Letter from Joel R. Reidenberg to Mary Doher (Aug. 16, 1994) (requesting full disclosure in conformity with the DMA GUIDELINES that provide individuals a right to access that information) (on file with author). *See also* Letter from Thomas Hiller, Vice President, Metromail, to Joel R. Reidenberg (Oct. 31, 1994) (stating that even though the personal information sold by Metromail is a matter of public record, Metromail did not disclose it because the company did not know requestor's (Joel Reidenberg's) "credentials") (on file with author).

73. For a further discussion of these standards, see *supra* notes 15-19 and accompanying text.

74. The rare examples of specific statutes that cover the range of quality standards are the Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1988 & Supp. V 1993), and the Cable Communications Policy Act, 47 U.S.C. § 551 (1988).

or correct their personal information. In sum, quality of information, as one of the issues raised by the present treatment of personal information, is, for the most part, entirely dependent upon unchecked self-regulators.

C. *The Values Distorted by the Network*

1. *Few standards and poor quality*

Ad hoc, narrowly targeted, and confusing standards cannot ensure the quality of information in a fluid, multilayered network. When combined with expanding networks, this approach creates an aggregate lack of sufficient standards to assure the fair participation of citizens. Because of the reactive nature of standards in the United States, citizens may be involved with their personal information for specific situations, but they will miss participating in both important cross-sectoral aspects and secondary uses of personal information. In effect, the network grants tremendous social power to the collectors of information. Even where there are far-sighted company policies, companies have little, if any, incentive to police themselves.[75] The business community has complete control over the disclosure of practices. The result is a lack of public awareness that such practices exist. Citizens are simply not aware of the possibilities afforded to them. Since citizens do not have access to their own information and cannot check or correct it, there is no guarantee that the information involved will be accurate despite the fact that the information and its accuracy may be very important to the individuals involved, such as patterns of telephone calls to particular numbers.

2. *Lack of confidence*

The multiplication of interactive communications increases the possibility of hidden surveillance of private citizens. Industries obtain bits of personal information from many sources. Interactive communications give the transaction details such as those collected through a credit card telephone call. Likewise, calls to toll free numbers, mail order purchases, as well as subscription lists from publications, and purchasing patterns at stores offer a great deal of information about individuals.[76] Even public records provide information to an industry: property records, for example, indicate the purchase price of an individual's home and any outstanding mortgage amounts. Those items of information are then cross-referenced and combined to establish detailed profiles of individuals. Most citizens are unaware of the uses to which such collected information is put. Ultimately, those profiles may result in the most amazing—and sometimes most offending—personal details, such as women wearing

---

75. *See* H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 167, 174-78 (1994) (discussing the role of corporations in developing U.S. corporate privacy domain).

76. *See* Jonathan Berry, *Database Marketing*, BUS. WK., Sept. 5, 1994, at 56-62.

wigs[77] or male buyers of fashion underwear.[78] These types of uses form a well-founded basis for the lack of citizen confidence in the treatment of their personal information.

Originally, commercial enterprises favored these cross-sectoral uses of information. However, they too are now experiencing a crisis of confidence in the treatment of information. What appeared to be a short-term benefit is turning out to be a long-term handicap. Indeed, when citizens learn how their information is used, they are likely to react negatively against the offending company.[79] In addition, while companies may have wanted unfettered access to information about individuals, they certainly do not want their own corporate information to be used in the same fashion. For example, companies will provide on-line public record information to reveal data such as the address and purchase price of the home owned by the Chief Justice of the Supreme Court,[80] yet they have suppressed the address of the American Express property in Phoenix, Arizona, where the company profiles the spending patterns of its cardholders.[81] In another telling example, AT&T planned to offer subscribers a directory of toll-free numbers; the directory sent to each recipient would match the profile of the household's calling patterns.[82] Thus, a directory of toll-free numbers for airlines would be sent to households that frequently called airline numbers. AT&T's business clients, however, objected vehemently to providing customers with information on their competitors' toll-free numbers.[83] These objections forced AT&T to abandon the project.

Even in terms of data integrity and security, the network distorts business confidence. The Internet, for example, is a thoroughly unsecure communications facility. Anyone can capture information transiting the network. For businesses to take advantage of networks, they must be able to assure the authenticity and confidentiality of communications. Encryption standards achieve this goal. Hence, when the federal government proposed the Clipper Chip, the very idea that a corporation could lose control over the encryption standard jeopardized corporate confidence in network transmissions.

---

77. *Carla Corcini Offers Wig Buyers*, DM NEWS, Oct. 19, 1992, at 54 (announcing "Ladies Wig Buyers" file from Venture Communications International, Inc.).

78. *Brawn of California Offers Three Lists*, DM NEWS, Apr. 5, 1993, at 34.

79. *See* SMITH, *supra* note 75, at 151-52.

80. *See Property Record for Arlington County, Va.*, Jan. 1, 1993, *available in* LEXIS, Assets library, VAown file (showing property address and details).

81. *See Property Record for Phoenix, Az., available in* LEXIS, Assets library, Azown file (showing no property address for several entries).

82. Terry Brenknan, *CADM Releases Its Unanimous Objection to AT&T 800 Directory; Joins Other Industry Leaders*, DM NEWS, Oct. 7, 1991, at 1.

83. *Id.*

3. *Lack of global interoperability*

The absence of comprehensive standards creates an important obstacle for the business community in its relationships with foreign countries. Indeed, the restrictions adopted over the last twenty years by some European countries and those contained in the European proposal have two important consequences. First, the transfer of personal information may be prohibited where the destination has insufficient privacy.[84] Second, the existing landscape raises the stakes for American businesses.

Foreign countries are necessarily interested in assessing the adequacy of American standards. Since there is no general set of legal standards, business practices will be under greater scrutiny and American businesses will be forced to justify the legitimacy of data flows to the United States. This scrutiny raises challenges for American businesses and can directly affect numerous activities, from payroll processing to travel reservations. The lack of compatibility with foreign countries also undermines business confidence, making the need for compatibility with foreign standards a large incentive to articulate and pursue key values.

IV. DIRECTIONS AND INCENTIVES TOWARD THE KEY VALUES

Global networks set new directions and incentives for society to move toward the key values. The need for confidence in the network realigns interests and pressures both within and outside the United States.

A. *Old Calls for Regulation Getting New Life*

There have been numerous proposals in Congress over the last two decades to establish a Privacy Protection Commission, most without any regulatory powers over the private sector. Until recently, there had been significant opposition in the business community to such proposals. This opposition is beginning to change, however, as businesses realize that the promulgation of fair standards will contribute to the development of a global information economy and will protect businesses as well. Despite the increased recognition of the value of fair information practice standards, even now, it is doubtful that a Privacy Protection Commission

---

84. *See* France, Loi no. 78-17 du 25 Janvier 1978, art. 24, *reprinted in* A.C.M. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC 353 app. C at 358 (1990); United Kingdom, Data Protection Act 1984, par. 12(2), *reprinted in* NUGTER, *supra*, at 366 app. D at 372. *See generally* Martine Briat, *Personal Data Flow and the Free Flow of Information in* FREEDOM OF DATA FLOWS AND EEC LAW: PROCEEDINGS OF 2ND CELIM CONFERENCE (1988); 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). *See also* Reidenberg, *Privacy Obstacle Course*, *supra* note 20, at S160-S165. As for the revised proposal, it still contains an important clause requiring the examination on data transfers outside the European Union to be permitted upon review of the sufficiency of standards at the destination. *See* Reidenberg, *Rules of the Road*, *supra* note 26, at 294 (arguing that first draft of directive which contemplated a blacklist of countries with inadequate standards for fair treatment of information was actually less likely to result in transfer prohibitions than revised proposal).

with regulatory power over the private sector would be welcomed by the business community.

Notwithstanding such continued opposition, a Privacy Protection Commission, even without regulatory powers, would still bring important benefits to the American component of the information society. A Commission would be instrumental in achieving public awareness of information practices and in securing greater citizen participation in the circulation of personal information. This step is critical to restore and develop citizen confidence in networks.

For business, a Commission, even with an advisory role rather than regulatory power, would be an ally for the development of publicly acceptable standards. A Commission might also assist in making technological choices to achieve fair standards. Such activities would contribute to business confidence in the long-term viability of information markets and the fair treatment of business information. Further, a Commission would be able to promote American interests in the global marketplace.

B. Shifting Business Incentives[85]

Global networks shift the perspective of American businesses and may help persuade lobbies to accept legal rules. American companies are beginning to understand that an absence of comprehensive private-sector standards harms the perception of business integrity in both domestic and international spheres. A number of major companies in the United States are already recognizing that fair information practices will define information services on the global network: they even refer, in their corporate annual reports, to the strategic importance of privacy policies.[86]

To be efficient, the development of corporate policies and standards requires the existence of disclosure rules. Indeed, invisible policies or practices disserve the business community as a whole. In addition to causing harm to relationships between businesses and citizens, invisibility threatens businesses directly. The cornerstone of the Clipper Chip proposal involved key escrow and invisibility of the encryption standard.[87] The strong business opposition illustrates the threat such invisibility (and government control of security) poses to confidence within the business community for network interactions.

Ironically, global corporations also have a strong incentive to support comprehensive standards of fair information practices. Standards can protect long-term global markets for large companies against competitors seeking short-term profits. As the leading corporate examples show, large companies are the first to recognize and value fair information practices. Telecommunications carriers like Pacific Bell and financial services companies like American Express, Equifax, and Dun & Bradstreet are seeking

---

85. *See* Reidenberg, *Setting Standards*, *supra* note 48.

86. DUN & BRADSTREET, 1993 ANNUAL REPORT (1993), *available in* LEXIS, Naars library, 93 file; EQUIFAX, INC., 1991 ANNUAL REPORT (1991), *available in* LEXIS, Naars library, 91 file.

87. *See* OTA, INFORMATION SECURITY, *supra* note 4, at 117-19.

to adapt to the new environment. This is not surprising. Large companies face greater scrutiny on both the domestic and international fronts because they are more visible and have more opportunities to abuse information. In order to protect their image and to keep their clients, large companies have had to develop standards. This evolution has now given them a competitive advantage with respect to smaller, less-noticed companies.

CONCLUSION

The establishment and the effective preservation of key values is an absolute necessity if we want to improve our daily lives without paying too great a social cost for the development of a networked society. It is possible to do so. Moreover, the network, as it is, may help us in our quest for those key values.

The emerging network amplifies many features of the treatment of personal information. It has made information more available and easier to access. It has increased the quantity of information available in society. It has multiplied the options for users. It has enabled multiple uses of information and developed the possibilities of cross-sectoral uses. At the same time, it has brought instantaneous connections around the globe. Networks thus appear to have contributed to the attainment of key values such as broad availability of information, increased quantities of information, low barriers to access and use, and interoperability with the rest of the world.

However, networks appear to present a conflict with the values of confidence and participation. Indeed, multiple secondary and cross-sectoral uses and broad access to information, coupled with a total absence of fair standards, first undermine the confidence of citizens and then lead to the distrust of businesses and governments. The only way to restore this confidence is to promote the participation of all actors in the establishment of fair standards for the treatment of information. Appropriately enough, networks may help in this endeavor. The Infobahn, by its magnifying effect, is at the source of a certain number of critical abuses, especially those regarding secondary and cross-sectoral uses. These abuses themselves are the origin of the reaction we now witness, namely the crisis of confidence of citizens and businesses in the treatment of information. As strange as it may seem, this reaction might be our best chance to reach and enforce key values. The refusal of citizens to be manipulated, the improved behavior of private companies, and a new recognition in Congress of the importance of fair information practices to citizens and the economy could finally constitute enough pressure to cause reconsideration of the old attitude founded on targeted standards, diversity of sources, and self-regulation. Like all good things, however, such a change will no doubt take time, responsibility, and patience.