# Privacy and Democracy in Cyberspace

*Paul M. Schwartz* 52 Vand. L. Rev. 1609 (1999)

*In this Article, Professor Schwartz depicts the widespread, silent collection of personal information in cyberspace. At present, it is impossible to know the fate of the personal data that one generates online. Professor Schwartz argues that this state of affairs degrades the health of a deliberative democracy; it cloaks in dark uncertainty the transmutation of Internet activity into personal information that will follow one into other areas and discourage civic participation. This situation also will have a negative impact on individual self-determination by deterring individuals from engaging in the necessary thinking out loud and deliberation with others upon which choice-making depends.*

*In place of the existing privacy horror show on the Internet, Professor Schwartz seeks to develop multidimensional rules that set out fair information practices for personal data in cyberspace. The necessary rules must establish four requirements: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight. Neither the market nor industry self-regulation are likely, however, to put these four practices in place. Under current conditions, a failure exists in the "privacy market." Moreover, despite the Clinton Administration's endorsement of industry self-regulation, this method is an unlikely candidate for success. Industry self-regulation of privacy is a negotiation about "the rules of play" for the use of personal data. In deciding on these rules, industry is likely to be most interested in protecting its stream of revenues. Therefore, it will benefit if it develops norms that preserve the current status quo of maximum information disclosure.*

*This Article advocates a legislative enactment of the four fair information practices. This legal expression of privacy norms is the best first step in promoting democratic deliberation and individual self-determination in cyberspace. It will further the attainment of cyberspace's potential as a new realm for collaboration in political and personal activities. Enactment of such a federal law would be a decisive move to shape technology so it will further–and not harm–democratic self-governance.*

# Privacy and Democracy in Cyberspace

*Paul M. Schwartz*[*]

INTRODUCTION ..... 1610
I. THE LACK OF PRIVACY IN CYBERSPACE ..... 1616
A. *A Tour of Personal Information Use in Cyberspace* ..... 1617
1. The Technical Infrastructure ..... 1618
2. The Privacy Horror Show ..... 1621
a. *The Personal Computer* ..... 1622
b. *The Internet Service Provider ("ISP")* ..... 1627
c. *Web Sites* ..... 1629
B. *The Current Legal Response* ..... 1632
C. *The Data Processing Model and the Internet: Cyberspace Meets Real Space* ..... 1640
II. SHARED LIFE AND DEMOCRACY IN CYBERSPACE ..... 1647
A. *Democratic Deliberation* ..... 1648
B. *Individual Self-Determination* ..... 1653
C. *Constitutive Privacy* ..... 1658
III. A MULTIDIMENSIONAL PRIVACY TERRITORY FOR CYBERSPACE ..... 1667
A. *Post's Pessimism* ..... 1667
B. *The Necessary Fair Information Practices* ..... 1670

---

* Professor of Law, Brooklyn Law School. This research was supported by a grant from the Dean's Research Fund of Brooklyn Law School. I wish to thank Dean Joan Wexler for this generous assistance.

For their comments on this Article, I also wish to thank Martin Flaherty, Robert Gellman, Michael J. Gerhardt, Kent Greenfield, Ted Janger, Won Joon Kouh, Amy de Jesus Lauren, Catherine Mangan, Joel R. Reidenberg, Laura J. Schwartz, Spiros Simitis, Peter J. Spiro, William M. Treanor, and Benjamin H. Warnke. Opinions expressed in the Article, however, are my own. Finally, Stefanie Schwartz provided the essential encouragement that made this project possible.

1. A Fabric of Defined Obligations ..... 1672
2. Transparent Processing Systems ..... 1676
3. Limited Procedural and Substantive Rights ..... 1677
4. Establishment of Independent Oversight ..... 1679
C. *The Creation of Fair Information Practices: The Market, Self-Regulation, and Law* ..... 1681
1. Let's Make A Deal: The Privacy Market ..... 1681
2. Industry Knows Best: Self-Regulatory Mechanisms ..... 1687
3. The Law's Domain ..... 1696
CONCLUSION ..... 1701

A right to privacy is not generally recognized on the Internet.[1]

## INTRODUCTION

Cyberspace is our new arena for public and private activities. It reveals information technology's great promise: to form new links between people and to marshal these connections to increase collaboration in political and other activities that promote democratic community.[2] In particular, cyberspace has a tremendous potential to revitalize democratic self-governance at a time when a declining level of participation in communal life endangers civil society in the United States.[3]

Yet, information technology in cyberspace also affects privacy in ways that are dramatically different from anything previously possible.[4] By generating comprehensive records of online behavior,

1. MICROSOFT PRESS COMPUTER DICTIONARY 382 (3d ed. 1997).

2. The Supreme Court invoked cyberspace's potential contribution to democratic community in *Reno v. ACLU* where it spoke of the "vast democratic fora of the Internet." 521 U.S. 844, 868 (1997). It also noted cyberspace's creation of a "dynamic, multifaceted category of communication" with unlimited possibilities for speech. *Id.* at 870; *see infra* Part II; *see also* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1407 (1996) (explaining that cyberspace "is a space filled with community").

3. *See infra* Part II.A.

4. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE at vii (1998) (stating

information technology can broadcast an individual's secrets in ways that she can neither anticipate nor control.[5] Once linked to the Internet, the computer on our desk becomes a potential recorder and betrayer of our confidences. In the absence of strong privacy rules, cyberspace's civic potential will never be attained.

At present, however, no successful standards, legal or otherwise, exist for limiting the collection and utilization of personal data in cyberspace.[6] The lack of appropriate and enforceable privacy norms poses a significant threat to democracy in the emerging Information Age. Indeed, information privacy concerns are the leading reason why individuals not on the Internet are choosing to stay off.[7]

The stakes are enormous; the norms that we develop for personal data use on the Internet will play an essential role in shaping democracy in the Information Age. Nevertheless, the Clinton Administration and legal commentators increasingly view the role of the Internet law of privacy as facilitating wealth-creating transmissions of information, including those of personal data.[8] This Article

---

that "[t]he Internet has made it easier for anyone to collect personal information about others . . ."); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998) (explaining that in cyberspace, "you are invisibly stamped with a bar code").

5. *See infra* Part I.A.2.

6. *See infra* Part I.B.

7. *See A Little Privacy, Please*, BUS. WK., Mar. 16, 1998, at 98 [hereinafter BUSINESS WEEK Poll]. This Business Week/Harris poll also found that of people who already use the Internet, "78% say they would use the Web more if privacy were guaranteed." *Id.*

The Graphic, Visualization, and Usability Center's ("GVU") Tenth World Wide Web User Survey also revealed a high level of public concern for information privacy. Graphic, Visualization & Usability Center, *Tenth World Wide Web Survey Results* (visited Oct. 1998) <http:www.gvu.gatech.edu/user_surveys/>. This survey, which relied on the self-reporting of visitors to the GVU Web site, found that over seventy-five percent of Internet users rated privacy as more important than convenience, and seventy percent agreed that a need existed for Internet privacy laws. *Id.* In addition, eighty percent of Internet users disagreed that content providers had a right to resell user information. *Id.*

Americans are also highly concerned with privacy issues when they are off-line. For example, a 1996 poll found that eighty-nine percent of Americans were either very or somewhat concerned about threats to their personal privacy. *See* Alan F. Westin, *"Whatever Works": The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, *in* NATIONAL TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 55 (1997) [hereinafter NTIA REPORT]. This poll also found that "[a] rising large percentage of the public feels that consumers have 'lost all control over how personal information about them is circulated and used by companies.'" *Id.*

8. For the views of the Clinton Administration, see U.S. GOV'T WORKING GROUP ON ELEC. COMMERCE, 1998 ANN. REP. [hereinafter WORKING GROUP ON E-COMMERCE] (stating that "[e]lectronic commerce should be a market-driven arena and not a regulated one" and the role of government is to "support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce."); *The White House, A Framework for Global Electronic Commerce*, Principles, § 2 (1997) <http://www.whitehouse.gov/WH/New/Commerce/read.html> (explaining

takes a different tack. It does not oppose a commercial function for cyberspace, but calls for something other than shopping on the Internet. Moreover, it argues that unfettered participation in democratic and other fora in cyberspace will not take place without the right kinds of legal limits on access to personal information.[9]

This Article seeks to advance the current debate about privacy and democracy in cyberspace through three lines of inquiry. The first concerns privacy risks on the Internet. Part I describes the privacy horror show currently existing in cyberspace and shows that the law has not responded with effective standards for personal data use.[10] The Article then puts these developments into a broader context by analyzing the emerging relationship between personal information use on the Internet and similar activities in the area that people in cyberspace call "Real Space."[11] The Article finds that the Internet creates a model for decisionmaking through personal data use that shifts power to private organizations and public bureaucracies. In particular, the lack of knowledge about personal data use allows the capture of information that might never be generated if individuals had a better sense of the Internet's data privacy zones. This ignorance allows bureaucratic decisionmaking to be extended into new areas in a stealth-like process unaccompanied by societal debate. It permits the creation of a new power structure in which scant room exists for privacy.

This Article's second line of inquiry evaluates the impact of this new power structure on cyberspace and shared life in the United States. Part II utilizes civic republican theory to argue that cyberspace has the potential to emerge as an essential center of communal

---

that "[p]arties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention").

For the views of academic commentators regarding the centrality of wealth creation on the Internet, see SWIRE & LITAN, *supra* note 4, at 88 (stating that "[while] people will engage in more electronic commerce if they believe their privacy will be protected[,]" at the same time "[a]ny such increases may be offset by the decreases in commerce that can occur because of interference with the free market"); Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 210-213 (1996) (emphasizing the essential role in cyberspace of "private transactions" and the establishment of property rights, "without which welfare-increasing bargains cannot occur"); see also Justin Mattick, *The Future of the Net: Don't Restrain Trade in Information*, WALL ST. J., Dec. 2, 1998, at A22 ("New privacy regulations would be at best redundant. At worst, they would raise the start-up costs of Web-based businesses . . . that don't need privacy policies.").

9. *See infra* Part III.C.3.

10. *See infra* Parts I.A-B.

11. *See infra* Part I.C.

activities and political participation.[12] Yet, poor privacy standards in cyberspace raise two threats to this promise: first, by discouraging participation in deliberative democracy; and second, by undercutting the development and maintenance of an individual's capacity for self-governance.[13] Both negative impacts are significant because democracy in the United States depends on group deliberation as well as individuals who are capable of self-determination.

This line of inquiry culminates in the development of a theory of constitutive privacy.[14] Development of this theory involves an exploration of the inadequacies of the traditional liberal understanding of information privacy, which views privacy as a right to control the use of one's personal data.[15] Building on the important scholarship of Robert Post, the Article then argues that information privacy is best conceived of as a constitutive element of civil society.[16] The Internet's potential to improve shared life in the United States will be squan-

---

12. *See infra* Part II.

13. *See infra* Parts II.A-B.

14. *See infra* Part II.C.

15. As the Supreme Court has observed, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1988).

For further examples of use of the paradigm of privacy-control by governmental entities, see, GENERAL ACCOUNTING OFFICE, MEDICAL RECORDS PRIVACY 4 n.4 (Feb. 1999) ("Privacy refers to the specific right of an individual to control the collection, use, and disclosure of personal information."); INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 5 (1995) [hereinafter IITF PRIVACY PRINCIPLES] (asserting that information privacy is "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed and used").

For examples of use of the paradigm of privacy-control by academics, *see, e.g.*, COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 26 (1992) ("For virtually every commentator, however, the fundamental issue has been the loss of human dignity, autonomy, or respect that results from a loss of control over personal information."); PRISCILLA M. REGAN, LEGISLATING PRIVACY 4 (1995) (noting her use of "the definition of privacy that has provided the basis for most policy discussions in the United States, namely that privacy is the right to control information about and access to oneself") (footnote omitted); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); Richard A. Posner, *Privacy*, *in* THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 103, 104 (Peter Newman ed., 1998) (stating that "economic analysis of the law of privacy . . . should focus on those aspects of privacy law that are concerned with the control by individuals of the dissemination of information about themselves"); Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 556 (1998) ("The privacy interest I address here is the power to control the facts about one's life.").

16. *See* ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 51-88 (1995) [hereinafter POST, CONSTITUTIONAL DOMAINS]; Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989) [hereinafter Post, *Social Foundations*].

dered unless we structure the kinds of information use necessary for democratic community and individual self-governance.[17] Participants in cyberspace need access to public, quasi-public and private "spaces" where they can engage in civic dialogue and the process of individual self-definition. Creation of such spaces requires the development of privacy norms that fulfill a constitutive function; these rules must draw on adequately complex coordinates to structure the personal data use of different entities.

This Article's third line of inquiry concerns the content of these "multidimensional" coordinates of constitutive privacy and the best method of creating these norms for the Internet.[18] Part III begins with Robert Post's pessimistic conclusions regarding the shaping of privacy rules under contemporary conditions.[19] For Post, "social life increasingly lacks the characteristics which are necessary to generate privacy rules."[20] He finds that the necessary "textured or dense" relationships that sustain vital behavioral rules are missing from our world, which is marked by interactions with impersonal institutions.[21] The current low level of privacy in cyberspace seems to confirm Post's analysis.[22]

This Article's response to Post draws on the idea of "fair information practices" as a necessary part of the development of a multidimensional Internet privacy territory.[23] Fair information practices are the building blocks of modern information privacy law. They are centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight.[24]

---

17. *See infra* Part II.B-C.

18. *See infra* Part III.

19. *See* Post, *Social Foundations*, *supra* note 16, at 1009-10.

20. *Id.* at 1009.

21. *Id.* Post argues, "privacy is for us a living reality only because we enjoy a certain kind of communal existence." *Id.* at 1010.

22. *See* MICROSOFT DICTIONARY, *supra* note 1, at 382. As this dictionary succinctly states, "[a] right to privacy is not generally recognized on the Internet." *Id.*

23. *See infra* Part III.

24. The idea of fair information practices has been present in information privacy law and policy since the era of mainframe computers in the 1970s. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306-08 (1989); THE PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 14-15, 500-02 (1977) [hereinafter PRIVACY STUDY COMM'N] (providing a description of early proposals regarding fair information practices).

For a more recent governmental discussion of a somewhat different set of fair information practices, see FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7-14 (June 1998).

The use of these four standards, bolstered by the concept of mandatory and default rules, allows the depiction of coordinates for a multidimensional privacy territory for personal data in cyberspace.[25]

Finally, Part III concludes with an analysis of the best manner in which to establish this privacy territory.[26] This analysis centers on the current policy debate regarding three potential, and potentially overlapping, regulatory techniques for Internet privacy. These techniques look to: (1) the market; (2) industry self-regulation; and, (3) the law's imposition of standards. Of these options for privacy protection, industry self-regulation is the most popular policy alternative for the Clinton Administration at present.[27] Yet, Congress has indicated a modest preference for the third option by enacting a law to protect children's privacy on the Internet.[28] In the closing days of the last Congress, President Clinton cooperated in this creation of legal standards by signing this privacy law for one small corner of cyberspace.[29]

This Article's conclusion is that all three of these techniques, including self-regulation, have an important role in developing effective privacy norms. Under current conditions in cyberspace, however, it is the law's imposition of standards that is of essential importance.[30] A statutory expression of privacy norms for cyberspace will be the most effective first step in promoting democratic deliberation and individual self-determination in this new realm.[31] This legal action will lead to three significant benefits: (1) the prevention of a lock-in of poor privacy standards on a societal level; (2) the creation of preconditions for effective market and self-regulatory contributions to privacy

---

For examples of my own previous analysis of fair information practices as the building blocks of information privacy, see Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 56-67 (1997) [hereinafter Schwartz, *Privacy Economics*]; Paul M. Schwartz, *Privacy and Participation*, 80 IOWA L. REV. 553, 563-564 (1995) [hereinafter Schwartz, *Participation*].

25. *See infra* Part III.B.

26. *See infra* Part III.C.

27. *See* WORKING GROUP ON E-COMMERCE, *supra* note 8, at iv (describing the"President's proposals for private sector leadership and self-regulation of the Internet"). Nevertheless, the Clinton Administration has also stated that the government should take action "through law or regulation . . . to protect the privacy of especially sensitive information and to prevent predatory practices." *Id.* at 17; *see also* Ken Magill, *Gore's Privacy Plans Signal No Clear Agenda: White House 'still ducking the hard problems,'* DM NEWS, Aug. 10, 1998, at 1 (stating that "people from all sides of the [privacy] debate are struggling to find where their agendas fall on the White House scorecard.").

28. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1999).

29. *See id.*

30. *See infra* Part III.C.3.

31. *See id.*

protection; and (3) the termination of United States intransigence on the wrong side of ongoing negotiations with the European Union about trans-Atlantic transfers of personal data.[32] The good news is that it is not too late to develop privacy rules for cyberspace; the bad news is that the cost of delay will be high.[33]

## I. THE LACK OF PRIVACY IN CYBERSPACE

The Internet is growing at a rate that outpaces any modern medium of communication.[34] Television took thirty-five years to reach thirty percent of households in the United States. The Internet's World Wide Web ("Web") is expected to achieve this degree of market penetration a mere eight years after its popular debut.[35] Indeed, one recent study predicts that by the end of the year 2000 over 100 million Americans will be "surfing" the Web on a regular basis.[36] In comparison, at the end of 1998, 57 million Americans were utilizing the Internet.[37] As more Americans go online, this electronic medium is of increasing significance for this country—it is the new arena for public and private life in the United States. Millions of people now seek connections with other individuals in cyberspace through activities that both track real world behavior and assume dimensions unique to this electronic setting.[38]

This Article begins with a brief three-part tour of this new and powerful communication medium. First, it examines the current technical infrastructure of cyberspace and the kinds of privacy abuses that occur on the Internet.[39] This Section is foundational: due to the newness and complexity of this medium, a legal analysis of cyberprivacy depends on an understanding of the underlying communication technologies and existing practices. The second part of the tour

---

32. *See id.*

33. *See infra* text accompanying note 517.

34. *See* U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY 4 (1998) ("The Internet's pace of adoption eclipses all other technologies that preceded it.").

35. PAINE WEBBER, CONVERGING TECHNOLOGIES: INVESTING IN THE INFORMATION AGE FOR THE NEW MILLENNIUM 9 (1998).

36. Perry H. Roth, *Internet Industry*, VALUE LINE, June 4, 1998, at 2219.

37. *Id.*

38. *See* Reno v. ACLU, 521 U.S. 844, 868-73 (1997) (describing some of the myriad forms on online behavior); SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 186-209 (1995).

39. *See infra* Part I.A.

discusses the current legal response to this technology and these privacy abuses. Finally, the third part of the tour contrasts the use of personal information in cyberspace with off-line processing. This part examines personal data use in Real Space.[40]

A description of this Article's later argument will increase the benefit of the Internet tour. The Internet, if accompanied by the right kind of legal rules for access to personal data, has tremendous potential to become a space for social and individual deliberation. Yet, cyberspace's territories for civic dialogue and individual self-definition must be structured through enforceable privacy standards that mark where different areas begin and end. In the following Section, this Article will show that the necessary kinds of privacy territories currently do not exist on the Internet and that the law does not provide rules capable of structuring such areas. Indeed, the Clinton Administration, largely interested in making the Web and the world safe for electronic commerce, is deferring to industry's self-regulatory efforts regarding privacy.[41]

### *A. A Tour of Personal Information Use in Cyberspace*

This Article's Internet tour starts by defining two terms. William Gibson coined the first term, "cyberspace," calling it "a consensual hallucination."[42] A more prosaic definition would describe cyberspace as the environment created for communication and other activities through interconnected computers.[43] Cyberspace makes the transmission of data more efficient and less expensive than ever before by permitting digital communication at the speed of light and largely independent of geographical constraints.[44]

The second definition is of "personal information." This term refers to any collection of characters or signals that one can use to identify a specific individual. In the Information Age, we leave extensive data trails, some initially anonymous, which can be linked to a person later.[45] Congress recognized this point as early as 1974 when

---

40. *See infra* Part I.C.

41. *See infra* text accompanying notes 199-205.

42. WILLIAM GIBSON, NEUROMANCER 51 (1984).

43. *See Reno*, 521 U.S. at 844-49; NATHAN J. MULLER, DESKTOP ENCYCLOPEDIA OF THE INTERNET 168-70 (1998).

44. *See Reno*, 521 U.S. at 849-54.

45. For example, clickstream data that a Web site collects can sometimes be linked to an individual. *See infra* Part I.A.2.b.

it enacted the Privacy Act.[46] This law broadly defines a "record about an individual" as "any item, collection, or grouping of information about an individual."[47] The Privacy Act further states that such a "record" can be an "identifying number, symbol or other identifying particular assigned to the individual."[48] As this statutory approach suggests, the term "personal information" inescapably reflects a conclusion that the data at stake are traceable to a specific person. At some point, however, information must be considered nonpersonal because of the amount and kind of effort necessary to link it to one individual and the improbability of such an endeavor. This Article is explicit, therefore, in admitting the inevitable contextuality of the term, "personal information."

### 1. The Technical Infrastructure

As currently organized, cyberspace depends upon a definite technical infrastructure. Specifically, cyberspace is constructed through the Internet's linking of computers. As the Supreme Court noted in *Reno v. ACLU*, cyberspace is "available to anyone, anywhere in the world, with access to the Internet."[49] The Internet is the worldwide collection of computer networks and gateways that utilizes TCP/IP, a specific set of software protocols for communication.[50] Put more simply, the Internet is a network of linked computers including all the millions of personal computers that are connected to it.[51] The Internet is the outgrowth of a government program called ARPANET, which was created to enable transfers of data between computers operated by the military, defense contractors, and universities.[52]

At the heart of the Internet are high speed data communication lines between major host computers, also called nodes, that route data and messages.[53] Yet, most people consider one standardized

---

46. 5 U.S.C. § 552a (1994).
47. *Id.* § 552a(a)(4).
48. *Id.* The Privacy Act, despite notable flaws, represents the most comprehensive attempt to structure information processing within the public sector. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 92 (1996). It applies, however, only to federal agencies. *Id.* at 92-93.
49. *Reno*, 521 U.S. at 851.
50. *See id.* at 849-50.
51. *See* MULLER, *supra* note 43, at 168-70.
52. *See id.* For a more complete history, see KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 43-218 (1996).
53. *See* MICROSOFT DICTIONARY, *supra* note 1, at 331.

format for transmitting documents as forming cyberspace; it is this standardized format that permits the World Wide Web ("Web") to function.[54] The Web is the total set of interlinked documents residing on Hypertext Transfer Protocol ("HTTP") Servers throughout the world.[55] Documents on the Web are written in Hypertext Markup Language ("HTML") and identified by Uniform Resource Locators ("URL's").[56] The Web's technical specifications make it particularly useful for presenting visual and multimedia information, as well as providing access through hypertext links to different documents.[57]

In an age where the key wealth-creating activity in the United States concerns the production, distribution, and manipulation of information,[58] the Internet is destined for a prominent role. This prominence is due to this medium's impressive ability to increase the speed and lower the costs of transferring and sharing information. This Article has already noted the Web's use of HTML and URL's, which greatly simplify the linking and location of information organized as Web pages.[59] Also significant for the Internet are packet switching, statistical sharing, and interoperability.[60] As a result of

---

54. *See Reno*, 521 U.S. at 852 ("The best known category of communication over the Internet is the World Wide Web."). Other methods of communication in cyberspace include electronic mail, automatic mailing list services, and "chat rooms." *Id.* at 849.

55. *See* MULLER, *supra* note 43, at 525.

56. *See id.*

57. *See id.* at 526.

58. *See* JAMES R. BENIGER, THE CONTROL REVOLUTION: TECHNOLOGICAL AND ECONOMIC ORIGINS OF THE INFORMATION SOCIETY 21-22 (1986) (addressing the origins and impact of the information society); FRITZ MACHLUP, THE PRODUCTION AND DISTRIBUTION OF KNOWLEDGE IN THE UNITED STATES 362-76 (1962) (originating the phrase "information society").

59. *See supra* text accompanying note 57.

60. Routing on the Internet is done through packet switching and statistical sharing. *See* Jeffrey K. Mackie-Mason & Hal R. Varian, *Economic FAQs About the Internet, in* INTERNET ECONOMICS 27, 33-34 (Lee McKnight & Joseph Bailey eds., 1997). Packet switching is a data delivery technique that handles information in small units; it breaks down a message into multiple packets that are relayed through stations in a computer network along the best route available between the source and destination. *See id.* at 33. Statistical sharing is the ability to permit packets from many different sources to share a transmission line. *See id.* at 34.

Through packet switching and statistical sharing, the Internet is able to transmit enormous amounts of information in a highly efficient manner. In comparison, most telephone conversations are still handled through circuit switching, which requires that an end-to-end circuit be established before a call can begin and that a fixed share of network resources be reserved for the call. *See id.* at 32. Even when pauses occur in a telephone conversation, telephone network resources are tied up in transmission of the sounds of silence. *See id.*

A further efficiency of the Internet for communication is that it permits inter-operability of computers. *See* Sharon Eisner Gillet & Mitchell Kapor, *The Self-Governing Internet: Coordination by Design, in* COORDINATING THE INTERNET 3, 6-7 (Brian Kahin & James H. Keller eds., 1997). Interoperability means that any computer in cyberspace can interact with any other computor; it occurs because cyberspace rests on a foundation of underlying agreement about

these aspects of its technical infrastructure, every time an additional person goes online, the Internet is able to create widespread benefits from positive network externalities for those already in cyberspace.[61] Network externalities are found in any product whose value depends on how many others make use of it; the more people who send and receive e-mail, for example, the more valuable it becomes for others to utilize this technology.[62]

The Internet's technical qualities also have a negative consequence: they make possible an intense surveillance of activities in cyberspace.[63] Digital reality is constructed through agreement about technical norms. This "code," to use Lawrence Lessig's term, creates cyberspace.[64] As a result of cyberspace code, surfing and other cyberspace behavior generate finely granulated data about an individual's activities—often without her permission or even knowledge.[65]

Technology is not fate, however, and cyberspace can be constructed in any number of fashions. Accordingly, it is neither impossible nor too late to establish effective rules for privacy in cyberspace.[66] Although software and other technical elements of infrastructure help create the conditions for personal data use in cyberspace, these conditions and other aspects of the Internet are malleable.[67] This concept is present in Lessig's notion of "code," and in Joel Reidenberg's parallel proposal, technological configurations and

---

software protocols and other essential issues of infrastructure design. *See id.* As a result, once someone uses a computer to enter cyberspace, operational differences generally are invisible and machines work in technical harmony. *See id.*

61. CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 13-14 (1999). These positive network externalities include an increased access to information, an increased ease of communication, and a decrease in a variety of transaction and overhead costs. *Id.* at 183-84.

62. *Id.* at 184; *See* ROBERT P. MERGES ET. AL, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 845-47 (1997); Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 488 (1998).

63. *See infra* Part I.A.2.

64. Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896 (1996) (explaining Internet software, "[t]his code, like nature, sets the terms upon which I enter or exist in cyberspace").

65. *See infra* Part I.A.2.

66. The danger is, however, that a low-level of privacy will be locked-in on the Internet. *See infra* Part III.C.2.

67. In an analogous fashion, the Telecommunications Act of 1996 views the technical infrastructure available for wired carriers of telephony as malleable. The role of regulation under the Act is te stimulate competition by altering economic and operational market barriers. *See, e.g.*, In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, 11 F.C.C.R. 15499-15505 (FCC 1996) first report and order (ordering that incumbent local telephone companies structure technical infrastructure for local telephony to permit "number portability" for customers who change local carriers).

system design choices constitute a powerful baseline structure of information policy.[68] Reidenberg describes these technical norms as the new "Lex Informatica," or information law, and calls for increased involvement by government and different policy communities in the process of standard-setting for technology.[69] A simple example illustrates the potential flexibility of cyberspace norms. Sherry Turkle, the leading sociologist studying the Internet, has explored the debate in some Multi-User Domains ("MUDs") regarding the use of virtual weapons.[70] MUDs are environments in cyberspace in which multiple users simultaneously participate in role playing games and interact in real time.[71] According to Turkle, "in a virtual world a few lines of [software] code can translate into an absolute gun ban."[72] Although regulation of the use of personal information on the Internet is certainly a more complex task than banning weapons in a specific MUD, Turkle's analysis remains valid.

Her example shows that choices about technology, including the design of software, will have an important role in structuring different kinds of access to our personal data. Unfortunately, as the next Section will demonstrate, current decisions are increasing, rather than decreasing, the quality and quantity of personal data that are processed and disseminated in cyberspace.

### 2. The Privacy Horror Show

The informational consequences of activities in cyberspace result from the generation, storage, and transmission of personal data in three areas: (1) personal computers; (2) Internet Service Providers ("ISPs"); and, (3) Web sites. Visitors to cyberspace sometimes believe that they will be fully able to choose among anonymity, semi-anonymity, and complete disclosure of identity and preferences. Yet, in each of the three areas, finely granulated personal data are created—often in unexpected ways. Moreover, most people are unable

68. Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 556 (1998). For an analysis of the impact of technological configurations within the context of choice-of-law in cyberspace, see Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1213-15 (1998).

69. Reidenberg, *supra* note 68, at 587.

70. *See* TURKLE, *supra* note 38, at 249-50.

71. *See id.* at 11-22.

72. *Id.* at 250.

to control, and are often in ignorance of, the complex processes by which their personal data are created, combined, and sold.

*a. The Personal Computer*

When tied to a network, an individual's personal computer makes access to the Internet available at her desk.[73] For some people, this machine may be no more than a necessary evil; they imagine the computer to be a glorified typewriter. For others, it is an evocative object, perhaps even a kind of friend with whom one can have an intense relationship.[74] The computer is not a silent and loyal friend, however, but more like Linda Tripp, the recorder and betrayer of Monica Lewinsky's confidences.[75] A personal computer records and reveals its users' confidences in a number of ways.

First, information deleted from a personal computer is generally easily recoverable, whether from the machine's hard drive or elsewhere.[76] Lewinsky's own digital experiences provide one example of how computer files may be deleted, but not destroyed. The Office of Independent Counsel's report to the House of Representatives includes numerous e-mails and draft letters, including messages to President Clinton that Lewinsky never intended to send, which were recovered from deleted files on Lewinsky's computer.[77] This recovery was possible because use of a "delete" button on a computer does not destroy the information, but merely hides it from view.

Deletion removes data from the hard disk drive's directory of files and marks the disk space where the file is still stored as avail-

---

73. *See* MULLER, *supra* note 43, at 169.

74. *See* TURKLE, *supra* note 38, at 177-85.

75. As for Linda Tripp, the Office of the Independent Counsel decorously explains, "[s]ome of Ms. Lewinsky's statements about the relationship [with President Clinton] were contemporaneously memorialized." OFFICE OF THE INDEP. COUNSEL, THE STARR REPORT: THE FIND-INGS OF INDEPENDENT COUNSEL KENNETH W. STARR ON PRESIDENT CLINTON AND THE LEWINSKY AFFAIR 34 (1998); *see* Elizabeth Hardwick, *Head Over Heels*, N.Y. REV. BOOKS, Apr. 22, 1999) 6, 8 ("And then Linda Tripp began to record the telephone calls, without permission and illegal in Maryland, where she lived.").

76. *See generally* Peter H. Lewis, *What's on Your Hard Drive?*, N.Y. TIMES, Oct. 8, 1998, at G1.

77. *See* THE STARR REPORT: THE EVIDENCE 448-59 (Phil Kuntz ed., 1998) [hereinafter STARR REPORT EVIDENCE]. The recovery of the deleted material is not perfect; hence, amidst these historical documents are strings of software programming language that inform us that while writing her letters to "Handsome," Lewinsky utilized a computer with Microsoft Word software and a Hewlett-Packard Laser Jet Printer. *Id.* at 431-32. Her recovered e-mails provide soft-ware product information indicating the use of Microsoft Mail. *Id.* at 453.

able for reuse.[78] In time, another file may be written over this area, but in the period before deleted data are overwritten, anyone with access to the computer can locate and restore the deleted file with relatively simple commands found in many software utility programs.[79] Even if files have been written over, or, more drastically, "wiped" by programs that hash over the designated disk space, software utility programs are sometimes capable of recovering the underlying data from the computer.[80]

Moreover, deleted files can be found not only on a personal computer's hard drive but also on another personal computer or elsewhere in a networked system.[81] For example, the Office of the Independent Counsel was able to find e-mails written by Lewinsky on the computer of the friend in Japan to whom she sent these communications.[82] The messages were stored on the hard drive of the friend's computer—some deleted, others undeleted.[83] Furthermore, to point to an example from an earlier political scandal, investigators into the Iran-Contra conspiracy recovered deleted electronic messages written by Oliver North in a government network's back-up records.[84]

As these examples show, a personal computer can betray confidences by failing to destroy files that its users sought to remove by use of a "delete" button. This machine causes a further problem for privacy, however, through its storage of information about Internet activities. Computers' Web browsers, such as Netscape Navigator or Microsoft Internet Explorer, contain software protocols that create files about Web sites that have been visited.[85] Anyone with physical access to a computer can access these data in a matter of seconds

78. *See* RON WHITE, HOW COMPUTERS WORK 78-79 (4th ed. 1999).

79. *See id.*

80. BRYAN PFAFFENBERGER, PROTECT YOUR PRIVACY ON THE INTERNET 182-91 (1997); David S. Bennahum, *Daemon Seed: Old email never dies*, WIRED, May 1999, at 100, 102.

The Office of the Independent Connsel appears to have used such a software program in recovering, for example, drafts of documents that Monica Lewinsky wrote and then deleted from her computer's hard drive. *See* STARR REPORT EVIDENCE, *supra* note 77, at 431; Lewis, *supra* note 76, at G8.

81. *See* MULLER, *supra* note 43, at 38-49, 302-06; Jerry Adler, *When E-Mail Bites Back*, NEWSWEEK, Nov. 23, 1998, at 45 (noting that in its investigation of Microsoft, the Justice Department has obtained "an estimated 3.3 *million* Microsoft documents, including megabytes of e-mail messages dating from the early 1990s—and is using them to contradict Gate's own videotaped testimony in the most significant antitrust case of the decade").

82. STARR REPORT EVIDENCE, *supra* note 77, at 438-55.

83. *Id.*

84. *See* LAWRENCE E. WALSH, FIREWALL: THE IRAN-CONTRA CONSPIRACY AND COVER-UP 76 (1997).

85. *See* BRIAN UNDERDAHL & EDWARD WILLETT, INTERNET BIBLE 124-26, 147 (1998).

either by looking at drop down files on the browser's location bar or by accessing the "History" menu item found on both Netscape Navigator or Microsoft Internet Explorer.[86] Even more significantly, remote access to these files is possible from the Internet by exploiting security flaws in Web browsers.[87]

Cyberspace behavior also results in the recording of data in computer cache files. In order to increase the computer's speed of access to information, these special memory subsystems duplicate frequently used data values, such as Web pages frequently visited.[88] Cache files exist on a computer's hard drive and, more temporarily, in its random access memory ("RAM").[89] From the Web, it is possible to access cache files through "JavaScripts" and "Java applets" that permit the remote uploading of these files.[90] These terms refer to programming languages for writing Web applications; both allow routines to be executed on an individual's personal computer remotely from the Web.[91]

A final way that personal computers linked to the Internet can reveal confidences is by their acceptance of "cookies," also known as "persistent client-side hypertext transfer protocol files."[92] These terms refer to identification tags and other blocks of data that a Web site sends to and stores on the hard drive of the computer of anyone who visits it.[93] When an individual returns to this same site at a later date, her browser automatically sends a copy of the cookie back to the Web site; the data identify her as a previous visitor and allow the site to match her to details regarding her prior visit.[94] As the *Microsoft Computing Dictionary* explains, "[c]ookies are used to identify users, to instruct the server to send a customized version of the requested Web page, to submit account information for the user, and for other administrative purposes."[95] This definition is, however, misleadingly

---

86. *See id.*
87. *See* PFAFFENBERGER, *supra* note 80, at 100-07.
88. *See* MICROSOFT DICTIONARY, *supra* note 1, at 72.
89. *See id.*
90. *See* MULLER, *supra* note 43, at 242-46; PFAFFENBERGER, *supra* note 80, at 105-20.
91. *See* PFAFFENBERGER, *supra* note 80, at 112-20.
92. MICROSOFT DICTIONARY, *supra* note 1, at 119. Somewhat confusingly, the disks found inside a standard floppy disk case or a zip drive are also called "cookies." WHITE, *supra* note 78, at 104.
93. *See Persistent Cookie FAQ* (visited Sept. 2, 1999) <http://www.cookiecentral.com/-faq.htm>.
94. *See id.*
95. *See id.* For another technical discussion, see MULLER, *supra* note 43, at 45.

soothing: cookies are a ready source of detailed information about personal online habits.

To begin with, anyone who sits at another's computer or has remote access to it through an internal network can examine the machine's cookies to gain the names of the Web sites that placed these blocks of data.[96] In addition, access to the cookies placed on one's computer is available from the Internet.[97] Cookies are designed to report back exclusively to the Web site that placed them and to reveal only a particular identification number assigned by that site on previous visits.[98] Nevertheless, access to cookies from the Internet can turn this numerical tag and information associated with it into "personal information." Once Web sites identify a specific visitor, they can match her to their rich stores of "clickstream data," which is information about the precise path a user takes while browsing at a Web site, including how long she spent at any part of a site.[99] Such finely grained information exists because, after all, a person only "moves" about cyberspace by means of a series of digital commands that her computer sends to HTTP servers.[100]

A Web site's collection of the names and addresses of its visitors is one way that this linkage takes place. One way that this linkage takes place is by a Web site's collection of the names and addresses of its visitors, which often occurs through different kinds of registration requirements or through participation in a sweepstake at the site.[101] Disclosure is not generally made, however, regarding the consequences of registration or participation in these sweepstakes.[102] In addition, some browsers can be set to provide one's name and home

96. *See* MICROSOFT DICTIONARY, *supra* note 1, at 92 (providing a definition of "clickstream" data); *Persistent Cookie FAQ*, *supra* note 93 ("The information that people reveal to each Web site they visit can be used by system administrators to build extensive personal profiles of visitors.");

97. *See* PFAFFENBERGER, *supra* note 80, at 79-85; *Cookie Values* (visited Sept. 2, 1999) <http://www.cookiecentral.com/mim03.htm> .

98. *Persistent Cookie FAQ*, *supra* note 93.

99. MICROSOFT DICTIONARY, *supra* note 1, at 92; UNDERDAHL & WILLETT, supra note 85, at 244.

100. *See* Kang, *supra* note 4, at 1223-29 (providing a cogent description of the technical issues).

101. *See* FTC, *supra* note 24, at 3; PFAFFENBERGER, *supra* note 80, at 56-59; SHAPIRO & VARIAN, *supra* note 61, at 34-37.

102. *See* James Glave, *Wired News Privacy Report Card* (visited Dec. 22, 1998) <http://-www.wired.com/news/print_version/politics/story/16963.html>.

address, thereby furnishing another means for the site that set the cookie to identify a specific computer user.[103]

As for technical limitations aimed at restricting the reading of a cookie to the Web site that set it, these can be made ineffectual. At the simplest level, nothing forbids the company that set a cookie from using it to gather personal data and then selling this information to third parties or sharing it with an affiliate.[104] In addition, under the right circumstances, a third party can gain information from a cookie without recourse to the company that set it. Because most cookies are placed in the same disk files, third parties on the Web can use malicious code to upload the contents of an entire cookies file.[105] Moreover, a series of different software "bugs" permit the overriding of restrictions set on the sharing of cookies.[106] Finally, a recent news story reported that some existing cookie files are accidentally being transmitted to Web sites other than the ones that set them.[107] In some cases, these transmitted data include identification information, including PINs (Personal Identity Numbers), used at the site that set the cookie.[108] The current best explanation for this software problem is that computer crashes or other hardware problems "corrupted" the cookie files.[109]

---

103. *See* Netscape, *Cookies and Privacy Frequently Asked Questions* (visited Sept. 2, 1999) <http://www.home.netscape.com/products/security/resources/faq.cookies.html> (explaining that "cookies can be used to store any information that the user volunteers").

104. As an example, Microsoft purchased Hotmail, a free Internet e-mail service, to gain access to Hotmail's existing customer base of 9.5 million subscribers. *See Microsoft Finds Free Email for MSN* (visited Jan. 2, 1998) <http://www.wired.com/news/news/business/story/-9450.html>. Since Microsoft's purchase of this company at the end of 1997, Hotmail has grown to 28 million accounts. Polly Sprenger, *Hotel Hotmail* (visited Mar. 22, 1999) <http://www.wired.com/-news/news/business/story/18617.html>.

A more recent information-driven Internet business transaction involves Universal Music and BMG; these companies seek "to use the interactive nature of the Internet to gather the names and E-mail addresses of their customers so they can sell more music to them by artists they already like and to introduce them to new ones." Saul Hansell, *Key to Music Deal is E-Promotion*, N.Y. TIMES, Apr. 8, 1999, at C4.

105. For example, Netscape Communicator stores cookies on individual PCs at C:\Program Files\Netscape\Users\user\cookies.txt. *See* UNDERDAHL & WILLET, *supra* noto 85, at 232-34; Kang, *supra* note 4, at 1228 n.147.

106. *See Cookie Exploit* (visitod Dec. 14, 1998) <http://www.cookiecentral.com/bug/-index.shtml>; Chris Oakes, *Browser Privacy Fix Fails* (visited Oct. 7, 1998) <http://www.wired-com/-news/print_version/technology/story/15459.html.

107. *See What's in them Cookies? Web Site is Finding Out*, PRIVACY TIMES, Feb. 15, 1999, at 1.

108. *See id.*

109. *Id.* at 2.

*b. The Internet Service Provider ("ISP")*

As this Article has noted, the Internet is a worldwide network of networks. Access to the Internet generally requires an individual to utilize an ISP, which is the entity that supplies Internet connectivity.[110] ISPs can take roughly two forms. First, commercial entities, such as American Online ("AOL"), provide access to the Internet for a monthly fee.[111] Second, other entities, such as employers or schools, supply Internet access, often without a fee; these bodies either function directly as an ISP or outsource this task to another company.[112]

ISPs obtain access to detailed, and sometimes highly sensitive information about their customers' behavior on the Internet. ISPs can combine these data with profiling information, which their clients share with them, as well as with information purchased from direct marketing companies.[113] Many outside entities, both governmental and commercial, are increasingly seeking access to these rich databases of personal information.[114]

ISPs are in an advantageous position to tie together the information that exists about anyone who surfs the Web. First, the ISP has highly accurate data about the identity of anyone who uses its services. This information is within its grasp because the ISP generally collects the client's name, address, phone number, and credit card number at the time it assigns an account.[115] Second, the ISP has detailed information about the Internet behavior of each of its customers. Through its role as an entrance ramp to the Internet, the ISP gains access to clickstream data and other kinds of detailed information about personal online habits.[116] It can easily take these scattered bits of cyberspace data, pieces of which at times enjoy different degrees of practical obscurity, and make them into "personal information" by linking them to the identity of its customers.[117]

---

110. *See* MULLER, *supra* note 43, at 197-99.

111. *See* Stephen E. Jones, *American Online*, VALUE LINE, June 4, 1999, at 2221.

112. For an example of a company taking this ISP role, see Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1996). *See also* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1748-49 (1995) (noting how a systems operator at a university can monitor activities of students and faculty on the Internet).

113. *See* PFAFFENBERGER, *supra* note 80, at 32-33.

114. *See* Edward C. Baig et al., *Privacy*, BUS. WK., Apr. 5, 1999, at 84 ("Personal details are acquiring enormous financial value. They are the new currency of the digital economy.").

115. *See* PFAFFENBERGER, *supra* note 80, at 32-33.

116. *See* Kang, *supra* noto 4, at 1233.

117. *See id.*

A recent federal case, *McVeigh v. Cohen*,[118] provides an excellent illustration of the ISP's central role in Internet privacy. For our immediate purposes, *McVeigh* is significant for its depiction of how ISPs can tie information about people's identity offline to data about their behavior online. This Article will explore other aspects of this significant decision in later sections.[119]

*McVeigh* involved AOL, the chief provider of Internet access in the United States with over nineteen million subscribers.[120] In 1996, AOL surrendered subscriber information about Timothy McVeigh, one of its customers, to the United States Navy, which believed that these data gave it grounds to court-martial him.[121] The contested investigation had started because McVeigh, a highly decorated enlisted man assigned to a nuclear submarine, had sent an e-mail to a crew member's wife, who was a volunteer for a charity.[122] AOL provides its subscribers with up to five different e-mail names, or "aliases," per account; McVeigh used his AOL account to join in a charity drive, but inadvertently sent his communication under his e-mail name "boysrch."[123]

Through an option available to AOL subscribers, the crew member's wife searched through the "member profile directory" to locate additional information about the sender of this e-mail.[124] Although this profile did not include his full name, address, or phone number, it specified that "boysrch" was an AOL subscriber named Tim, who lived in Honolulu, worked in the military, and identified his marital status as "gay."[125] At this moment, the ISP's role became critical. Once McVeigh's e-mail and the directory information were brought to the Navy's attention, a military investigator promptly contacted AOL.[126] Without identifying himself as representing the government, the investigator explained that he wished to find out the identity of "boysrch."[127] Despite its established policy otherwise, AOL

118. McVeigh v. Cohen, 983 F. Supp 215 (D.D.C. 1998). For Judge Sporkin's decision reinstating the order in *McVeigh*, see *McVeigh v. Cohen*, 996 F. Supp. 59 (D.D.C. 1998).

119. *See infra* text accompanying notes 172-79; 232; 295-99.

120. *See* Jones, *supra* note 111, at 2230.

121. *McVeigh*, 983 F. Supp. at 217-18. This Timothy R. McVeigh is not related to the Oklahoma City bomber. *Id.* at 216.

122. *Id.* at 217.

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

promptly turned over subscriber data that linked McVeigh to this specific account.[128] This disclosure fits in with a pattern of behavior on AOL's part; it has sold different kinds of subscriber information to third parties, such as direct marketers, and even proposed sale of home phone numbers before a storm of protest forced it to change this plan.[129]

*c. Web Sites*

Web sites are the third and final locus for the collection of personal information in cyberspace. According to a recent survey by the Federal Trade Commission ("FTC"), up to eighty-five percent of Web sites collect personal information from consumers.[130] A widespread capture, sharing, and commercialization of personal data take place on this part of the Internet. As this Article has noted, Web sites collect personal data through cookies, registration forms, and sweepstakes that require surrendering e-mail addresses and other information.[131] Other invasions of privacy relating to Web sites involve archives of comments made on the "Usenet" or to "list servs";[132] the deceptive promises that Web sites sometimes make about privacy practices;[133] and, finally, an increase by Web sites of the availability of information about behavior both in cyberspace and in Real Space.[134] These additional problem areas will now be examined in turn.

---

128. *See id. See AOL Admits Error in Gay Sailor Case,* N.Y. TIMES ON THE WEB 1 (Jan. 21, 1998) <http://www.nytimes.com/aponline/w/AP-Navy-Gay-Dismissal.html>.

129. Seth Schiesel, *American Online Backs Off Plan to Give Out Phone Numbers,* N.Y. TIMES ON THE WEB 1-3 (July 25, 1997) <http://www.nytimes.com/library/cyber/week/-072597aol.htm>; Evan Hendricks, *American Online Snoops Into Subscribers' Incomes, Children,* PRIVACY TIMES, Dec. 15, 1997, at 1-3.

130. FTC, *supra* note 24, at iii.

131. *See supra* text accompanying notes 88-109.

132. *See infra* text accompanying notes 135-37.

133. *See infra* text accompanying notes 141-46.

134. A further threat to privacy at many Web sites is unintentional; it arises from the low level of data security in this part of the Internet. "Data security" refers to the extent to which a computer system and its data are protected from unauthorized access. UNDERDAHL & WILLETT, *supra* note 85, at 240.

At present, data security is often a low priority for Web sites. In one recent incident, CBS SportsLine mistakenly made public the personal information that contestants in a sweepstakes had given to it. *See* Craig Bicknell, *SportsLine Contestants Exposed* (visited Dec. 19, 1998) <http:www.-wired.com/news/print_version/politics/story/16939.html>. These data, which included home addresses and phone numbers, were posted on a publicly available part of its Web site. *Id.* Although CBS SportsLine corrected this error once alerted to it, this incident accurately indicates the often glaring mistakes that reduce data security on much of the Web. *See Id.*

Participation on the "Usenet" or in a "list serv" has significant informational consequences. The Usenet allows participants to post communications into a database that others can access; list servs are listings of names and e-mail addresses that are grouped under a single name.[135] Although sending messages to these areas feels like an ephemeral activity, an individual may be creating a permanent record of her opinions. Transcripts of contributions to both the Usenet and list servs are sometimes collected and archived, often without disclosure to participants and without restrictions on further use.[136] One such catalogue of these comments, "www.deja.com," provides four different archives, including one for "adult" messages.[137]

The FTC's recent enforcement action against the GeoCities company provides a further illustration of weak privacy practices at Web sites.[138] GeoCities markets itself as a "virtual community"; it organizes its members' home pages into forty different areas, termed "neighborhoods."[139] In these areas, members can post a personal Web page, receive e-mail, and participate in chat rooms.[140] Non-members can also visit many areas of GeoCities.

According to the FTC, GeoCities engaged in two kinds of deceptive practices in connection with its collection and use of personal information.[141] First, although GeoCities promised a limited use of the data it collected, it in fact sold, rented, and otherwise disclosed this information to third parties who used it for purposes well beyond those for which individuals had given permission.[142] Second, GeoCities promised that it would be responsible for maintenance of the data

---

This incident was the consequence of sloppy management. Other security problems are caused by technical flaws at many Web sites. For more information on recent data security lapses at Web sites, see James Glave, *GM Recalls Faulty Web Site* (visited Mar. 19, 1999) <http:www.wired.com/news/print_version/politics/story/18602.html>; James Glave, *TV Site Reveals Personal Data,* (visited Jan. 20, 1999) <http:www.wired.com/news/print_version/-chnology/story/17437.html>.

135. *See* MICROSOFT DICTIONARY, *supra* note 1, at 286; MULLER, *supra* note 43, at 32-37; UNDERDAHL & WILLETT, *supra* note 85, at 501-20.

136. *See, e.g., Deja.com* (visited Sept. 3, 1999) <http://www.deja.com>.

137. *Id.*

138. *See* GeoCities, File No. 9823015 (Fed. Trade Comm. 1998) (agreement containing consent order). The Geo-Cities Consent Order can also be found at <http://www.ftc.gov/os/1998/-9808/geo-ord.htm>.

139. For a discussion, *see* FTC, *Analysis of Proposed Consent Order to Aid Public Comment* (visited Aug. 1998) <http:www.ftc.gov/os/1998/9808/9823015.-ana.htm>. The GeoCities Web site is located at <http://www.geocities.com> (visited Sept. 3, 1999).

140. FTC, *supra* note 139.

141. *Id.*

142. *Id.*

collected from children in the "Enchanted Forest" part of its Web site.[143] Instead, it turned such personal information over to third parties, whom it had dubbed "community leaders."[144] As this Article will discuss in its next Section, the FTC's settlement with GeoCities left both kinds of behavior elsewhere on the Web largely unaffected.[145] Through the enactment of the Children's Online Privacy Protection Act in 1998, however, Congress has created strong pressure to end at least some deceptive practices regarding the collection and use of children's personal data on the Internet.[146] Yet, adults on the Web are unprotected by this law.

A final point remains about Web sites and privacy. Web sites not only provide easy access to data about activities in cyberspace but also increase the availability of information about behavior in Real Space. One example will suffice to illustrate this phenomenon; it concerns the new breeds of "look up" services that are emerging on the Internet. These cyber-reference services offer wide-ranging products at a low cost and without restrictions on their customers.[147] Web-based reference sites have broken free of the norms of traditional "look up" services, which sold their products with at least some restrictions as to the parties with whom they would do business and at least some safeguards placed on the purchasers.[148] In contrast, the new cyber-look up services create limits neither on their market nor on their customers' use of the data they receive.

Web sites with names like "Dig Dirt," "WeSpy4U," and "Snoop Collection" sell medical histories, criminal justice records, educational accomplishments, unlisted telephone numbers, yearly income, bank balances, stocks owned, and a variety of other kinds of financial data.[149] For example, the Snoop Collection promises "for one low fee"

---

143. *Id.*

144. *Id.*

145. *See supra* notes 28-29 and accompanying text; *infra* Part I.B.

146. *See infra* text accompanying notes 206-08.

147. For a sampling of these sites and sales policies, see *Dig Dirt Inc.* (visited Sept. 3, 1999) <http://www.digdirt.com>; WeSpy4U.com (visited Sept. 3, 1999) <http://www.wespy4u.com>; *Snoop Collection* (visited Apr. 1, 1999) <http://www.spycave.com/spy.html>.

148. For a FTC report on these traditional look up services, see FTC, *Individual Reference Services: A Report to Congress* (visited Dec. 1997) <http:www.ftc.gov/bcp/privacy/wkshp97/-irsdoc1.htm>.

Following the FTC's investigation, this industry sought to formalize and, in some cases, improve its privacy practices. *See* FTC, *Information Industry Voluntarily Agrees to Stronger Protections for Consumers*, (visited Dec. 17, 1999) <http://www.ftc.-gov/opa/1997/9712/inrefser.-htm>.

149. *See supra* note 147.

to provide the "enchantment of finding out a juicy tidbit about a co-worker" or checking "on your daughter's new boyfriend."[150] Anyone with a computer and access to cyberspace can purchase this kind of information. In this manner, these sites expand the range of available personal information.

### *B. The Current Legal Response*

Legal protection of personal information on the Internet is generally limited and often incoherent.[151] For example, the law in the United States today protects transactional data for the viewer of a film when rented at the video store, but not when seen over the Internet.[152] To further an understanding of this state of affairs, this Section starts with three general observations about American information privacy law and then turns to the specifics of how the law responds to privacy issues on the Internet. This Section concludes with a discussion of the Clinton Administration's emerging response to this situation.

First, regulation of the treatment of personal information in the United States occurs through attention to discrete areas of information use. Thus, in contrast to the approach in many other nations, it is unusual in the United States to find any comprehensive privacy laws, which legal experts term "omnibus laws" and that enumerate a complete set of rights and responsibilities for those who process personal data.[153] Regulation of the treatment of personal information in the United States generally targets specific, sectoral activities, such as credit reporting. It is directed at the treatment of information by either government or industry.[154]

---

150. *Snoop Collection* (visited Sept. 3, 1999) <http://www.spycave.com/spy.html>.

151. *See* Kang, *supra* note 4, at 1230 (stating that "[t]he collection of personal information in America by transacting parties is largely unregulated by law.").

152. *See* notes 155-56, *infra*, and accompanying text. To make another comparison, federal law currently places greater limits on use of video rental records than on health care records. *See* Schwartz, *Privacy Economics*, *supra* note 24, at 7.

On the rise of "streaming video" technology that permits films te be watched over the Internet, see Eben Shapiro, *PC Matinee: The Race is On to Make Web a Cyber-Cinema*, WALL ST. J., Mar. 2, 1999, at B1.

153. *See* Kang, *supra* note 4, at 1230. One such omnibus law in the United States is the Privacy Act, which, however, regulates only how federal agencies collect and use personal data. *See* SCHWARTZ & REIDENBERG, *supra* note 48, at 92-93.

154. *See* SCHWARTZ & REIDENBERG, *supra* note 48, at 7-10.

Second, this narrow approach has proceeded in an inconsistent manner. Thus, congressional outrage at the release of information about the video rentals of Judge Robert Bork at the time of his ill-fated Supreme Court nomination led to enactment of a sectoral law, the Video Privacy Protection Act, that regulated use of these data.[155] Yet, as already mentioned, the law contains no safeguards regarding disclosure of video content chosen from a Web site.[156] The result of a sectoral approach carried out in an inconsistent and episodic manner is that American information privacy law contains gaps equal to its content.

Third, the traditional American legal approach to information privacy law emphasizes regulation of government use of personal data rather than private sector activities.[157] From the earliest days of the Republic, American law has viewed the government as the entity whose data use raises the greatest threat to individual liberty.[158] For example, federal and state constitutional protections seek to assure freedom from governmental interference for communications and for the press.[159] This approach means that treatment of personal information in the private sector is often unaccompanied by the presence of basic legal protections.[160] Yet, private enterprises now control more

155. *See* REGAN, *supra* note 15, at 199. For the text of the Act, see 18 U.S.C. § 2710 (1994).

156. *See supra* text accompanying note 152.

Moreover, a further shortcoming of American information privacy law should be noted. While the law now protects the titles of video films that Judge Bork rents, it places no restrictions on the release of the titles of any books that Judge Bork purchases—even if this transaction takes place at the same store where he rents films. *See* Joel R. Reidenberg & Paul M. Schwartz, *Legal Perspectives on Privacy*, *in* INFORMATION PRIVACY: LOOKING AHEAD, LOOKING BACK 1, 20-21 (Robert J. Bies et al. eds., forthcoming 2000).

This distinction is highlighted by certain information sought by the Office of the Independent Counsel headed by Kenneth Starr. As part of its investigation of the Clinton Administration, special prosecutors from Starr's office obtained the titles of books purchased by Monica Lewinsky. *See* Doreen Carvajal, *The Investigations: Book Industry Vows to Fight 2 Subpoenas Issued by Starr*, N.Y. TIMES, Apr. 2, 1998, at A20. Lewinsky had no legal basis for blocking the release of this information. *See id.*; *see also* Karen Alexander, *Are Book Buys Anybody's Business?*, LEGAL TIMES, Mar. 30, 1998, at 2.

157. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 50-51 (1997); SCHWARTZ & REIDENBERG, *supra* note 48, at 6; SWIRE & LITAN, *supra* note 4, at 153.

158. *See* SCHWARTZ & REIDENBERG, *supra* note 48, at 6.

159. *See* CATE, *supra* note 157, at 50-51; Post, *Social Foundations*, *supra* note 16, at 966-1006.

160. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1032 (1996); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 507-31 (1995).

powerful resources of information technology than ever before.[161] These organizations' information processing contributes to their power over our lives. As the Internet becomes more central to life in the United States, the weaknesses and illogic of this existing legal model for information privacy are heightened. Let us now consider in turn the legal responses to each of the three loci of the privacy horror show in cyberspace.

The first location for personal data collection and processing is one's own computer—the Linda Tripp on our desktop. Current law fails to respond to such issues as the undeleting of files, the collection of clickstream data, and the placing of cookies on the hard drive of one's computer.[162] Although the most likely place to begin a search for legal safeguards is the tort law of privacy, it is of little help in cyberspace. The common law has developed a set of tort rights that protect against four types of invasion of privacy: (1) intrusion upon one's seclusion; (2) misappropriation of one's name or likeness without permission; (3) public disclosure of private facts; and (4) publicity that places one in a false light.[163] Unfortunately, various limitations that the common law has established on each of these branches eliminate their usefulness in responding to violations of privacy in cyberspace.[164]

As a result of these restrictions, most data processing on the Internet is excluded from the scope of the four branches of the privacy tort. Unless courts expand these torts over time, which is unlikely, the increasingly routine use of personal information within cyberspace is likely to fall entirely outside tort protection.[165] Beyond tort

---

161. *See supra* Part I.A.2.

162. *See* Kang, *supra* note 4, at 1230-37.

163. *See* RESTATEMENT (SECOND) OF TORTS § 652A-E (1977). Regarding the weaknesses of the privacy tort in the Information Age, see SCHWARTZ & REIDENBERG, *supra* note 48, at 180-82, 329; F. LAWRENCE STREET, LAW OF THE INTERNET 107-24 (1997); Joel R. Reidenberg, *Privacy in an Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 221-26 (1992).

For a sampling of the case law, see Porten v. University of San Francisco, 134 Cal. Rptr. 839, 841 (Ct. App. 1976); Dwyer v. American Express Co., 652 N.E.2d 1351, 1352 (Ill. App. Ct. 1995); Miller v. Moterola, Inc., 560 N.E.2d 900, 903 (Ill. App. Ct. 1990); Shibley v. Time, Inc. 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

164. For a more detailed discussion, see Kang, *supra* note 4, at 1231; Reidenberg & Schwartz, *supra* note 156, at 20;.

On the weaknesses of the privacy tort in Real Space, see Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2388 (1996); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 292-93 (1983).

165. *See* Reidenberg & Schwartz, *supra* note 156, at 7; Reidenberg, *supra* note 163, at 224-26.

law, sectoral statutes that govern such areas as electronic communications and consumer credit are also of scant help. In Jerry Kang's judgment, for example, "none of these statutes substantially constrains a transacting party from collecting [personal data]."[166]

The second loci for data collection, the ISP, provides a good example of statutory shortcomings. The Electronics Communications Privacy Act ("ECPA") is the statute most likely to provide restrictions on an ISP's data use.[167] Provisions in the Telecommunications Act of 1996 and the Cable Communications Policy Act of 1984 may be more strict, but their applicability to ISPs is thus far untested.[168] As for ECPA, unfortunately, numerous loopholes exist in it. For example, ECPA's strongest statutory prohibition forbids unauthorized access to an electronic communication while in storage in an electronic communication service facility.[169] Yet, under the logic of ECPA, "unauthorized access" does not include access to personal data that an ISP has authorized.[170] As a result, activities such as an ISP's sale of its customers' personal data will not be "unauthorized access" under ECPA. Moreover, ECPA's protection for subscriber records only limits release to "a governmental entity."[171] ISPs are free to sell and share these data, which are increasingly sought after, to anyone other than the government.

The Navy's pursuit of Timothy McVeigh provides a concrete example of how legal regulations that are focused on narrow contexts of information use have failed to respond to personal data use on the Internet. This Article has already utilized *McVeigh v. Cohen* as proof of how ISPs can tie information about a person's identity in Real Space to data about her behavior in cyberspace.[172] We will now examine the legal context of this case.

In *McVeigh*, Judge Sporkin held that the government's behavior violated its "Don't Ask, Don't Tell" policy regarding armed

166. Kang, *supra* note 4, at 1232.

167. 18 U.S.C. §§ 2510-2522, 2701-2709, 3121-3126 (1988 & Supp. 1994).

168. *See* 47 U.S.C. § 222(f)(1) (1994) (providing Telecommunications Act's provisions for Customer Proprietary Network Information ("CPNI")); *id.* § 522(7) (1994) (containing Cable Communications Policy Act's provisions for "cable system"). As currently interpreted, these statutes are not likely to be extended to ISPs. *See* PETER W. HUBER ET AL., THE TELECOMMUNICATIONS ACT OF 1996, at 54-55 (1996); Kang, *supra* note 4, at 1235 n. 188.

169. *See* 18 U.S.C. § 2701(a) (1994).

170. *Id.* § 2701(c)(1). *See* Kang, *supra* note 4, at 1234.

171. 18 U.S.C. § 2703(c)(1). *See* Tucker v. Waddell, 83 F.3d 688, 691 (4th Cir. 1996) (noting ECPA's private cause of action against governmental entities that violate it).

172. *See supra* Part I.A.2.b.

forces personnel.[173] The violation of the policy occurred because the Navy contacted AOL without the "credible information" legally required for such an investigation.[174] Judge Sporkin also noted that the Navy's action had likely violated ECPA's ban on disclosure of telecommunication subscriber data to the government without a subpoena.[175]

Despite the positive result of this litigation for McVeigh, this case reveals how little protection exists for most Americans whose personal data are found in cyberspace. If McVeigh had worked for a private company rather than the Navy, Judge Sporkin's hands would have been tied. McVeigh received additional—and clearly needed—privacy protection because of the congressionally mandated "Don't Ask, Don't Tell" policy.[176] Most Americans do not work for the military, however, and are not covered by this policy.[177] Moreover, ECPA would not have stopped the ISP from releasing McVeigh's personal subscriber data to a private employer. As noted earlier, this law generally permits ISPs to disclose subscriber information to entities other than the government.[178] Indeed, since the Navy investigator had represented himself as a private, nongovernmental person, AOL had a strong argument that it had not violated the ECPA.[179]

Beyond the shortcomings of statutory law, courts have failed to enforce explicit promises made by companies that collect personal data in cyberspace. For example, in *Smyth v. Pillsbury Co.*,[180] a federal court refused to force a company to honor its detailed assurances of e-mail confidentiality for its employees.[181] In this case,

---

173. McVeigh v. Cohen, 983 F. Supp. 215, 218-20 (D.D.C. 1998).

174. *Id.* at 219.

175. *Id.* at 219-20.

176. In *McVeigh*, Judge Sporkin observed, "[a]t this point in history, our society should not be deprived of the many accomplishments provided by people who happen to be gay. The 'Don't Ask, Don't Tell, Don't Pursue' policy was a bow to society's growing recognition of this fact." *Id.* at 220.

This federal policy is codified at 10 U.S.C. § 654 (1994). For an analysis of it, see WILLIAM N. ESKRIDGE, JR. & NAN D. HUNTER, SEXUALITY, GENDER, AND THE LAW 396-407 (1997).

177. For more on sexual orientation discrimination in the workplace, see ESKRIDGE & HUNTER, *supra* note 176, at 948-57.

178. *See supra* text accompanying note 171.

179. *See* Carl S. Kaplan, *Sailor's Case Leaves Question of Liability*, N.Y. TIMES ON THE WEB 2-3 (visited Jan. 29, 1998) <http://www.nytimes.com/library/cyber/law/012998law.html>.

180. Smyth v. Pillsbury914 F. Supp. 97 (E.D. Pa. 1996).

181. *Id.* at 100-01. This company's detailed promises about privacy included the statements that "all e-mail communications would remain confidential and privileged" and that "e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand." *Id.* at 98.

Pillsbury, a private company, took an ISP-like role by providing e-mail accounts for its employees.[182] Privacy in the Information Age comes in many different shades of anonymity. For the *Pillsbury* court, however, the access of system operators and others at the place of work meant that an employee could not consider her e-mail as confidential, even when the employer explicitly promised this result.[183] The *Pillsbury* court flatly declared that no "reasonable expectation" of privacy could exist "in e-mail communications voluntarily made by an employee."[184]

The third and final loci of data collected in cyberspace are Web sites. Here, too, the law generally leaves privacy practices unregulated. The FTC's action against GeoCities is a good indication of the limited nature of the present legal regime.[185] The first of the two deceptive practices alleged by the FTC against GeoCities was GeoCities's misrepresentation of a limited use of the data that it collected.[186] Despite its promise, GeoCities engaged in an all-too-classic case of unrestricted utilization of personal data without an individual's knowledge or permission.[187]

The second deceptive practice GeoCities engaged in was to allow third parties on its Web site to maintain and utilize personal data collected from children, despite its promises otherwise.[188] This threat to the privacy of a discrete group, children, raises a separate set of issues. GeoCities turned over potentially sensitive information about children to private individuals whom it had not screened in any meaningful fashion and without any effective restrictions on their use of these data.[189] This practice largely mirrors the first deceptive practice, but extends it to a group that is especially vulnerable.[190]

---

182. *See id.* at 98.

183. *See id.* at 101.

184. *Id.* For a general discussion of privacy issues concerning employee e-mail, see STREET, *supra* note 163, at 143-47.

185. *See* GeoCities Consent Order, *supra* note 138.

186. *See* FTC, supra note 139.

187. *See id.*

188. *See id.*

189. *See id.*

190. For more on deceptive practices on the Web directed toward children, see FTC, *supra* note 24, at 31-38. Regarding the vulnerability of children on the Internet, see the statement on introducing the Children's Online Privacy Protection Act of 1998 by one of its sponsors, Senator Richard Bryan: "The Internet offers unlimited potential for assisting our child's growth and development. However, we must not send our children off on this adventure without proper guidance and supervision." 144 CONG. REC. S8482-83 (daily ed. July 17, 1998) (statement of Sen.

Due in part to the timing of its initial public offering, GeoCities was willing to settle with the FTC and promised to make significant changes in its privacy practices.[191] Nevertheless, similar behavior elsewhere on the Web is unaffected by this government action.[192] Indeed, the FTC's ability to engage in these kinds of investigations is itself limited. This agency was able to obtain jurisdiction in this case only because GeoCities' false representations regarding its privacy practices constituted "deceptive acts or practices" under the Federal Trade Commission Act.[193] Web sites that make no promises about privacy, therefore, are not only unaffected by the *GeoCities* consent order, but also are likely to fall outside the FTC's jurisdiction.[194]

Another statutory limit exists on the FTC's jurisdiction. The FTC's enabling act restricts its powers to situations where an unfair act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[195] As this statutory language indicates, the FTC may be open to challenges to its power to stop activities that it claims to be unfair or deceptive trade practices.[196] Due to the difficulty in monetizing many privacy violations and other problems in fulfilling this jurisdictional calculus, the FTC may face objections should it take an aggressive role in policing information privacy in cyberspace with

---

Bryan); *see also* CHRIS PETERSON, I LOVE THE INTERNET, BUT I WANT MY PRIVACY TOO! 99-100 (1998).

191. *See* FTC, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case* (visited Aug. 13, 1998) <http://www.ftc.gov/opa/1998/9808/geocitie.htm>; Saul Hansell, *Amid Downturn, Another Internet Company's IPO Catches Fire* N.Y. TIMES ON THE WEB (Aug. 12, 1998) <http:www.nytimes.com/library/tech/98/08/biztech/articles/12geocities-ipo.html>.

192. The FTC recognizes as much in its report in June 1998 that found the vast majority of online businesses failing te adopt fundamental fair information practices. *See* FTC, *supra* note 24, at 41.

193. FTC, *supra* note 139.

194. See FTC, *supra* note 24, at 41 (stating "failure to comply with stated information practices may constitute a deceptive practice in certain circumstances, and the Commission would have authority te pursue the remedies available . . . for such violations," but "as a general matter, the Commission lacks authority to require firms to adopt informatiou practice policies"). Even Web sites that make explicit promises that they violate will not necessarily be investigated by the FTC. For one such case involving Sun Microsystems, see James Glave, *Sun violated my privacy* (visited Dec. 18, 1998) <http://www.wired.com/news/news/politics/story/16929.html>.

195. 15 U.S.C. § 45(n) (1994).

196. For interpretation of the circumstances under which "substantial injury" to consumers has been found under the FTC statute, see *Thompson Med. Co. v. FTC*, 791 F.2d 189, 196 (D.C. Cir. 1986); *International Harvester Co.*, 104 F.T.C. 949, 1041 ¶ 308 (1984); PETER C. WARD, FEDERAL TRADE COMMISSION: LAW, PRACTICE AND PROCEDURE § 5.04[2] (1999).

no more authorization than the general grant found in its enabling statute.[197] It also faces serious resource constraints because Internet privacy policy work is only a small part of its overall activities, even concerning cyberspace. The FTC's privacy protection activities already are dwarfed by its more aggressive investigations of fraud and deceptive marketing practices on the Internet.[198]

The Clinton Administration has not responded to the low level of privacy on the Internet with a legislative agenda. Rather, it considers the best privacy policy alternative to be industry self-regulation, which the online industry also strongly supports.[199] By focusing on facilitating wealth-creating transfers over the Internet,[200] this approach fits in with the emphasis of much of information policy in the United States. In particular, the Clinton Administration wants to make the Web and the world safe for e-commerce. This priority became clear during the 1998 holiday season when President Clinton and Vice President Gore heralded the increase in online commerce and introduced various proposals to speed the development of "the virtual shopping mall," including plans to help merchants and shoppers in lesser developed countries.[201]

Specific examples are also available of the Clinton Administration's deference to industry development of privacy standards for the Internet. Thus, Vice President Gore's ambitiously titled proposal for an "Electronic Bill of Rights" modestly responds to information privacy exigencies with a call for "industry self-regulation with en-

197. *See* Robert Gellman, *What Policy Does FTC Set In Its GeoCities Decision?*, DM NEWS, Sept. 21, 1998, at 15. For a claim of broad enforcement authority over commerce on the Internet by the Chairman of the FTC, however, see FTC, *Consumer Privacy on the World Wide Web*, (visited July 21, 1998) (prepared statement before the subcommittee on telecommunications trade and consumer protection).

198. *See* John Simons, *FTC Has a Committed Foe of Internet Fraud*, WALL ST. J., July 30, 1999, at A20.

199. For the Clinton Administration policies, see *supra* note 8 and accompanying text. For an example of industry views, see, Direct Marketing Ass'n, *Welcome to Privacy Action Now* (visited October 21, 1998) <http://www.the-dma-org/pan7/main.shtml> (expressing views of DMA, the Direct Marketing Association, on self-regulation, including the heading: "How to Catch the Best Online Customers"); Online Privacy Alliance, *Resources* (visited Sept. 7, 1998) <http://www.privacy-alliance.com/resources/> (providing Online Privacy Alliance's guidelines for self-regulation).

200. *See supra* text accompanying note 8.

201. The White House, *Remarks By the President and the Vice President at Electronic Commerce Event* (visited Nov. 30, 1998) <http://www.pub.whitehouse.gov/urires/12?urn:pdi//-oma.eop.gov.us/1998/12/1/5.text.1>.

forcement mechanisms."[202] In Gore's view, the Administration's role is to monitor the effectiveness of industry activity and of any enforcement mechanisms that industry provides against itself.[203] The Commerce Department is of a similar opinion, and the U.S. Government Working Group on Electronic Commerce has stressed that "privately enforced codes of conduct should be a central instrument for protection."[204] Should the online industry fail to improve its practices, however, the Clinton Administration on occasion has threatened to support a legal response.[205]

Where the Clinton Administration has hesitated, Congress has acted. Congressional action has forced the Administration's hand regarding one small corner of cyberspace. Congressional passage of the Children's Online Privacy Protection Act in 1998 requires Web sites directed to children to follow fair information standards.[206] This law also explicitly grants the FTC power to develop privacy standards for Web sites directed at children and to investigate violations of these standards as "an unfair or deceptive act or practice."[207] Here, Congress has provided a clear statutory authorization for an FTC role in one part of cyberspace.[208]

### *C. The Data Processing Model and the Internet: Cyberspace Meets Real Space*

This Article has described a privacy horror show—the widespread collection and disclosure of detailed personal data on the

---

202. Office of the Vice President, *Vice President Al Gore Announces New Steps Toward An Electronic Bill of Rights* (visited July 31, 1998) <http://www.pub.whitehouse.gov/urires/12?urn.-pdi//oma.eop.gov.us/1998/8/3/7.text.1> [hereinafter E-BILL OF RIGHTS].

For media reports, see Ted Bridis, *'E-Bill of Rights' Moves Forward* (visited July 31, 1998) <http://-abcnews.go.com/sections/tech/DailyNews/netprivacy_kids980731.html>; Magill, *supra* note 27, at 1.

203. E-BILL OF RIGHTS, *supra* note 202.

204. WORKING GROUP ON E-COMMERCE, *supra* note 8, at 16. This organization's praise of the private sector did note, however, the government's "important role to play in setting the goals of self-regulation, in working with industry to help make self-regulation effective, and in legislating in certain limited areas." *Id.* at 8

205. *See* The White House, *A Framework for Global Electronic Commerce* (visited July 1, 1997) <http://www.ecommerce.gov/framewrk.htm> ("If privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online.").

206. Children's Online Privacy Protection Act of 1998, *supra* note 28, § 6502.

207. *Id.* § 1303(c).

208. *See* 144 CONG. REC. S8482-83 (daily ed. July 17, 1998) (providing statement in favor of Act by one of its sponsors, Senator Richard Bryan).

Internet. It has also depicted the law's incomplete response to this pattern of personal data use. Yet, the Internet has an impact beyond this information use. The privacy horror show on the Internet can be put into a broader context by considering the emerging relationship of such information use to similar activities in the real world. This Article will argue that the present historical moment marks a dramatic turning point: the Internet is altering an already existing approach to data processing in the real world.

Many organizations in Real Space are information-driven. This Article's term for such an approach to administration is the "managerial model of data processing." This expression indicates the treatment of information as a data flow within a rationally organized stream of activities. Such Weberian administration already took place at a simple level during the Industrial Revolution; at that time, enterprises utilized personal and nonpersonal data to control production and to manage their administration.[209] As industrial techniques were applied to more specialized services, bureaucrats began to collect more detailed personal data to utilize in decisionmaking.[210]

Companies now engage in a constant process of collection and analysis of personal data to allow the customization of products, services, and relationships. One vision of this process, which is currently popular among business consultants, is called "one to one marketing."[211] According to this concept, modern business requires a "mass customization" of products and customer relations through the gathering and manipulation of finely grained personal data.[212] In the view of two leading business advisors, executives are to ask themselves, "If we had all the customer-specific information we could possibly want, what would we do differently in conducting business with our customers?"[213] This exercise first leads to identification of a desired application of personal data, and then, inevitably, to a com-

209. *See* BENIGER, *supra* note 58, at 210-87; THOMAS P. HUGHES, AMERICAN GENESIS: A CENTURY OF INVENTION AND TECHNOLOGICAL ENTHUSIASM 184-87 (1989); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1326-29 (1992).

210. OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, COMPUTER-BASED NATIONAL INFORMATION SYSTEMS: TECHNOLOGY AND PUBLIC POLICY ISSUES 78 (1981); Schwartz, *supra* note 209, at 1329.

211. DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE: BUILDING RELATIONSHIPS ONE CUSTOMER AT A TIME 14-17 (1993).

212. *Id.* at 138-41.

213. DON PEPPERS & MARTHA ROGERS, ENTERPRISE ONE TO ONE: TOOLS FOR COMPETING IN THE INTERACTIVE AGE 352 (1997) (emphasis omitted).

mand to obtain the personal information if the enterprise does not already have it.[214]

This Section has, thus far, described only half of the data processing model, that half formed by private enterprise. Yet, the government also makes use of data processing in its attempt to safeguard the collective basis of shared existence through its administrative activities.[215] One of the best portrayals of this State activity occurs in the scholarship of Jerry L. Mashaw, who has analyzed the shift in administrative technique from a decentralized, contextual interpretation of values to a systematic, instrumental implementation of policies.[216] Mashaw convincingly depicts the rise of "bureaucratic rationality." A related if distinct point is that the managerial apparatus that carries out this essential activity is increasingly organized around the use of personal information. The State collects and processes personal data to create and maintain public services and public goods, to manage those who work for it, and to regulate human behavior.[217]

Private industry and the government alike have come to rely on administration by use of detailed databases. Through these activities, personal information itself has been increasingly commodified during the last decades. In the private sector, a flourishing trade exists in selling personal data for profit.[218] As for the government, its goal in making its stores of personal information available is sometimes its own institutional economic profit and sometimes the promotion of communal goals.[219] Nevertheless, the State, like private enter-

---

214. *Id.* at 354. *See* BILL GATES, BUSINESS @ THE SPEED OF THOUGHT: USING A DIGITAL NERVOUS SYSTEM at xiv (1999) (stating that "though at heart most business problems are information problems, almost no one is using information well"); Julie Pitta, *Garbage in, gold out*, FORBES, Apr. 5, 1999, at 124-25 (discussing new developments in software that allow easier analysis of customer data now buried in corporate systems).

215. An administrative state now plays an essential role in safeguarding the conditions for the social, political, and physical environment in the United States. For a description of the transformation of the government's role, see generally Bruce Ackerman, *Constitutional Politics/Constitutional Law*, 99 YALE L.J. 453, 488-515 (1989).

216. *See* JERRY L. MASHAW, DUE PROCESS IN THE ADMINISTRATIVE STATE 230-32 (1985); JERRY L. MASHAW, BUREAUCRATIC JUSTICE 171-80 (1983).

217. *See* DAVID F. LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? 81 (1989) (explaining that federal government controls the "largest inventory of computers of any single organization in the world").

218. *See* BUS. WK. Poll, *supra* note 7, at 99 (noting value of customers' data and the trade in them).

219. For example, governmental disclosures under the federal Freedom of Information Act seek to provide citizens with the information necessary to evaluate government action for the purpose of democratic self-rule. 5 U.S.C. § 552 (1994). *See* Bibles v. Oregon Natural Desert

prises, commodifies personal data. Its stores of personal information are not only alienable, but also highly sought after by third parties because of the value its administration apparatus adds to the data.[220] Statutes such as the recently enacted Electronic Freedom of Information Act further heighten the utility of federal information by requiring its release whenever possible in digital formats.[221]

Management through use of personal information seeks to organize life instrumentally to achieve specific objectives. It is a realm of hierarchical authority, where decisions are made through the application of processes that are formalized and sometimes automated. The present historical moment, however, marks the Internet's extension and perfection of the established data processing model. Building on the depiction of the privacy horror show in the previous Section, this Article will demonstrate the three ways in which the Internet, as it is currently structured, heightens the impact of this managerial model.

To summarize: first, the Internet is increasing the quality, quantity, and accessability of personal information relating to behavior both in cyberspace and Real Space. Second, the Internet is reducing the zones of data anonymity that were once available. Finally, the Internet is heightening uncertainty about which person or what organization is utilizing our personal information and the circumstances of this use. These three factors demonstrate the fashion in which this extension of bureaucratic rationality is creating a new structure of power in our society.

The first manner in which the Internet affects the data processing model is by increasing the quality, quantity, and accessibility of personal data. The Internet works along these dimensions by

---

Ass'n, 117 S.Ct. 795, 795 (1997); DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1988).

As for the profit motive, many states seek to raise money by selling databases of personal information about drivers. *See* SCHWARTZ & REIDENBERG, *supra* note 48, at 148-51. Congress bas placed some statutory limits on the states' ability to sell this information by requiring that they provide an opportunity for drivers to opt out. *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (1994). For an analysis, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: 1998 SUPPLEMENT 24-34 (1998) [hereinafter REIDENBERG & SCHWARTZ, DATA PRIVACY SUPPLEMENT].

220. For a discussion of different policy issues relating to the government's adding of value to information, see Henry H. Perritt, Jr., *Electronic Freedom of Information*, 50 ADMIN. L. REV. 391, 402-12 (1998).

221. For the text of the Electronic Freedom of Information Act, see Electronic Freedom of Information Act Amendments of 1996, 5 U.S.C. § 552 (Supp. II 1996). For a discussion, see Perritt, *supra* note 220, at 395-98.

decimating previous barriers to data sharing.[222] This Article has already described the new cyber-reference services, such as the Internet's Dig Dirt, WeSpy4U, and Snoop Collection.[223] This example shows how the managerial data processing model is being extended as decisionmaking regarding wider areas of life is made with reference to more detailed databases.

The Internet's second impact on the data processing model is a dramatic reduction of existing zones of data anonymity. Consider how activities in the real world's physical topography generally are incompletely mapped through data records. Here, this Article will develop the idea of *physical* and *data topographies*. For the most part, one's behavior in the physical topography of Real Space takes place without generating any records within a data map. To make this point more concrete, consider a walk outside in the mass society in which most Americans live. Although technology is beginning to map more of Real Space's physical topography by utilizing means such as video cameras in public settings, most activities in Real Space's physical settings take place under conditions of personal anonymity and without creating trails of personal data.[224] The level of data anonymity in Real Space does change, however, if one makes a purchase at a store with a credit card—suddenly a record has been created of the visit and the sale at a particular time in a particular location.[225]

Let us now imagine a different scenario: every time that this stroll took place, one left a record of all activities in the shadow data map. Depending on where one was located in Real Space, this record might consist of: the path that one took, the words that a soapbox speaker uttered, the amount of time spent listening to this speech, any chance comments exchanged with people encountered on the

---

222. These barriers were sometimes based on legal distinctions about differences in communication technology, which are of less relevance in cyberspace. *See* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 1006-08 (1996). These barriers were also sometimes based on social or industry customs, which are in flux on the Internet. *See infra* Part III.C.2. Finally, limits on data sharing were sometimes due simply to the practical obscurity of files physically located in paper records. *See Reporters Comm.*, 489 U.S. at 764 ("[P]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information").

223. *See supra* notes 147, 149-50 and accompanying text.

224. For discussion of a survey of surveillance cameras in public spaces in Manhattan that identified 2,380 of these devices, see Bruce Lambert, *Secret Surveillance Cameras Growing in City, Report Says*, N.Y. TIMES, Dec. 13, 1998, at 61.

225. For a discussion, see SCHWARTZ & REIDENBERG, *supra* note 48, at 270-76.

street, the content of the brochure that someone distributed, and the amount of time spent looking at each page in this document. If one entered a store, the record would reveal the time spent gazing at different products, the dialogue engaged in with a salesperson, and any products that were purchased.

This imaginary scenario for Real Space becomes possible when one surfs the Web. Because the Internet is an interactive telecommunication system, a computer linked to it does not merely receive information but transmits it. This Article has discussed the fashion in which personal data are collected at the computer on one's desk, by one's ISP, and the Web sites that one visits.[226] This information also includes "clickstream" data, which potentially record every movement that one makes on the Internet.[227] To return to this Article's metaphor of physical and data topographies, these two realms can become seamless in cyberspace. Internet behavior generates more finely grained personal data than Real Space activities such as the use of a credit card. The resulting reduction in available zones of data anonymity on the Internet dramatically increases the areas of life open to managerial decisionmaking by facilitating management through data processing.

A final comparison with the use of the credit card in Real Space illustrates the third and final connection between the Internet and the managerial model of data processing. This point concerns the fashion in which the Internet increases uncertainty about the societal circumstances of information use. We begin again with Real Space, where most people have a relatively accurate sense of the range of identity disclosure that occurs in different parts of the physical topography.[228] In contrast to this awareness of the privacy zones of Real Space's *physical settings*, a lower level of public awareness exists as to Real Space's precise *data topography*.[229] Yet, even fewer individuals today have a sense of the Internet's precise data topography.[230]

---

226. *See supra* Part I.A.2.

227. *See supra* notes 99-100 and accompanying text.

228. *See* Lessig, *supra* note 64, at 866 (noting how regulation of pornography in Real Space is simplified because "we find these features of the architecture of real space, we don't make them").

229. The classic example is the public's relatively strong confidence that its personal medical information is well protected by law. *See* HARRIS-EQUIFAX, HEALTH INFORMATION PRIVACY STUDY 2, 33 (1993). In contrast, those who know the most about the current legal protection of medical information—physicians, heads of medical societies, health insurers, and hospital CEO's—are also the most concerned about threats to personal privacy. *Id.* at 22; *see*

Monica Lewinsky undoubtedly believed that her electronic messages were evanescent and that her deleted draft letters and e-mail had been sent to a permanent electronic version of a garbage can.[231] Timothy McVeigh probably considered the communications that he sent with his different AOL mail aliases to be semi-anonymous, allowing him to maintain control over the most important decisions regarding any linkage of his cyberspace behavior to his Real Space identity.[232] Those who make comments in "chat rooms" or "list servs," or who simply visit Web sites, are also likely to have similar mistaken beliefs regarding the specific level of disclosure of personal data involved in their activities. At the same time, however, that only a few people understand the precise data topographies of the Internet, Americans do have a growing, if uncertain, awareness of a privacy problem in cyberspace.[233]

The lack of precise knowledge about personal data use allows the managerial data processing model to capture personal information that might never be generated if individuals had a better sense of the Internet's data privacy zones. As a further result, bureaucratic decision-making can be extended into new areas in a stealth-like process unaccompanied by societal debate. Finally, the widespread ignorance about personal data use makes clear the ultimate result of the current pattern of data use on the Internet. These developments, experienced in small and large ways by millions of Internet users, are creating a new hierarchy of power. The new power structure emerging in cyberspace is problematic, however, to the extent that we as a society seek something incompatible with such instrumental management. As Robert Post warns, "[s]tructures of control acquire their own life, turn, and bite the progressive hand that establishes them."[234]

The next Part will discuss the dangers of the power structure created by personal information use on the Internet. At the same time, however, it will argue that the proper response to this conflict is not to maximize secrecy about individuals and their pursuits. Personal data often involve a social reality that is external to the indi-

---

*generally* Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295 (1995).

230. For example, to the extent that individuals even are aware of "cookies," misunderstandings abound. For a discussion of some of these misperceptions, see Kang, *supra* note 4, at 1227-28; *Persistent Cookie FAQ*, *supra* note 93.

231. *See* ANDREW MORTON, MONICA'S STORY 220-21 (1999).

232. For a further discussion, see *infra* text accompanying notes 296-99.

233. For polling data, see *supra* note 7.

234. POST, CONSTITUTIONAL DOMAINS, *supra* note 16, at 288.

vidual; as a result, the optimal utilization of this information is unlikely to exist at either extreme on a continuum that ranges from absolute privacy to complete disclosure.[235]

## II. SHARED LIFE AND DEMOCRACY IN CYBERSPACE

The absence of privacy on the Internet reflects a deeper current, namely the establishment of the managerial data processing model in cyberspace. This Part examines the implications of this development by contrasting the Internet's potential as the new realm of shared life with the consequences of this social arrangement of hierarchical control. The utilization of information technology in cyberspace will act as a powerful negative force in two ways. First, as currently configured, it will discourage unfettered participation in deliberative democracy in the United States.[236] Second, the current use of information technology on the Internet can harm an individual's capacity for self-governance.[237] These two negative effects are significant because our nation's political order is based both on democratic deliberation and on individuals who are capable of forming and acting on their notions of the good.

As this précis makes clear, this Article's Part II is both anchored in and seeks to develop civic republican theory. At first glance, this perspective may appear unusual for scholarship concerned with information privacy. After all, civic republicanism is a political philosophy that generally is more concerned with obligations than with rights, more interested in community than individuals.[238] Moreover, to the extent that civic republican theorists talk at all about privacy, they have been less concerned with information privacy, dismissed by Michael Sandel as the "old privacy," than with the freedom to engage in certain activities free of governmental restrictions.[239] This Article will, nevertheless, demonstrate the

---

235. For a similar conclusion regarding the use of personal medical information, see Schwartz, *Privacy Economics*, *supra* note 24, at 41.

236. *See infra* Part II.A.

237. *See infra* Part II.B.

238. *See* MICHAEL J. SANDEL, DEMOCRACY'S DISCONTENTS: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY 117 (1996) (noting that "the republican tradition emphasizes the need to cultivate citizenship through particular ties and attachments").

239. *Id.* at 97; *see* Frank Michelman, *Law's Republic*, 97 YALE L.J. 1493, 1533-34 (1988) (arguing for a "constitutional privacy principle" suitable to "modern republican constitu-

promise of republican thought for invigorating the debate about information privacy.

### A. Democratic Deliberation

Cyberspace has the potential to emerge as an essential focal point for communal activities and political participation. This development would help counter several negative trends in the United States. Voter turnout is declining; membership in many kinds of traditional voluntary associations is sinking; and a sense of shared community is frayed.[240] Information technology in general and the Internet in particular have the potential to reverse these trends by forming new links between people and marshalling these connections to increase collaboration in democratic life.

Elements of this provocative vision are already being realized. For example, the Internet is being used to modernize the historical and constitutional right of petition. In June 1995, Senator Patrick Leahy became the first Congressperson to bring an Internet-generated petition onto the Senate floor.[241] This document consisted of 1,500 pages listing the names of citizens who had indicated their opposition to a Bill then under debate.[242] In addition, neighborhoods throughout the United States are setting up virtual community bulletin boards.[243] These and other networking ideas are intended to improve dissemination of information about and discussion of community issues such as zoning, new ordinances, and city government.[244]

If Congress and policy experts have glimpsed cyberspace's potential for revitalizing democratic life, it has been less clear that civic republicanism offers a suitable, if partial, framework for this

---

tionalism" that protects "admission to full and effective participation in the various arenas of public life").

240. *See* BENJAMIN R. BARBER, A PLACE FOR US: HOW TO MAKE SOCIETY CIVIL AND DEMOCRACY STRONG 9 (1998).

The midterm national election of 1998 illustrates the point about declining voter turnout; it suffered from the lowest turnout in half a century. *See* R.W. Apple, Jr., *The President's Acquittal*, N.Y. TIMES, Feb. 13, 1999, at A1.

241. *See* GRAEME BROWNING, ELECTRONIC DEMOCRACY: USING THE INTERNET TO INFLUENCE AMERICAN POLITICS 52-53 (1996).

242. *See id.*

243. *See* STEPHEN DOHENY-FARINA, THE WIRED NEIGHBORHOOD at xi, 45 (1996) (describing "wired community" as "geophysical neighborhoods" lined by electronic communication technologies). For another description of these sites, see William R. Long, *For Neighborhoods in Many Cities, Virtual Community Centers*, N.Y. TIMES, Mar. 4, 1999, at G7.

244. *See* Long, *supra* note 243, at G7.

idea. Indeed, while civic republicanism itself has been slow to apply its principles to cyberspace, the connection is unmistakable.[245] Although a disparate group, civic republican theorists are bound by a core set of beliefs. In their view, the good society is a self-governing one based on deliberative democracy.[246] In place of liberalism's emphasis on the individual, civic republicans seek an ongoing social project of authorship of a country's fundamental political values by its people.[247] In searching for ways to construct strong democracy, this group emphasizes common participatory activities, reciprocal respect, and the need for consensus about political issues.[248]

From the civic republican perspective, the true promise of the Internet will not be as a place for electronic commerce, but as a forum for deliberative democracy. Cyberspace appears as the answer to their search for a new hospitable space. It satisfies Benjamin Barber's wish for shared areas "where we can govern ourselves in common without surrendering our plural natures."[249] Cyberspace can provide a space for "civic forums," where, to cite Frank Michaelman's general formulation, "the critical and corrective rigors of actual democratic discourses" can occur.[250] Or, to return to Barber, cyberspace offers the

245. In the era before the Internet became ubiquitous, civic republican theorists discussed use of a civic videotext service "to equalize access to information and promote the full civic education of all citizens," BENJAMIN R. BARBER, STRONG DEMOCRACY: PARTICIPATORY POLITICS FOR A NEW AGE 307 (1984) as well as televoting and deliberative video town hall meetings, *see* JAMES S. FISHKIN, DEMOCRACY AND DELIBERATION: NEW DIRECTIONS FOR DEMOCRATIC REFORM 81-104 (1991).

More recent efforts by civic republicans to evaluate developments in information technology generally have been modest, see, e.g., BARBER, *supra* note 240, at 84-85 (calling for a "national civic forum" using satellite uplinks); Benjamin R. Barber, *Three Scenarios for the Future of Technology and Strong Democracy*, 113 POL. SCI. Q. 573, 586 (1998-99) (criticizing "an anarchic and wholly user-controlled net").

Outside of civic republican theorists, however, others have discovered the democratic potential of the Internet. *see, e.g.*, BROWNING, *supra* note 241, at 4; DOHENY-FARINA, *supra* note 243, at 50-76.

246. *See* SANDEL, *supra* note 238, at 117-18; Joshua Cohen, *Deliberation and Democratic Legitimacy*, *in* DELIBERATIVE DEMOCRACY: ESSAYS ON REASON AND POLITICS 67 (James Bohman & William Rehg eds., 1997) [hereinafter DELIBERATIVE DEMOCRACY]; Michelman, *supra* note 239, at 1534.

247. *See* Frank Michelman, *How Can the People Ever Make the Laws? A Critique of Deliberative Democracy*, *in* DELIBERATIVE DEMOCRACY, *supra* note 246, at 145, 147.

248. *See id.* at 147-48; *see also* SANDEL, *supra* note 238, at 5-6; BARBER, *supra* note 245, at 197-203.

249. BARBER, *supra* note 240, at 3.

250. Michelman, *supra* noto 247, at 165.

promise to fulfill his call for a "free space in which democratic attitudes are cultivated and democratic behavior is conditioned."[251]

This framework offers a fruitful basis for understanding why certain proposals regarding the future development of cyberspace are so important. For example, Stephen Doheny-Farina has pointed to some of the trends already mentioned, such as the setting up of virtual community bulletin boards, and has described them as proof of the promise of the "wired neighborhood."[252] In his view, there is a critical need for a proliferation of civic networks that originate locally and organize community information and culture to foster responsibility and pride in our neighborhoods.[253] Beyond the idea of such local networks, Laura Gurak views cyberspace as an electronic place of speed and simultaneity that allows people with common values to gather around an issue and take effective political action.[254] While Doheny-Farina is interested in the potential of a wired neighborhood, Gurak explores the potential of interest communities that are national and international in scope.[255] She argues for further study of computer-mediated communication with the goal of improving existing electronic systems to encourage democratic participation.[256]

Such deliberative democracy will not occur in cyberspace unless certain preconditions are in place. One of these prerequisites concerns access to the Internet. Research by social scientists and the National Telecommunications and Information Administration ("NTIA") has identified an emerging "digital divide" in the United States.[257] Access to the Internet by racial minorities lags significantly behind that of whites.[258] Others in the group of "information havenots" are the poor, the disabled, and Americans living in rural areas.[259] As a stark example of these disparities, the NTIA has found that households with incomes of $75,000 and higher are *twenty times*

---

251. BARBER, *supra* note 240, at 6.

252. DOHENY-FARINA, *supra* note 243, at 125.

253. *Id.* at 19-37.

254. LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE: THE ONLINE PROTESTS OVER LOTUS MARKETPLACE AND THE CLIPPER CHIP 8 (1997).

255. *Id.* at 56.

256. *Id.*

257. National Telecomm. & Info. Admin., *Falling Through the Net: Defining the Digital Divide* (visited July 1999) [hereinafter *NTIA Report*] <http://www.ntia.doc.gov/ntiahome/fttn99/contents.html>; Thomas P. Novak & Donna L. Hoffman, *Bridging the Racial Divide on the Internet*, 280 SCIENCE 390 (1998).

258. *NTIA Report*, *supra* note 257, at 6; Novak & Hoffman, *supra* note 257, at 391.

259. *NTIA Report*, *supra* note 257, at 6-9, 77.

more likely to have access to the Internet than those in the lowest income levels.[260] This organization has also found that in some instances the digital divide is widening.[261] Public policies and private initiatives are needed to connect all Americans to the Internet. Beyond access, a second issue concerning deliberative democracy in cyberspace is information privacy.

In the absence of strong rules for information privacy, Americans will hesitate to engage in cyberspace activities—including those that are most likely to promote democratic self-rule. Current polls already indicate an aversion on the part of some people to engage even in basic commercial activities on the Internet.[262] Yet, deliberative democracy requires more than shoppers; it demands speakers and listeners. But who will speak or listen when this behavior leaves finely-grained data trails in a fashion that is difficult to understand or anticipate? Put differently, when widespread and secret surveillance becomes the norm, the act of speaking or listening takes on a different social meaning.

Consider the Supreme Court's decision in *Reno v. ACLU*.[263] In striking down certain provisions of the Communication Decency Act, the Supreme Court declared its intention to protect the "vast democratic fora" of the Internet.[264] The Supreme Court considered the Internet to be a speaker's paradise. As the Court noted, "[t]his dynamic, multifaceted category of communication" permits "any person with a phone line" to "become a town crier with a voice that resonates farther than it could from any soapbox."[265] This language is redolent of civic republicanism. In Benjamin Barber's vision, civil society is the free space in which democratic attitudes are cultivated and conditioned.[266] In Barber's words, "the public needs its town square."[267]

---

260. *Id.* at xiii.

261. *Id.*

262. *See* BUS. WK. Poll, *supra* note 7, at 98.

263. Reno v. ACLU, 521 U.S. 844 (1997).

264. *Id.* at 885. In a similar fashion in 1982, Judge Harold Greene stressed the importance of the telephone network to the political life of this nation in his Modified Final Judgment upholding and altering the Justice Department's Consent Order with AT&T that began the break-up of the Bell System. *See* United States v. American Tel. & Tel. Co., 552 F. Supp. 131, 145 (D.D.C. 1982).

265. *Reno*, 521 U.S.at 870.

266. BARBER, *supra* note 240, at 76.

267. *Id.*

Without information privacy, however, the implications of congregating in the town square are dramatically changed. The Supreme Court's decision in *Reno v. ACLU* is also illustrative in this regard. The Supreme Court praised the Internet's potential for furthering free speech. For the Court, the Internet represented a "new marketplace of ideas."[268] It must be noted , however, a paradox in this regard: while listening to ideas in Real Space generally does not create a data trail, listening on the Internet does. The Internet's interactive nature means that individuals on it simultaneously collect and transmit information. As a result, merely listening on the Internet becomes a speech-act.[269] A visit to a Web site or a chat room generates a record of one's presence.[270] To extend the Supreme Court's metaphor, the role of town crier in cyberspace is often secretly assigned—a person can take on this role, whether or not she seeks it or knows afterwards that she has been given it. Already one leading computer handbook, the *Internet Bible*, concludes its description of the low level of privacy in cyberspace with the warning, "Think about the newsgroups you review or join—they say a lot about you."[271]

At this point, a further complication must be mentioned. Deliberative democracy not only requires limits on access to personal information, but also demands that access to these data be gnaranteed in many circumstances. Such information disclosure is needed for public accountability; democratic community relies on a critical assessment of public persons and events.[272] To return to the town crier metaphor, the release of at least some personal information about speakers at the public square is needed under some circumstances. In the language of the First Amendment, for example, we call some individuals "public figures" and permit them less privacy due to the demands of democratic discourse.[273]

Information privacy rules must evaluate the demands for personal data along with the need for restrictions on access that will encourage speech. If cyberspace is to be a place where we develop our commonality through democratic discourse, the right kinds of rules must shape the terms and conditions under which others have access

268. *Reno*, 521 U.S. at 885.
269. *See supra* Part I.A.2.
270. *See supra* Part I.A.2.c.
271. UNDERDAHL & WILLETT, *supra* note 85, at 247.
272. *See* SANDEL, *supra* note 238, at 79 (noting that free speech is tied to self-government).
273. *See* Thomas I. Emerson, *The Right of Privacy and Freedom of the Press*, 14 HARV. C.R.-C.L. L. REV. 329, 356-60 (1979); Post, *Social Foundations*, *supra* note 16, at 999-1000.

to our personal data. The issue is of the highest importance; the Internet's potential to improve democracy will be squandered unless we safeguard the kinds of information use that democratic community requires.

### *B. Individual Self-Determination*

Beyond democratic deliberation, information use in cyberspace poses an important threat to a second value necessary for life in a democracy. Here, one must go beyond existing civic republican thought, which is largely focused on the group, and consider the individual. Decisionmaking in a democracy takes place not only within a given community, but also within individuals who, at any time, are anchored in a variety of social settings.[274] The health of a democratic society depends both on the group-oriented process of democratic deliberation and the functioning of each person's capacity for self-governance.[275]

This Article will therefore supplement the idea of democratic deliberation by elaborating a principle of individual self-determination. It will first define this concept and then explore the threat to it posed by current information processing in cyberspace. The argument is that without the right kind of privacy rules, the potential of cyberspace for promoting self-governance will be lost. The fashion in which society and law insulate certain acts and places from data collection affects the process of development of identity. The need is to insulate an individual's reflective facilities from certain forms of manipulation and coercion. Privacy rules for cyberspace must set aside areas of limited access to personal data in order to allow individuals, alone and in association with others, to deliberate about how to live their lives.

This Section begins by returning again, briefly, to civic republicanism. Although civil republican theory does not elaborate a detailed concept of individual self-determination, this Article's attention to autonomy is compatible with this strain of political thought. For example, Michael Sandel has noted that self-government today

---

274. *See, e.g.*, Jeremy Waldron, *Virtue en masse*, *in* DEBATING DEMOCRACY'S DISCONTENT 32, 33 (Anita L. Allen & Milton C. Regan, Jr. eds., 1998) (warning against purely community pursuit of moral commitments as leading to "grey, fearful mass conformism, dictated by something like the moral version of the fashion industry").

275. *See, e.g.*, Schwartz, *Participation*, *supra* note 24, at 563-65; James E. Fleming & Linda C. McClain, *In Search of a Substantive Republic*, 76 TEX. L. REV. 509, 521 (1997) (book review).

requires development of a capacity to participate in politics in a multiplicity of settings.[276] He argues, "[t]he civic virtue distinctive to our time is the capacity to negotiate our way among the sometimes overlapping, sometimes conflicting obligations that claim us, and to live with the tension to which multiple loyalties give rise."[277] Despite Sandel's insight on this point, neither he nor other civic republicans identify the precise ability needed to fulfill these negotiations and the external programmatic structure essential to nurture this ability.[278] This absence represents a considerable flaw in the civic republican project.[279]

Civic republicanism must undergird its existing concept of democratic deliberation with a foundation based on an individual's capacity for critical reflection. Outside of this movement, an important corrective attempt is already underway. James E. Fleming has argued, for example, that democracy in general and constitutional law in particular must secure the preconditions for "citizens to apply their capacity for a conception of the good to deliberat[ions] about . . . how to live their own lives."[280] His call is for a deliberative autonomy that is the locus of moral agency, responsibility, and independence.[281] This quality involves both decisionmaking internal to the individual and a person's consulting with others, taking their views into account, and associating with them.[282]

From this perspective, democracy requires more than group deliberation at a town square located either in Real Space or in cyberspace. It requires individuals with an underlying capacity to form and act on their notions of the good in deciding how to live their lives. This anti-totalitarian principle stands as a bulwark against any coer-

276. SANDEL, *supra* note 238, at 350.

277. *Id.*

278. In contrast, Mark Tushnet has criticized Sandel for merely expressing a "mood"—and one that reflects the "reduced autonomy" of "today's professional-managerial class"—without developing satisfactory solutions. Mark Tushnet, *A Public Philosophy for the Professional-Managerial Class*, 106 YALE L.J. 1571, 1571-1600 (1997) (book review).

279. The danger is that without promotion of this personal quality, the end of republicanism will not be democratic solidarity, but tribal fraternalism, or worse. For an expression of this concern from within the civic republican movement, see BARBER, A PLACE, *supra* note 240, at 28-29.

280. James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 2-3 (1995).

281. *Id.* at 30-34.

282. *Id.* at 37. *See* James E. Fleming, *Constructing the Substantive Constitution*, 72 TEX. L. REV. 211, 289 (1993); *see also* Clifford Orwin, *The Encumbered American Self in* DEBATING DEMOCRACY'S DISCONTENT, *supra* note 274, at 86, 90-91.

cive standardization of the individual.[283] Yet, a considerable difficulty arises in identifying the kinds of government or group behavior that raises a threat to personal self-governance. Part of the problem is that autonomy is a notoriously slippery concept.[284] Even more to the point, however, communal life requires something beyond isolated decisionmaking—self-governance takes place in individuals who are not located on discrete behavioral islands, but are tied to others and necessarily open to influence through outside persuasion.[285]

Social life's give-and-take is not merely compatible with individual autonomy, but an essential factor in it because life is lived among others. Prior and ongoing commitments make a difference in the choices we make and in the hierarchy of our goals.[286] As a result, we must comprehend autonomous people as being only partially the authors of their lives. As Joseph Raz has proposed, "[t]he ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives."[287] Individuals who exercise self-determination, therefore, should be defined as people who, as part authors of their lives, substantially shape their existence through the choices they make.

Self-determination is a capacity that is embodied and developed through social forms and practices. The threat to this quality arises when private or government action interferes with a person's control of her reasoning process. To understand the harm of this

---

283. *See* Schwartz, *Participation*, *supra* note 24, at 560.

284. *See* GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY 5-6 (1988) (noting how autonomy is often "used in an exceedingly broad fashion" in moral and political philosophy); Stephen Gardbaum, *Liberalism, Autonomy, and Moral Conflict*, 48 STAN. L. REV. 385, 394 (1996) (explaining that liberals tend to promote "hopelessly vague conceptions of autonomy").

285. *See, e.g.*, Gardbaum, *supra* note 284, at 394 (noting that "commitment to the value of autonomy may itself be best understood as a response to the profound reality of the 'social construction of individuality' ").

286. *See* Jeremy Waldron, *Autonomy and Perfectionism in Raz's Morality of Freedom*, 62 S. CAL. L. REV. 1097, 1119 (1989) ("Parents instill aspirations in their children, lovers thrust projects upon one another, and society as a whole makes certain options available and others unavailable.").

287. JOSEPH RAZ, THE MORALITY OF FREEDOM 369 (1986). As Jeremy Waldron has observed:

> [T]he autonomous person's life is marked not only by what it is but also by what it might have been and by the way it became what it is. A person is autonomous only if he had a variety of acceptable options . . . . A person who has never had any significant choice, or was not aware of it, or never exercised choice in significant matters . . . is not an autonomous person.

Waldron, *supra* note 286, at 1104 (citing RAZ, *supra*, at 204); *cf.* Morris Lipson, Note, *Autonomy and Democracy*, 104 YALE L.J. 2249, 2270-71 (1995) (noting different degrees of autonomous choice).

manipulation, consider David Strauss's examination of different kinds of manipulation in the speech context.[288] In that setting, coercion occurs when one compels another to pursue the speaker's objectives instead of the victim's own objectives.[289] Such coercion can take place through simple use of physical force or through inducements that interject false facts into the thought processes of the listeners.[290] Drawing on Strauss's work, we can state that a coercive influence on decisionmaking is that which takes over, or colonizes, a person's thinking processes.[291]

Having developed the idea of individual self-determination and identified the nature of coercion upon it, once again this Article will inquire in to the dangers raised by the lack of cyberspace privacy. As we have seen, physical coercion or false statements of fact corrupt decisionmaking by commandering the listener's mind to produce an outcome that the speaker desires. Autonomy manipulation on the Internet reaches a similar result in a different fashion. Its perfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking.

George Orwell carried out the classic analysis of how surveillance can exert this negative pressure. In the novel *1984*, first published in 1949, Orwell imagined a machine called the "telescreen."[292] This omnipresent device broadcasted propaganda on a nonstop basis and allowed the state officials, the "Thought Police," to observe the populace.[293] Computers on the Internet are reminiscent of the telescreen; under current conditions, it is impossible to know if and when the cyber-Thought Police are plugged in on any individual wire. To extend Orwell's thought, one can say that as habit becomes

---

288. *See* David A. Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91 COLUM. L. REV. 334 (1991).

289. *See id.* at 364-66.

290. *See id.*

291. *See* Gardbaum, *supra* note 284, at 413 ("For the government te treat its citizens with equal respect requires that it treat each citizen's interest in autonomy as equal, and that it respect and enhance the capacity of each citizen to choose her own ends and not have them determined or unduly influenced by others.").

292. GEORGE ORWELL, 1984 at 6 (Penguin Books 1954) (1949).

293. *Id.* at 24-25. Orwell wrote:

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

*Id.* at 6.

instinct and people on the Internet gain a sense that their every mouse click and key stroke might be observed, the necessary insulation for individual self-determination will vanish.[294]

In illustrating this point about the Cyber-Thought Police, we return once again to Timothy McVeigh. The military's pursuit of McVeigh indicates the potential of information surveillance for undermining decisionmaking. For McVeigh, self-determination involved his finding a path between at least two aspects of his personality, the distinguished military veteran and "boyscrch," whose AOL profile stated an interest in "boy watching" and "collecting pics of other young studs."[295] The danger in a limitless surveillance of expression in cyberspace is that it can corrupt individual decisionmaking about the elements of one's identity.

For McVeigh and many other Americans, the Internet provides a place to think about choices through interactions with others. McVeigh, like many others, utilized cyberspace as a place to do thinking about who he is and who he would become. In this light, *McVeigh v. Cohen* represents an attempt to set limits on the surveillance of thought in cyberspace. Judge Sporkin's language supports this reading; in his view, the military's persistent investigation of McVeigh was no less than a "search and destroy" mission.[296] For Judge Sporkin, the enlisted man's behavior was not proof of an immutable identity, but instead revealed virtual activities that were permissible

294. This regulation of surveillance is especially important because cyberspace improves upon the negative potential of Orwell's fictitious "telescreen" in at least three ways. First, Orwell imagined surveillance taking place through an analogue device that required monitors to be watched in real time and that appears to have lacked any internal capacity to store data. *Id.* at 6, 137. In contrast, the Internet creates digital surveillance with nearly limitless data sterage possibilities and efficient search possibilities in any database using complex algorithms and other techniques of data mining. *See* Pitta, *supra* note 214, at 124 (describing data mining).

Second, surveillance on the Internet involves the subjects of surveillance directly in the project. On the Internet, every mouse click and key stroke transmission by an individual generates personal information. *See supra* Part I.A.2.

Finally, Orwell imagined the threat to the individual as resting in Big Brother, the leader of the state of Oceania. *See* ORWELL, *supra* note 292, at 6. Today, myriad Big and Little Brothers are involved in the collection and processing of personal data in the United States. For example, information technology has greatly encouraged the sharing of personal data *between* govern-ment and business. For a description of this process in the context of health care, see Schwartz, *Privacy Economics*, *supra* note 24, at 12-16.

295. McVeigh v. Cohen, 983 F. Supp. 215, 217 (D.D.C. 1998).

296. *Id.*

under the Navy's guidelines.[297] Indeed, Sporkin's opinion in *McVeigh* noted that cyberspace was a "medium of 'virtual reality' that invites fantasy."[298] The Navy's "search and destroy" mission would have blocked McVeigh's pathfinding among the different aspects of his personality.

Information processing coerces decisionmaking when it undermines an individual's ability to make choices about participation in social and political life. This analysis also reveals the considerable positive role that privacy on the Internet can play in our society. Judge Sporkin commented on the element of fantasy sometimes present in cyberspace behavior.[299] This judicial observation can be elaborated: the Internet, if accompanied by the right kind of rules for access to personal data, has a tremendous potential to become a space for individual deliberations about identity. The pursuit of self-governance today depends on a capacity to make choices among a multiplicity of external and internal demands placed on each of us. As Sandel points out, frequently we must make choices in today's society among "the conflicting obligations that claim us," and live life "with the tension to which multiple loyalties give rise."[300] In a similar vein, Sherry Turkle has argued that "virtuality" can provide an important means for growth.[301] In her view, part of the promise of the Internet is that it allows multiple online personae; Turkle terms these devices, "evocative objects for thinking about the self."[302]

### *C. Constitutive Privacy*

The maintenance of a democratic order requires both deliberative democracy and an individual capacity for self-determination. This Article has explored how the emerging pattern of information use in cyberspace poses a risk to these two essential values. Our task now is to develop privacy standards that are capable of structuring the right kind of information use. In carrying out this task, we begin

297. *Id.* (stating that McVeigh's comments in his profile "do not by definition amount to a declaration of homosexuality" as required by the Navy's Guidelines to justify further military investigation).

298. *Id.* at 219.

299. *See supra* text accompanying note 298.

300. In a similar fashion, Raz advises, "the ideal of personal autonomy is not to be identified with the ideal of giving one's life a unity . . . . The autonomous life may consist of diverse and heterogeneous pursuits." RAZ, *supra* note 287, at 370-71.

301. TURKLE, *supra* note 38, at 256.

302. *Id.*

with Robert Post's scholarship regarding the tort law of privacy. Post argues that the privacy tort safeguards social norms by establishing rules that establish "information preserves."[303] These rules create and maintain both individual and community identity in significant measure.[304]

We can better appreciate the merit of Post's thought by backtracking for a moment to examine the conventional wisdom regarding information privacy law. Most scholars, and much of the law in this area, work around a liberal paradigm that we can term "privacy-control." From the age of computer mainframes in the 1960s to the current reign of the Internet's decentralized networks, academics and the law have gravitated towards the idea of privacy as a personal right to control the use of one's data. In this fashion, a liberal autonomy principle has been identified and conceptualized around an individual's power over her data.

Two academic examples of this thought will initially suffice. In 1967, at the start of the age of mainframe computers, Alan F. Westin's *Privacy and Freedom* provided an early and influential formulation of privacy-control.[305] Westin defined information privacy as the claim of "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[306] For Westin, this interest was an essential element in preserving human freedom. As he observed, "[f]or the individual, there is a need to keep some facts about himself wholly private, and to feel free to decide for himself who shall know other facts, at what time, and under what conditions."[307] In Westin's view, choice-making about the use of one's personal data forms the essential basis for individual self-determination.[308]

Thirty years after Westin's seminal work, at the start of the age of the Internet, Jerry Kang characterized information privacy in a similar fashion.[309] In his opinion, "control is at the heart of information privacy."[310] Kang defined data privacy by quoting the Clinton Administration's Information Infrastructure Task Force, which

303. Post, *Social Foundations*, *supra* note 16, at 979.
304. *Id.* at 985-86.
305. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).
306. *Id.*
307. *Id.* at 368.
308. *Id.*
309. Kang, *supra* note 4, at 1218.
310. *Id.* at 1266.

termed it "an individual's claim to control the terms under which personal information . . . is acquired, disclosed, and used."[311] Here, too, a legal scholar looked to a conception of power over personal data as a title or right. Kang even predicted that such a conception of privacy was likely to be "the foundation for future federal privacy legislation."[312] Many other scholars and much case law have accepted this idea. The conventional wisdom seeks to place the individual at the center of decisionmaking about personal information use by conceiving of privacy as a right of control over data use.

This approach has proven flawed, however, for a number of reasons. From the perspective of this Article, the critical problem with the model of privacy-as-control is that it has not proved capable of generating the kinds of public, quasi-public, and private spaces necessary to promote democratic self-rule. Two of these relevant shortcomings will be discussed later in this Article; they concern this model's underlying use of the neoclassical principle of social ordering through private exchange. Specifically, in Part III, this Article explores the fashion in which individuals have systematically been left unable to interact with private organizations and the government to achieve the proper amount of disclosure or nondisclosure of personal information available on the Internet.[313] These two flaws are: (1) the "knowledge gap," which refers to the widespread ignorance regarding the terms that regulate disclosure or nondisclosure of personal information, and (2) the "consent fallacy," which consists of weaknesses in the nature of agreement to data use.[314] Here, however, this Article discusses two other problematic aspects of the conventional wisdom of information privacy. We can refer to these ideas as (3) the "autonomy trap" and (4) the "data seclusion deception."

To begin with the autonomy trap, the organization of information privacy through individual control of personal data rests on a view of autonomy as a given, preexisting quality. Westin, Kang, and others conceive of the individual's freedom to decide about access to her data as an independent quality that predates and is independent of society.[315] A third scholar, Fred Cate, also provides an excellent

311. *Id.* at 1205 (quoting IITF PRIVACY PRINCIPLES, *supra* note 15, at 5).
312. *Id.* at 1206.
313. *See infra* Part III.C.1.
314. *Id.*
315. CATE, *supra* note 157, at 30; WESTIN, *supra* note 305, at 7; Kang, *supra* note 4, at 1266.

example of this thought. His scholarship views privacy-control as furnishing the basis for rugged self-reliance on a digital frontier.[316] In Cate's view, the process of creating and maintaining privacy rules in the age of the Internet is simple: each person should act for herself, and the government should stay out of the way.[317] Individual stewardship of personal data is nearly always preferable to governmental intervention into a privacy market. As Cate puts it, data privacy must be constructed around "the primacy of individual responsibility and nongovernmental action."[318] Cate's argument is prescriptive; he expects individuals to generate and maintain appropriate information privacy rules through their responsible behavior.

As a policy cornerstone, however, the idea of privacy-control falls straight into the "autonomy trap." The difficulty with privacy-control in the Information Age is that individual self-determination is itself shaped by the processing of personal data. As an indication of this phenomenon, Esther Dyson states, "It's inevitable that people will simply become more comfortable with the fact that more information is known about them on the Net."[319] Dyson also hopefully observes, "we may all become more tolerant if everyone's flaws are more visible."[320] This optimism is misplaced. The autonomy trap ignores the extent to which the use of personal data helps set the terms under which we participate in social and political life and the meaning that we attribute to information-control.

To give an example of an autonomy trap in cyberspace, the act of clicking through a "consent" screen on a Web site may be considered by some observers to be an exercise of self-reliant choice.[321] Yet, this screen can contain boilerplate language that permits all further processing and transmission of one's personal data.[322] Even without a

316. CATE, *supra* note 157, at 30. Indeed, at times in his book, Cate's vision assumes a digital frontier whose residents verge on the misanthropic. As he writes, "privacy may be seen as an antisocial construct. It recognizes the right of the individual, as opposed to anyone else, to determine what he will reveal about himself." *Id.*

317. *Id.* at 103.

318. *Id.*

319. ESTHER DYSON, RELEASE 2.0: A DESIGN FOR LIVING IN THE DIGITAL AGE 216-17 (1997). Dyson is an enterpreneur and one of the leading gurus of emerging information technology.

320. *Id.* at 217.

321. For criticism of an over-reliance on these screens in the context of the licensing of intellectual property, see Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 481-95 (1998); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1283-86 (1995).

322. For a discussion of these kinds of screens, see Lemley, *supra* note 321, at 1283-84.

consent screen, some Web sites place consent boilerplate within a "privacy statement" on their home page or elsewhere on their site. For example, the online version of one New York newspaper states, "By using this site, you agree to the Privacy Policy of the *New York Post*."[323] This language presents the conditions for data processing on a take-it-or-leave-it basis.[324] It seeks to create the legal fiction that all who visit this Web site have expressed informed consent to its data processing practices.[325] An even more extreme manifestation of the "consent trap" is a belief that an initial decision to surf the Web itself is a self-reliant choice to accept all further use of one's personal data generated by this activity.[326]

Thus, the autonomy trap refers to a specific kind of "lock-in" of individual choice. Economists have already identified a series of circumstances under which technology and existing markets constrain consumer choice.[327] For example, most personal computer users are currently locked into Microsoft's Windows as their operating system.[328] A low level of privacy can be locked in as well. One way in which this result is reached is due to industry's standard-setting in a fashion that disfavors privacy. Part III.C.2 will discuss this phenomenon in more detail.

The liberal ideal views autonomous individuals as able to interact freely and equally so long as the government or public does not interfere. The reality is, however, that individuals can be trapped

---

323. N.Y. POST, *Privacy Policy* (visited Sept. 7, 1999) <http://www.nypost.com/legal/-privacy.htm>.

324. As the Disney Web site states:

> By using this site, you signify your assent to the Disney Online Privacy Policy and the GONetwork. If you do not agree to this policy, please do not use our sites. Your continued use of the Disney Online and GONetwork sites following the posting of changes to these terms will mean you accept those changes.

*Disney Online Privacy Policy and Internet Safety Information*, (visited Sept. 7, 1999) <http://-disney.go.com/legal/privacy_policy.html>. This site first presents a privacy policy on a take-it-or-leave-it-basis and then assumes that visitors will regularly scrutinize a four page, single-spaced privacy policy to find whether or not any changes have been made in previous terms. *Id.*

325. For an example of whole-hearted acceptance of this legal fiction, see Matlick, *supra* note 8, at A22. For a path-breaking rejection of this legal fiction in the context of standard form contracts, see W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 556 (1971).

326. *See* Matlick, *supra* note 8, at A22 ("Each time they visit a site, Web users control what information they relinquish and how it is used. To begin with, users do not have to use Web sites in the first place.").

327. *See* Cohen, *supra* note 321, at 482-95; Lemley, *supra* note 321, at 1283-86.

328. Part of this lock-in is due to high switching costs associated with any available alternatives. *See* SHAPIRO & VARIAN, *supra* note 61, at 12.

when such glorification of freedom of action neglects the actual conditions of choice.[329] Here, another problem arises with self-governance through information-control: the "data seclusion deception." The idea of privacy as data seclusion is easy to explain: unless the individual wishes to surrender her personal information, she is to be free to use her privacy right as a trump to keep it confidential or to subject its release to conditions that she alone wishes to set.[330] The individual is to be at the center of shaping data anonymity. Yet, this right to keep data isolated quickly proves illusory because of the demands of the Information Age.

Privacy-control as permitting information seclusion is swept aside because of two collective demands that weigh heavily against this right. First, as shown in this Article's discussion of democratic deliberation, public accountability often requires outside access to personal information.[331] Second, as indicated in this Article's analysis of managerial data processing, bureaucratic rationality often demands outside access to personal information.[332] The idea of data seclusion is a deceptive paradigm because it applies to such a narrow exception. Information seclusion is rarely achievable. As a result, scholars and courts, in their evaluation of interests, frequently reject entirely personal claims framed in terms of privacy-control in favor of requests for personal data made by outside entities, whether the state or private organizations.[333]

In summary then, privacy-control either leads to empty negotiations that fall into the autonomy trap, or collapses completely in the face of the weighty reasons in support of revealing personal in-

---

329. This argument has been cogently made by Julie E. Cohen regarding contracts for intellectual property. *See* Cohen, *supra* note 321, at 515-37; *see also* Slawson, *supra* note 325, at 557-60.

In another area of scholarship, Catharine MacKinnon has expressed a feminism criticism of this formalistic idea of autonomy. She writes:

> The liberal ideal of the private—and privacy as an ideal has been formulated in liberal terms—holds that, so long as the public does not interfere, autonomous individuals interact freely and equally . . . . [Privacy] is, in short, defined by everything that feminism reveals women have never ben allowed to be or to have.

CATHARINE A. MACKINNON, FEMINISM UNMODIFIED: DISCOURSES ON LIFE AND LAW 99 (1987).

330. *See, e.g.*, Matlick, *supra* note 8, at A22.

331. *See supra* Part II.A.

332. *See supra* Part I.C.

333. A fairly standard explanation by courts and scholars is that a given collective interest in disclosure must be considered as more weighty than an individual's interest in nondisclosure. Along these lines, for example, Fred Cate has observed that privacy is "only one tool, which must be used in coordination with other tools, to achieve the ends we desire" before noting that these ends often require access to personal information. CATE, *supra* note 157, at 102.

formation. The danger is one that a belief in the virtue of self-reliant data control cannot acknowledge: information processing itself can undermine an individual's ability to participate in social and political life.[334] The external conditions of data use begin by affecting what it means to agree to information processing, and end by helping to form the conditions of social and individual life. Within this paradigm of privacy-control, however, no solution exists to this dilemma.

In contrast, the scholarship of Robert Post provides a solid foundation for information privacy. His starting point is not the atomistic individual who is to fend for herself against a nosy outside world. As Post observes, information privacy is not "a value asserted by individuals against the demands of a curious and intrusive society," but a necessary aspect of relations with others.[335] Rather than upholding "the interests of individuals against the demands of community," information privacy creates rules that in some significant measure "constitute both individuals and community."[336]

The fashion in which privacy standards carry out this constitutive task is by confining personal information within boundaries that the standards normatively define. In Post's words, privacy's function is to develop "information territories."[337] The contrast with the conventional wisdom is clear; rather than establishing individual privacy-control, constitutive privacy seeks to create boundaries about personal information to help the individual and define terms of life within the community.[338] In the place of a paradigm of choice-making about one's personal data, Post views the establishment of "information preserves" as a critical means for defining social and individual life.[339]

Building on Post's notion of the information territory requires stressing the necessary multidimensionality of these data preserves. A privacy territory should not function as an isolated data fortress. The optimal utilization of personal data is unlikely to be found at the extreme either of absolute privacy or of complete disclosure. Rather, information privacy norms should create shifting, multidimensional data preserves that insulate personal data from different kinds of

334. *See supra* Part II.B.
335. Post, *Social Foundations*, *supra* note 16, at 957.
336. *Id.* at 959.
337. *Id.* at 984-85.
338. *See id.* at 985.
339. *Id.*

observation by different parties. Constitutive privacy is a matter of line-drawing along different coordinates to shape permitted levels of scrutiny. Its limits on access to information will, in turn, have an impact on the extent to which certain actions or expressions of identity are encouraged or discouraged.

A Supreme Court decision, *Planned Parenthood v. Casey*, offers a good introduction to constitutive privacy.[340] One aspect of *Casey* has generated the most commentary; this decision marks the moment when the Supreme Court declined to reverse *Roe v. Wade*.[341] In *Casey*, a plurality of five justices reaffirmed *Roe*'s essential holding recognizing a woman's right to choose an abortion before fetal viability.[342] Beyond this element of *Casey*, the Supreme Court invalidated aspects of a Pennsylvania law mandating disclosure and record-keeping requirements for the abortion procedure.[343]

This state law sought to employ physicians as government agents to ensure that husbands were informed of their wives' reproductive choices. Among the statute's record-keeping provisions, Pennsylvania had required that physicians collect a statement indicating either spousal notification by the woman seeking an abortion, or that a significant reason existed to allow bypass of such notification.[344] The law also placed strong pressures on physicians to ensure their fidelity in this role. Physicians who failed to collect the required spousal notification data from women would be subject both to revocation of their medical licenses and to liability to the husbands for damages.[345]

The *Casey* Court found this aspect of the Pennsylvania law to be unconstitutional.[346] In doing so, it created an information preserve for wives who seek independence in making constitutionally-protected reproductive decisions. This information territory was required, in the judgment of Justice O'Connor's plurality opinion, because of the high level of domestic violence in the United States and the "secrecy

340. Planned Parenthood v. Casey, 505 U.S. 833 (1992).

341. For Ronald Dworkin's account of *Casey* as perhaps "one of the most important Court decisions of this generation," see RONALD DWORKIN, FREEDOM'S LAW: THE MORAL READING OF THE AMERICAN CONSTITUTION 117 (1996). For Bruce Ackerman's analysis, see BRUCE ACKERMAN, WE THE PEOPLE: TRANSFORMATIONS 397-403 (1991).

342. *Casey*, 505 U.S. at 846.

343. *See id.* at 887-91, 899-901.

344. *See id.* at 888-89.

345. *See id.* at 887-88.

346. *See id.* at 898.

[that] typically shrouds abusive families."[347] Through such secrecy about family violence, law and social norms had already created a destructive information territory about the family, which the plurality self-consciously sought to undermine. As a result, a spousal notification requirement, even one with a bypass provision, would devastate women's free decisionmaking about reproductive choice.[348]

*Casey* indicates how restrictions on access to personal information serve to protect actions and identity. This decision also reveals a further, critical point about constitutive privacy: the structure that it creates must be multidimensional. Under conditions of modern life, privacy rules must combine both disclosure and confidentiality standards for the same piece of information.[349] The state's release to a woman's husband of information that revealed her wish to have an abortion would threaten reproductive freedom; yet, the Supreme Court in *Casey* also upheld aspects of this law that required limited disclosures of personal data about the woman to the state for public health purposes—including information relating to the nature of the abortion procedure performed.[350] From this perspective, we see that *Casey* created two aspects of the necessary multi-dimensional rules. The Supreme Court found that an informational preserve was: (1) constitutionally mandated for wives who seek to make reproductive decisions, and (2) did not extend to the state's public health reporting requirement.[351] Many information privacy issues are not constitutionally cognizable, however, and additional dimensions of this particular data preserve are needed to map the conditions under which this information is to be shared with other entities, such as health insurance companies.[352]

---

347. *Id.* at 889.

348. *See id.* at 893-94. As O'Connor's plurality opinion notes, the Pennsylvania law would empower a husband "with this troubling degree of authority over his wife." *Id.* at 898. A consequence of spousal notification would be men preventing "a significant number of women from obtaining an abortion." *Id.* at 893.

349. *See* Schwartz, *Privacy Economics*, *supra* note 24, at 52-55.

350. *Casey*, 505 U.S. at 900-01, 994. In an earlier case, *Thornburgh v. American College of Obstetricians & Gynecologists*, 476 U.S. 747, 765-69 (1986), the Supreme Court voided a more detailed public health reporting requirement that was likely to reveal information to the public about abortion.

351. *See Casey*, 505 U.S. at 898-90.

352. This task is less the realm of higher law than such non-constitutional means as health care privacy statutes. For a discussion, see NATIONAL RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 39-46 (1997); SCHWARTZ & REIDENBERG, *supra* note 48, at 172-84.

## III. A MULTIDIMENSIONAL PRIVACY TERRITORY FOR CYBERSPACE

Thus far, this discussion of privacy territories has been in fairly general terms. For example, it has analyzed the kind of confidentiality and disclosure rules that the *Casey* Court found to be constitutionally mandated for information about abortions. Privacy territories are also needed for personal data in cyberspace; multidimensional privacy norms must draw on workable standards capable of creating information preserves. Participants in cyberspace need access to public, quasi-public, and private spaces where they can engage in civic dialogue and the process of self-definition. Moreover, these information territories must be well-defined with enforceable rules that set different boundaries for different entities. The first issue regarding these privacy territories for the Internet is their content; this Part will also assess different regulatory techniques for putting standards of constitutive privacy into place.

### *A. Post's Pessimism*

Robert Post has a specific method in mind for developing privacy rules. His model first identifies the importance of an informational privacy interest in reference to an act and then makes a judgment about the appropriate use of the related personal information.[353] This judgment confirms or elaborates shared values and thereby strengthens community.[354] For Post, moreover, the Restatement of Torts' skeletal provisions for privacy already express the essential legal standards.[355] In the resulting system, litigants, judges, and juries draw on and refine the legal expression of general community norms. This process entails open-ended inquiries around such issues as whether the "reasonable person" would find certain invasions of privacy "highly offensive."[356]

In Post's view, this legal method works because it rests upon a certain kind of community. Post argues that "privacy is for us a living reality only because we enjoy a certain kind of communal existence."[357]

---

353. Post, *Social Foundations*, *supra* note 16, at 979.

354. The necessary communal universe is one, for example, in which we all know that a wiretap in a marital bedroom violates "the general level of moral judgment in the community." *Id.* at 959-61.

355. *Id.* at 964-65 (citing RESTATEMENT (SECOND) OF TORTS, § 652B-E).

356. *Id.* at 978-79.

357. *Id.* at 1010.

Only social life with "density and intensity" is able to sustain the vital behavioral rules on which "the ritual idiom" of information privacy rests.[358] At precisely this moment, however, a difficulty arises: in Post's judgment, the nature of community is changing. We now interact increasingly with large bureaucracies, and the resulting relationships are not sufficiently textured to generate and sustain privacy rules.[359] These ties are not "social and communal," but are based on managerial efficiency.[360] According to his pessimistic verdict, social life increasingly lacks the characteristics which are necessary to generate privacy rules.[361]

Initially, the Internet's current low level of privacy seems to confirm Post's pessimism about the creation of privacy rules under the conditions of contemporary life. Such gloom might even cause one to sink into outright depression; after all, the right kind of rules about privacy are needed because cyberspace is our new location for shared life.[362] Fortunately, it is not necessary to join Post's pessimism about creating information privacy rules applicable to the Internet.

One of the most striking aspects of cyberspace is the "density and intensity" of relations on it. Whether in MUDs, Web sites organized by special interest communities, or electronic campaigns centered around cyber-petitions, the Internet is the focus of dense and intense relations.[363] Millions of people now seek connections with others in cyberspace, and some first generation scholars of the Internet even argne that the shared experience of this electronic realm makes those who are using it the best parties to design rules for ordering their behavior.[364] This claim is overstated; for one thing, spillover from

358. *See id.* at 1009.

359. *See id.*

360. *Id.* at 1009-10.

361. *See id.* at 1010.

362. *See supra* Part II.A-B.

363. *See, e.g.*, DOHENY-FARINA, *supra* note 243, at 66 (noting the "emotional intensity of interpersonal relationships that develop online"); GURAK, *supra* note 254, at 42 (noting the "sense of community felt by those on the Internet"); TURKLE, *supra* note 38, at 78-114 (discussing friendships and emotionally intense behavior in MUDs).

364. For examples of leading regulation skeptics, see David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1393 (1996); see also James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 178 (1997) (explaining that "for a long time, the Internet's enthusiasts have believed that it would be largely immune from state regulation"); Gillet & Kapor, *supra* note 60, at 33-34 (noting that authority on Internet tends to be "bottom up" and "scattered across many different organizations"); Matlick, *supra* note 8, at A22 (noting government privacy regulations for the Web would "create a new reliance on government solutions to online 'problems,' eroding the cornerstones of individual freedom, responsibility and accountability that form the

cyberspace into Real Space alone is a significant enough reason under various circumstances to justify external regulation.[365] Nevertheless, in the context of online privacy we can reject Post's negative conclusions about the inability to create meaningful privacy rules in the age of organizations.

At precisely this point, however, a further problem appears: the model that Post locates in tort law is unlikely to be successful for generating privacy territories for cyberspace. Litigation under the privacy tort looks at such broad standards as "reasonable" privacy and "highly offensive" information use.[366] Through the process of adjudicating the meaning of these terms in different settings, the tort provides a forum for an "assessment of the total context of the communicative act by which that information is revealed."[367] Enforcement by aggrieved parties will lead to a legal verdict that represents a social judgment about the public/private contours of different activities and the personal data that they generate.[368] On the Internet, however, a different process of norm generation becomes necessary.

The necessary consensus about how community members process and share personal data in cyberspace cannot be left to emerge slowly over time through the tools of tort law and the push and pull of litigants, judges, and juries. This Article has already suggested two problems with privacy-control that also speak to the weaknesses of Post's reliance on tort litigation. First, the discussion of an "autonomy trap" indicated that the use of personal data itself helps set the terms under which we participate in social and political life and the meaning we give to information-control.[369] As a result, what is "reasonable" privacy and "highly offensive" information use is not exogenous to social trends regarding data processing, but rather is likely to reflect closely that which already takes place. In particular,

---

foundation of Internet culture"). *See generally* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993 (1994) (discussing various approaches taken towards resolving cyberspace legal issues); Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities,* 38 VILL. L. REV. 349 (1993) (proposing a framework for dispute resolution in cases where there has been a denial of access to electronic networks or where defamatory messages have been transmitted across the network).

365. *See* Cohen, *supra* note 321, at 540-43; Goldsmith, *supra* note 68, at 1201.

366. For an analysis, see Post, *Social Foundations, supra* note 16, at 978-95.

367. *Id.* at 981.

368. As Post states, "[t]his pattern can be viewed as an attempt to disperse enforcement authority." *Id.* at 966.

369. *See supra* Part II.C.

computer technology can lock-in a poor level of privacy, which will then diminish beliefs about a "reasonable" level of privacy.

Second, the Article pointed to the "data seclusion deception" regarding the rejection of personal claims for information isolation in favor of the demands of outside organizations.[370] It argued that courts and academics predictably will favor collective demands for disclosure over privacy interests framed as an individual right of control. This issue reappears in the context of tort litigation; litigation of tort privacy claims also is likely to over-disclose personal data in cyberspace through its initial framing of privacy interests as narrow individual claims and its likely rejection of such separate interests.[371]

These two issues suggest that, given only general privacy tort standards, judges and juries will create a stable but bad equilibrium about personal data use. Indeed, as a threshold matter, the common law privacy tort will generate adequate privacy norms through litigation self-help only when the law provides sufficient incentives for plaintiffs to bring their claims to court.[372] The incentives for this volume of tort privacy litigation are not now in place, and this factor alone helps explain a development that this Article has noted: thus far, the tort law of privacy has been of no help in responding to personal data use on the Internet.[373] Indeed, this lack of incentives and other flaws in the privacy tort have rendered it largely useless in Real Space.[374] Common law litigation is unlikely to develop the right kind of privacy territories on the Internet.

### *B. The Necessary Fair Information Practices*

The protection of online privacy requires the establishment of more detailed norms in a more rapid fashion than the common law tort is likely to provide. This Article will now build on its concept of privacy territories by utilizing the idea of "fair information practices,"

---

370. *See id.*

371. Emblematic is *Smyth v. Pillsbury*, in which the federal district court considered only one worker's interest in e-mail privacy rather than the likely larger impact when employers that also act as ISPs are not held to their promises of confidentiality. Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

372. *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 299 (2d ed. 1997) (noting that "costly litigation" will prevent tort victims from bringing suit, "and so the potential injurers will not receive the signal from the tort-liability system that what they are doing is unacceptable").

373. *See supra* Part I.B.

374. Reidenberg & Schwartz, *supra* note 156, at 20; Kang, *supra* note 4, at 1231.

which are the building blocks of modern information privacy law. This Article will further refine these standards where necessary through reliance on mandatory and default rules.

In the Information Age, one-size privacy will not be adequate for all situations; our task is to develop nuanced concepts for use in charting and fixing the bounds of different privacy domains. Cyberspace must have public, quasi-public, and private spaces where individuals can engage in civic dialogue and the process of self-definition. Moreover, these data territories must be well-defined through enforceable rules. Fair information practices provide the precise tools for this task; these standards allow the definition of privacy spaces along more complex coordinates than the common law privacy tort permits. A distillation of fair information principles should be made around four requirements: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight.[375]

In setting out these fair information practices, this Article will also draw on the concept of mandatory and default rules. Social and legal norms often fall into two general categories. These rules set either background conditions around which parties may negotiate or immutable standards that are not to be altered.[376] For example, while parties are free to contract around most rules of contract law, the UCC contains an immutable requirement that all parties perform contracts in good faith.[377] Or to point to corporate law, parties are not free to negotiate around the detailed set of rules for corporate directors that "prevent fraud and opportunism."[378]

---

375. For a previous proposal regarding fair information practices, see Schwartz, *Privacy Economics*, *supra* note 24, at 57-67.

376. Privacy scholars have already begun to make use of the concept of default and mandatory rules. *See, e.g.*, Kang, *supra* note 4, at 1246-65; Richard Murphy, *supra* note 164, at 2402-03; Schwartz, *Privacy Economics*, *supra* noto 24, at 53-56.

For a general discussion of default and mandatory rules in the context of cyberspace, see Goldsmith, *supra* noto 68, at 1213-16. For analysis of the function in Real Space of default and mandatory rules, see Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989); Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 730-32 (1992) [hereinafter Ayres & Gertner, *Optimal Choice*].

377. *See* U.C.C. § 1-203 (1994).

378. John C. Coffee, Jr., *The Mandatory/Enabling Balance in Corporate Law: An Essay on the Judicial Role*, 89 COLUM. L. REV. 1618, 1624 (1989). *See also* Jeffrey N. Gordon, *The Mandatory Structure of Corporate Law*, 89 COLUM. L. REV. 1549, 1555-85 (1989) (describing the role that mandatory rules play in a contractual system).

A final introductory comment to this Section: in describing information privacy territories on the Internet, the Section seeks to spell out the approach to personal data use that best protects democratic self-rule. This task is unabashedly normative. Within the limits of an Article of manageable length, however, it is impossible to respond to every element of the privacy horror show that this Article has depicted. Rather, my goals are to develop differentiated principles capable of responding to information use in varied circumstances in cyberspace; to evaluate different methods of setting them in place; and, finally, throughout this Section, to draw on examples that indicate how these fair information standards should respond to the commercial use of personal data on the Internet.

### 1. A Fabric of Defined Obligations

Let us first consider the necessary fabric of defined obligations for personal data on the Internet. As this Article has shown, the Internet is increasing the quality, quantity, and accessibility of personal information relating to behavior both in cyberspace and Real Space.[379] It is also reducing the zones of once available data anonymity.[380] This current emerging standard of maximum collection and use of personal data is inconsistent with the values of democratic community and individual self-determination.

One way to think of this developing norm is as a general default rule in favor of widespread personal data collection and transmission. This norm has been expressed through technological, social, and legal standards. In some instances, however, technology, such as encryption programs and anonymity filters, can help counter some of the elements of the privacy horror show that this Article has depicted.[381] In this way, determined and adept individuals have already been able to negotiate around some of these existing default disclosure norms.[382] Yet, technology solutions favor the technologi-

379. *See supra* Parts I.A.2 & I.C.

380. *See supra* Part I.C.

381. It might help, for example, in increasing the confidentiality of personal data on one's computer or providing ways to surf in anonymity. *See* PFAFFENBERGER, supra note 80, at 230-255; 269-72 (instructing users how te post messages anonymously and use encrypted e-mail). *But see* Kang, *supra* note 4, at 1244 (noting that technology is no panacea for solving privacy issues).

382. For a description of technology's possible contributions, see, e.g., MARCUS GONCALVES ET AL., INTERNET PRIVACY KIT 52-165 (1997); PFAFFENBERGER, *supra* note 80, at 137-272.

cally savvy; for most Americans, such self-help is not a realistic alternative.[383] In addition, these solutions are limited even on their own terms.[384]

One should not accept a disclosure default norm of maximum data collection and use in cyberspace as fate. In at least some other areas, American society has successfully opposed the establishment of such standards of maximum personal information use. This Article has already mentioned one such moment, which culminated in the enactment of the Video Privacy Protection Act.[385] It is worth noting two other instances in which such maximum information defaults have been reversed.

A second countering of a default of maximum disclosure was set in place through the Cable Communications Policy Act of 1984, which created careful safeguards regarding the personal data of subscribers to cable services.[386] Of particular note is this law's restrictions on cable operators that prevent collection of personally identifiable information beyond the minimum necessary to render the service or to detect unauthorized reception of cable communications.[387] The third such statutory move came in the Telecommunications Act of 1996.[388] Here, Congress prohibited telecommunications carriers from using customer proprietary network information ("CPNI") beyond "the provision of . . . the telecommunications service from which such information is derived."[389] The FCC has ruled that this language

383. Jerry Kang has also noted the negative distributional consequences of a public policy that relies on technology to supply informational privacy. *See* Kang, *supra* note 4, at 1245 ("Only those sophisticated enough to take advantage of public key encryption and anonymity filters may do so, with the rest of the population left defenseless due to ignorance.").

384. One problem is that this approach can lead to a "privacy arms race," in which privacy protecting technology spurs further development of privacy invading technology. For example, the software utilities that allow hard drives to be "wiped" have encouraged development of software that permits reading of these erased files. *See* Bennahum, *supra* note 80, at 102-04. For a more detailed discussion of the role of technology in privacy protection, see *infra* Parts III.C.1-2.

385. 18 U.S.C. § 2710 (1994).

386. 47 U.S.C. § 551 (1995).

387. *Id.* § 551(b).

388. 47 U.S.C. § 151-614 (Supp. III 1999).

389. *Id.* § 222(c)(1)(B). As the Federal Communications Commission explained in issuing regulations under this section of the Telecommunications Act, "CPNI includes information that is extremely personal to customers as well as commercially valuable to carriers, such as to whom, where and when a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent the service is used." F.C.C., Implementation of the Telecommunications Act of 1996, Second Report and Order, CC Docket No. 96-115, ¶ 2 (Feb. 19, 1999).

prevents carriers from marketing services outside of customers' "existing service relationship without express customer approval."[390] In a fashion similar to these three examples, we need a privacy norm in cyberspace that counters the current emerging norm of unrestricted data collection and processing. To anticipate this Article's future argument, in all three instances, it has been statutory law that has created such restrictions rather than market mechanisms or industry self-regulation.[391]

The necessary standard for personal data use on the Internet should contain both default and mandatory components. The *default norm* for cyberspace should permit: (1) collection of only the minimum amount of personal data necessary, and (2) further transmission of this information only for purposes that are compatible with the original collection.[392] The idea of minimization requires the collection of the least amount of personal data necessary to accomplish the underlying purpose for which the information is sought.[393] The idea of compatibility calls for a significant degree of convergence between the purpose for which the personal information was gathered and any subsequent use.[394]

A move beyond this default norm by data processors would require formal consent from individuals.[395] Such an approach will lead to a higher quality of negotiations than those around the current default standard. Because formal consent becomes necessary only

---

390. In the Matter of Implementation of the Telecommunications Act of 1996, CC Docket No. 96-115, at ¶ 4(b). The FCC also declared that telephone companies, termed "carriers" in telecommunications law's terminology, were permitted to use customer proprietary network information ("CPNI") and other customer information obtained in their provision of telecommunication services "to market improvements or enhancements to the package of telecommunications services the carrier already provides to a particular customer." Telecommunications Act of 1996, Clarification, CC Docket No. 96-115, ¶ 2 (May 21, 1998). For a legal attack on these regulations, see U.S. West v. F.C.C., 182 F.3d 1224 (10th Cir. 1999).

391. *See infra* Parts III.C.2-3.

392. For a health care privacy bill that attempted a similar approach, see Health Information Privacy Act of 1999, H.R. 1941, 106th Cong. (1999).

For a discussion of this proposed approach for health care information, see Schwartz, *Privacy Economics*, *supra* note 24, at 59-60.

393. For an analogous recommendation, see PRIVACY STUDY COMM'N, *supra* note 24, at 304 (arguing that medical records should be made "available only to authorized recipients and on a 'need-to-know' basis").

394. In the context of the Privacy Act, the Third Circuit has carried out an insightful discussion of "compatibility." *See* Britt v. Naval Investigative Serv., 886 F.2d 544, 550 (3d Cir. 1989).

395. *Cf.* Ayres & Gertner, *Optimal Choice*, *supra* note 376, at 761 (examining the consequences of establishing default rules that favor less informed parties to contracts).

under circumstances when the processing of information occurs beyond the functionally necessary, consent screens will become less frequent and subject to greater scrutiny.[396]

In some limited circumstances, however, this kind of default rule is likely to cause overdisclosure or underdisclosure of personal data in a way that threatens either democratic community or individual self-determination. To counter this threat, some narrowly defined *mandatory norms* are required for personal data use. For example, our society generally has not looked for negotiations around default rules as the way to resolve issues about law enforcement agencies' access to personal data.[397] More specifically, it is unlikely that three-party negotiations involving law enforcement agencies, ISPs, and customers will lead to the proper level of disclosure of personal data.[398] The appropriate norm for cyberspace makes use of the judiciary and its power to issue subpoenas: a law enforcement agency should be permitted to obtain protected personal data only upon a showing of clear and convincing evidence of materiality to criminal activity. This kind of disclosure requirement is already required by law for the personal data that cable companies collect.[399]

---

396. Existing laws in the United States and abroad have taken a similar approach to narrow use of a consent requirement by first spelling out statutory restrictions on the use of personal data. To point to an American example, this model is followed by the Cable Communications Policy Act of 1984, 47 U.S.C. § 551(b) (1995). Moreover, in the Federal Republic of Germany, the Teleservices Data Protection Act of 1997 provides strong limitations on the use of personal information by providers of telecommunication services, including those on the Internet. An English text of this important statute is reprinted in THE PRIVACY LAW SOURCEBOOK 299-300 (Marc Rotenberg ed., 1998). For analysis of this law, see JOEL R. REIDENBERG & PAUL M. SCHWARTZ, ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY: REGULATORY RESPONSES 22-115 (1998). This report, which was commissioned by the European Union's Directorate General on Internal Market and Finance Services, examines the emerging response to issues of online privacy in Belgium, France, Germany, and the Unitod Kingdom. It is available at <http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.htm>.

397. The law enforcement exception has proved to be the single most difficult drafting issue in the receut failed attempts in Cougress to create a health information privacy bill. For an example of a proposed statute with a law enforcement exception, see Fair Health Information Practices Act of 1997, H.R. 52, 105th Cong. §§ 119-120 (providing for disclosure of health information to a law enforcement agency in certain limited circumstances).

398. To the extent that these rules are expressed through law, parties can, of course, seek to alter them through recourse to the legislative arena. While mandatory rules are relatively unexplored in the legal literature, *see, e.g.*, Murphy, *supra* note 164, at 2381-416 (examining privacy rules implied in contracts), they appear increasingly important as more of public well-being is tied to state agencies and private organizations that collect personal data. *See supra* Part I.C.

399. *See* 47 U.S.C. § 551(h) (Supp. 1990).

### 2. Transparent Processing Systems

This Article has demonstrated the fashion in which the Internet is decimating previous barriers to data sharing.[400] Yet, few individuals today have a sense of the Internet's data topography. Widespread ignorance concerning the precise nature of personal information use in cyberspace is the rule, not the exception.[401] At the same time, a growing, if vagne, sense exists that there is a privacy problem on the Internet.[402] A continuation of this secretive processing of personal data risks a chilling of discussions necessary to democratic community as well as suppression of an individual's free choice. In contrast, notice of data processing practices in cyberspace would provide knowledge of whether one will be assigned the role of town crier. Such notice, if part of adequate substantive limitations on data collection and transmission, would provide the necessary insulation for an individual's reflective facilities and the larger process of deliberative decisionmaking.

The second fair information practice requires a structuring of data processing to make it open and understandable to individuals. The transparency standard requires the sharing of knowledge regarding how one's personal information will be utilized.[403] Here, a mandatory requirement must provide for notice of the details of personal data collection.[404] This information should be provided prior to the beginning of data collection and be readily available at all times. A notice requirement should be mandatory because of the importance of knowledge of cyberspace's data topographies; only when more individuals have a sense of the Internet's precise data zones will adequate negotiations take place around a default standard of minimal data use.[405]

---

400. *See supra* Part I.A.2.

401. *See supra* text accompanying notes 229-33.

402. For a collection of polling information, see *supra* note 7.

403. For a discussion in the context of the Privacy Act, see SCHWARTZ & REIDENBERG, *supra* note 48, at 104-08.

404. The discussion of notice by The Privacy Protection Study Commission in 1976 remains highly useful. *See* PRIVACY STUDY COMM'N, *supra* note 24, at 18-19 (recom-mending authorization as a pre-condition to disclosure and asserting that the disclosure should contain no information other than the authorized request specifies).

405. *Cf.* Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630, 669-70 (1979) (arguing that consumers may benefit from the creation of statutes that make relevant information readily available).

An individual must be provided with information regarding the type and scope of processing of her personal data.[406] The notice document should first describe purposes for which data are collected, including if any third parties will be receiving the information. Second, this writing should specify the nature of any limits, legal or otherwise, on additional, unrelated use or disclosure of the collected data. Finally, the notice document should describe the extent of any personal interest that the individual is assigned. As this Article explains in the next Section, these interests are both substantive and procedural in nature.

### 3. Limited Procedural and Substantive Rights

This Article has argued that the idea of privacy through data-control is of limited usefulness in the Information Age. At present, social and legal norms about privacy promise too much, namely data control, and deliver too little.[407] Rather than a right of control, the focus of information privacy law should be construction of a privacy space that promotes civil society and individual decisionmaking. As part of this project, the third fair information standard seeks to involve the individual in this enterprise through the assignment to her of certain limited procedural and substantive rights. At the present time, however, these individual interests are absent from cyberspace.[408] An individual cannot find out the personal information that is stored about her, cannot know who has access to this information, and cannot correct it when inaccurate. The absence of enforceable expectations about where public, quasi-public, and private territories are in cyberspace will deter individuals from participating in activities that promote cyber-democracy and self-definition on the Internet.

Three significant procedural rights must be created to protect personal data generated in cyberspace. It must be stressed, however, that these rights are useful only when external standards also exist to prevent empty consent leading to uninformed, nonvoluntary exchanges.[409] The individual whose personal data are processed must: (1) be able to allow or refuse collection of more than a minimum

406. These protections are modeled on those found in the Privacy Act. *See* 5 U.S.C. § 552a(e)(3) (1994). For an analysis of that law, see SCHWARTZ & REIDENBERG, *supra* note 48, at 104-07.

407. *See supra* Part II.C.

408. *See supra* Part I.B.

409. *See infra* text accompanying note 451.

amount of these data or further use for a noncompatible use; (2) be informed of the data consequences of relevant behavior, such as signing up for service with an ISP or entering a specific Web site; and (3) be granted a mechanism by which she can inspect and correct personal data and find out which parties have gained access to her records.[410]

The first two of these interests have already been mentioned; they relate to the requirements of defined obligations for data processors and transparent processing of information. As for the third requirement, it indicates how technology can make possible not only the invasion of privacy, but also its protection. This last procedural interest obliges those who process personal data to utilize software that allows the creation of audit trails.[411] In the health care setting, as the medical profession shifts to electronic health care records, this kind of software is already being developed.[412] In cyberspace, a right of access by individuals to such audit trails will create a strong deterrence to an institution's violation of its privacy standards.

As for the creation of substantive rights, they begin with an interest in informed consent. Here, I wish to build on my critique of reliance on empty consent mechanisms.[413] One's clicking through a consent screen to signify surrendering of her personal data for all future purposes is an example of both uninformed consent and a bad bargain in cyberspace. This Article's solution begins with a default norm of minimal information collection with further transmission for only compatible purposes.[414] It goes on to require formal documentation of consent only under circumstances that exceed the processing of information beyond the functionally necessary. Combined with transparent processing and audit trails, this approach will encourage more careful scrutiny of consent screens and improve the quality of negotiations in a privacy marketplace.

In addition, substantive interests for the individual require the provision of effective remedies, which are absent from the current

410. For a discussion of related procedural interests, see PRIVACY STUDY COMM'N, *supra* note 24, at 20-22 (recommending an "expectation of confidentiality" comprised of a legally enforceable duty of the record keeper and a legal interest in the record for the individual).

411. *See* NATIONAL RESEARCH COUNCIL, *supra* note 352, at 94-99 (explaining that audit trails may protect privacy by deterring privacy invasions and by providing evidence of possible invasions).

412. *See id.* at 98-99 (discussing different audit trail technologies).

413. *See supra* text accompanying notes 319-34.

414. *See supra* Part III.B.1.

norms for cyberspace privacy.[415] This protection must provide timely and adequate relief when personal interests are violated. In different settings in cyberspace, standards of relief must be created that are commensurate to the harm involved in the misuse of personal data.[416]

### 4. Establishment of Independent Oversight

The fourth and final fair information practice for cyberspace is external oversight of data processing. In an age of rapid technological change, the effective balancing of confidentiality and disclosure depends on the assistance of outside, expert bodies who monitor developments within the different information territories of cyberspace.[417] At present, the lack of an independent centralized point of contact for individuals regarding information privacy issues further heightens the already widespread individual ignorance of data processing practices.[418] Indeed, a recent report of the National Research Council's Special Committee on Privacy drew on the idea of the ombudsman in suggesting the creation for consumers of "a visible, centralized point of contact regarding privacy issues."[419] It is also difficult for Congress and other governmental bodies to gain independent advice regarding the privacy consequences of different technological developments and of how well existing regulation is functioning.[420]

In this context, a role exists for both governmental and nongovernmental oversight entities. We begin with the government. Such existing agencies as the FCC and the FTC have already made important contributions to monitoring developments in information

---

415. *See generally supra* Part I.B.

416. For example, violations of a limited group of fair information practices should be punishable by criminal penalties. Among those violations would be obtaining personal information under false pretenses with the intent to apply such information for monetary gain. *See* Schwartz, *Privacy Economics*, *supra* note 24, at 64-65. This form of threat represents a coercive transfer that should be met by the imposition of criminal penalties. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 217-23 (4th ed. 1992).

417. For a discussion of these oversight agencies in Europe, see FLAHERTY, *supra* note 24, at 385-404; Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 473-88 (1995).

418. *See* Schwartz, *Privacy Economics*, *supra* note 24, at 66-68 (advocating the creation of a national data protection agency that would provide information on privacy issues to the legislature, citizens, and community).

419. NATIONAL RESEARCH COUNCIL, *supra* note 352, at 184.

420. *See* Schwartz, *Privacy Economics*, *supra* note 24, at 66-68 (arguing for the establishment of a national data protection agency structured as an independent advisory body).

use in cyberspace.[421] Where permitted, these agencies have also taken enforcement actions and further developed existing law.[422] Beyond these agencies, however, a United States Data Protection Commission is needed to carry out a more general oversight function.[423] The FCC and the FTC have specific and narrow mandates related respectively to promoting "the public interest" in access to telecommunications and hindering "unfair or deceptive trade practices."[424] A more general governmental body is needed to assist the public, social groups, and the legislature in understanding strengths and weaknesses in the boundaries of existing information territories.

It is striking that virtually all Western nations, with the exception of the United States, have created such independent government data protection commissions.[425] Of the different international models, the "advisory model," utilized in countries including Canada and Germany, provides the best example for the United States.[426] Data protection commissions in these countries are independent advisory bodies without any direct enforcement powers.[427] They advise the legislature, act as ombudsmen for citizen complaints, and audit the federal government's processing of personal information.[428] They also carry out the important task of informing the public and the media of developments concerning data privacy.[429] These generalist data protection agencies are also playing a significant role outside of the United States in shaping a social response to the explo-

---

421. *See supra* text accompanying notes 185-97, 388-90.

Both organizations provide important information about their privacy activities on their Web sites. *See* FTC: *About Privacy* (visited Apr. 5, 1999) <http://www.ftc.gov/privacy/index-html>; *FCC Clarifies Customer Privacy Provisions of 1996 Act* (visited Apr. 5, 1999) <http://-www.fcc.gov/Bureaus/Common_Carrier/News_Releases/1998/-nrcc8019.html> (providing a case sensitive URL).

422. *See infra* text accompanying notes 185-91, 390.

423. *See generally* BARBER, *Supra* note 245, at 310 (calling for encouragement of ombudsmen in civil society).

424. *See* 15 U.S.C. §§ 45, 46 (1988) (establishing role of FTC); 47 U.S.C. §§ 151, 303 (1994) (establishing role of FCC). It must be added that a movement is underway to reduce the FCC's various responsibilities, or even to abolish this agency. *See, e.g.*, PETER HUBER, LAW AND DISORDER IN CYBERSPACE: ABOLISH THE FCC AND LET THE COMMON LAW RULE THE TELECOSM 200-202 (1998); Bryan Gruley, *From 'Dr. Dissent' Even a 'Yes' Vote Can Sound Like 'No,'* WALL ST. J., Apr. 6, 1999, at A1.

425. *See* FLAHERTY, *supra* note 24, at 394-97.

426. *See id.* at 40-47, 259-62.

427. *See id.*

428. *See id.* at 385-404; *see also* BENNETT, *supra* note 15, at 195-229.

429. *See* Schwartz, *supra* note 417, at 492-95.

sion of personal data use that has accompanied the rise of the Internet.[430]

Beyond a United States Data Protection Commission, nongovernmental monitoring bodies also have an important role to play in the age of the Internet. Of most potential is oversight by nongovernmental "Trusted Third Parties." Such entities, including "infomediaries" and outside "privacy seal" companies, are to negotiate on behalf of consumers and ensure that data processors keep their privacy promises.[431] These companies can also be a venue for seeking redress after violations of privacy agreements. In the absence of real independence and the right market conditions, however, Trusted Third Parties will not be worthy of individuals' trust. At present, moreover, the existing Trusted Third Parties suffer from notable weaknesses.[432]

### *C. The Creation of Fair Information Practices: The Market, Self-Regulation, and Law*

This Article has now identified the ideal privacy norms for the promotion of democratic community and individual self-determination. The issue then becomes determining the ideal fashion for setting these rules in place. Current debate focuses on three possibilities: the market, industry self-regulation, and the law. By far, the most popular of these alternatives at present is industry self-regulation.[433] This Article will argue, however, that reliance on the market and industry under current conditions will have unsatisfactory results unless the law first imposes the necessary fair information practices.

#### 1. Let's Make A Deal: The Privacy Market

A pure market approach to privacy relies on interactions between individuals and data processors to generate and maintain

430. REIDENBERG & SCHWARTZ, *supra* note 396, at 44-64.

431. John Hagel, III and Jeffrey F. Rayport first predicted the development of these organizations and coined the eponymous (if hardly euphonous) term, "infomediaries." John Hagel, III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, HARV. BUS. REV., Jan.-Feb. 1997, at 53, 54; *see infra* Part III.C.

432. *See infra* Parts III.C.1-2.

433. *See supra* text accompanying notes 199-205.

appropriate norms for information privacy.[434] Yet, the market, like government, is a creation of human choice, and all markets do not function equally well to serve different aims.[435] In particular, I would like to distinguish at this point between making the Web safe for e-commerce, which is the focus of much information policy at present, and the possibility of using market exchanges to develop information territories for privacy in cyberspace.

At present, information policy in the United States focuses on facilitating wealth-creating transfers over the Internet. As discussed earlier, the Clinton Administration is striving to make the Web and the world safe for e-commerce.[436] This Article takes a different tack; its perspective is not in opposition to a commercial function for cyberspace, but rather for the necessity of something other than shopping on the Internet. Specifically, cyberspace has the potential to revitalize participatory democracy if we can establish the right level of disclosure/confidentiality in it. While the marketplace can have a role in generating the borders of multidimensional territories in cyberspace, the current market for privacy is unlikely to reach a result that will promote democratic self-rule. Once fair information practices are firmly established, however, the market can play an important role in maintaining and enforcing these norms.

Four reasons exist for the current failure of the privacy market. Two of these factors are known suspects by this point; Part II of this Article explained how the autonomy trap and the data seclusion deception contributed to difficulties with the liberal idea of data-control by individuals.[437] Just as these phenomena undercut the control paradigm, they contribute to shortcomings in the current privacy market. First, data exchanges depend on autonomous individuals who are able to negotiate freely and equally for the right level of privacy. Yet, the conditions of choice play a critical role in shaping outcomes. Individuals' abilities to engage in autonomous decision-making through marketplace negotiations can be diminished by the actual choices that the privacy marketplace offers.[438] Second, reliance

434. For a criticism of the pure market model for privacy, see Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* NTIA REPORT, *supra* note 7, at 3-4.

435. For more on this perspective on the market, see Arthur Alan Leff, *Economic Analysis of Law: Some Realism About Nominalism*, 60 VA. L. REV. 451, 468-70 (1974).

436. *See supra* text accompanying notes 199-205.

437. *See supra* Part II.C.

438. *See supra* text accompanying notes 321-29.

on the data seclusion paradigm considers negotiations that block access to personal information as likely to benefit society as a whole. Yet, this use of the marketplace seeks an outcome that applies to an unusual exception rather than a useful central goal for information privacy.[439]

Two further reasons exist for caution regarding a pure market approach under present conditions. These are: (1) the "knowledge gap," which refers to the widespread ignorance regarding the terms that regulate disclosure or nondisclosure of personal information, and (2) the "consent fallacy," which points to weaknesses in the nature of agreement to data use. Both support a conclusion that reliance on a privacy market will not generate appropriate rules regarding personal data use in cyberspace.

To begin with the "knowledge gap," individuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed. This widespread individual ignorance hinders development through the privacy marketplace of appropriate norms about personal data use. The result of this asymmetrical knowledge will be one-sided bargains that benefit data processors.[440] As James Glave, a reporter for *wired.com*, has written, "the vast majority of the Internet-viewing public still has no idea how to judiciously use their personal information, or even why they should."[441] The lack of knowledge of processing practices is, moreover, a systematic consequence of the social and institutional structure of personal data use.

This lack of knowledge rests on two factors. First, at a time when more Americans from all backgrounds are going online, the extent of privacy in cyberspace largely depends on an opaque technical infrastructure.[442] A result of this ignorance is that individuals

---

439. *See supra* text accompanying notes 329-34.

440. *See generally* COOTER & ULEN, *supra* note 372, at 41 (discussing severe information asymmetries as a standard cause of market failure).

441. James Glave, *Wired News Privacy Report Card,* (visited Dec. 22, 1998) <http://www.wired.com/news/print_version/politics/story/16963.html?wnpg=all>.

442. In the context of cyberspace, much of digital reality is constructed through the setting of technical norms; it is this "code," to use a term of Lawrence Lessig's, that creates cyberspace. Lessig, *supra* note 64, at 896. Yet, most individuals' ability to exercise any rights, whether provided through positive law or otherwise, has been overwhelmed by the complexities of this "code." Understanding the meaning of "code" for one's privacy interests involves grasping the implications of such elements of technical infrastructure as "cookies" and the consequences of such seemingly trivial behavior as surrendering one's e-mail address for online sweepstakes. *See supra* Part I.A.2.

are handicapped in negotiating for their privacy interests. Second, the online industry, the entity with superior knowledge, generally has incentives to provide suboptimal information to guide individual decisionmaking about personal data use.[443] Silence works in the favor of the parties who construct "code" and utilize it in their business endeavors.[444] The resulting societal ignorance of the terms of data processing contributes to the failure of the privacy market.

Beyond the "knowledge gap," a final reason exists for caution about use of a market to establish privacy standards. I term this critique, the "consent fallacy." A standard requirement for valid consent is that it be both informed and voluntary.[445] We have already seen that individuals are likely to lack knowledge of the technological context of data use and that parties with the necessary knowledge may be unwilling to disgorge all relevant data. As a result, one cannot as a general matter characterize consent to data processing as "informed."[446] The "voluntary" nature of consent is also doubtful. Even when consent to an exchange of personal data is carried out in a formal manner, its voluntariness is often suspect.

Personal data use in cyberspace increasingly is structured around an empty process of consent that takes both formal and informal variants. As noted earlier, some Web sites currently present screens with a consent form that must be clicked on as a condition for

---

443. Philip Agre and Joel Reidenberg have identified two related aspects of this incentive structure. Agre notes that the relationship between data processing organizations and individuals is generally based on asymmetric knowledge. Philip R. Agre, *Introduction*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 1, 11 (Philip E. Agre & Marc Rotenberg eds., 1997). As a result, "the organization [has] the greater power to control what information about itself is released while simultaneously obscuring the nature and scope of the information it has obtained about individuals." *Id.*

Joel R. Reidenberg has pointed to the payoff that organizations obtain when they create smokescreens about their data processing practices. Reidenberg, *supra* note 160, at 533. He has observed that companies largely 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. *See id.*; *see also* H. JEFF SMITH, MANAGING PRIVACY 51-54 (1994) (describing refusal of corporations to participate in Harvard Business School research on their information policies and practices in Real Space despite researcher's offer to sign nondisclosure agreements).

444. For a discussion on "code," see Lessig, *supra* note 64, at 894-96.

445. For a discussion of informed consent in the health care setting, see Joseph Goldstein, *For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent and the Plea Bargain*, 84 YALE L.J. 683, 690-94 (1975); Peter H. Schuck, *Rethinking Informed Consent*, 103 YALE L.J. 899, 902-04 (1994).

446. The consent is not "informed" due to the lack of disclosure about planned data use that most Americans would view as "material" to their decision to agree to the processing. *See* Schwartz, *supra* note 229, at 311.

entering the site.[447] Beyond this seeking of formal consent, other Web sites, such as that of the *New York Post*, contain consent boilerplate in their privacy statements that seek to create the legal fiction of informal agreement to data processing practices for all that visit the site.[448] In either manner of "consent," formal or informal, agreement to data processing in cyberspace is likely to turn into a hollow ritual. Individuals may not bother to read a given "informed consent" screen or know where to look for a "privacy statement" before they click through or "surf" deeper into a Web site.[449] In addition, the language on a consent screen or "privacy statement" may approve any and all use of an individual's personal information.[450] Self-reliant consent cannot fulfill its assigned role if individuals are guided into making uninformed, nonvoluntary exchanges.[451]

This analysis suggests that current conditions are not favorable for the marketplace to generate the fair information practices that this Article has advocated. Nevertheless, once these fair information practices are in place, the market has a potentially important role. In particular, different kinds of Trusted Third Parties can help individuals negotiate around privacy default standards. As I have noted, Trusted Third Parties are already emerging.[452] In particular, the "infomediary" seeks to act on behalf of individuals in creating a

---

447. *See supra* text accompanying note 321.

Outside of cyberspace, a similar example of empty formalization of consent concerns disclosures of personal health care information. The current approach requires physicians and hospitals to obtain consent in writing from consumers of health care before the collection, storage, and processing of their personal medical information. *See* Schwartz, *supra* note 229, at 311 (describing "blanket" medical data disclosure releases).

Yet, by any standard, such consent to data processing cannot be said to fulfill this task. In the health care setting, patients generally are offered: (1) an incomplete disclosure statement that creates no meaningful knowledge, and (2) a requirement that these forms be signed before treatment takes place. *Id.* at 312. This use of blanket disclosure structures a process of uninformed consent that can approach outright duress and, hence, an unconscionable agreement. *Id.* The duress exists because in the absence of consent, medical treatment will not be allowed. *Id.* Individuals are consenting to use of their health care information without an adequate process in place to inform their decisions and without having freedom *not* to consent. *Id.*

448. N.Y. POST (visited Apr. 5, 1999) <http://www.nypost.com>.

449. *See* Glave, *supra* note 441, at 2 ("A privacy-practices statement is meaningless unless consumers know to look for it.").

450. *See supra* text accompanying note 323-26.

451. *See* Cohen, *supra* note 321, at 553 (arguing that individuals may miscalculate how to act on their preferences); Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111, 129-30 (1999) (criticizing "shrinkwrap" licensing terms that give copyright owners excessive rights).

452. *See supra* Part II.B.

new "information supply chain."[453] Individuals are first to express their privacy preferences, including the personal data that they wish to reveal to the Trusted Third Party. These entities then locate firms that agree to accept this information and gather no more.[454]

Taken by themselves, however, infomediaries are unlikely to turn fair information practices into cyberspace's predominant norms. Infomediaries negotiating around a default of *maximum* disclosure of personal information will be incapable of shifting the customs of the Web through their practices. This transformation will be hindered by consumer ignorance and the lack of market incentives to make the majority of firms oppose their self-interest, which lies in maintaining the status quo.[455] The next Section will explore in more detail why the industry collectively benefits if it can resist changes in current privacy norms, including that of maximum information disclosure.[456] The result of this likely market equilibrium will be one-sided bargains for consumers and the marginalization of infomediaries.[457]

This analysis suggests, however, that infomediaries will have great potential in helping individuals negotiate around a default of

---

453. Hagel & Rayport, *supra* note 431, at 60.

454. *Id.* at 60-61; *see also* JOHN HAGEL, III & MARC SINGER, NET WORTH: SHAPING MARKETS WHEN CUSTOMERS MAKE THE RULES 109-31 (1999).

Infomediaries make this customization of privacy possible by developing new data management software. For example, the CEO of Lumeria promises to hand millions of consumers a "superWallet" with a "superPassword" that will let them control and update personal information "including which marketers get to what parts of it, how much these firms are allowed to see, or if they can see it at all." James Glave, *The Dawn of the Infomediary* (visited Feb. 24, 1999) <http://www.wired.com/news/print_version/business/story/18094.html/-wnpg=all>.

455. One infomediary, Firefly, recognized the possibility that its business as infomediary might turn out to be the "killer application" of which all companies dream in the Information Age. *See Firefly* (visited Apr. 2, 1999) <http://www.firefly.com/>. Beyond working with consumers as an intermediary, Firefly hedged its bets by also selling its powerful data management software directly to businesses. Its promise is that its data management software will permit businesses "to create, manage, and extend personal profiles . . . for each customer throughout online or networked applications." *Firefly* (visited Mar. 10, 1999) <http://www-firefly.com/-company/keyproducts.fly/>. These products were not sold, however, with effective limits on how Firefly's business customers will utilize the personal information that they harvest. As this example indicates, the products of infomediaries are capable not only of protecting privacy, but also violating it.

456. *See infra* Part III.C.2.

457. As an example of the marginal role of the infomediary at present, no more than a few hundred people visited Firefly on any given day. *See Firefly* (visited Apr. 9, 1999) <http://www-firefly.com/People.fly> (152 people online at Firefly). This lack of popularity con-tributed to Microsoft's ultimate decision to close Firefly.com. In contrast, AOL has 19 million subscribers. *See supra* text accompanying note 111. Or, to give another example, Salon.com, an online magazine, has 1.2 million members. *Salon Magazine Buys a Virtual Community*, N.Y. TIMES, Apr. 9, 1999, at C6.

*minimum* disclosure. Once this default norm is established, industry will have a strong incentive to offer more in exchange for personal data and have more interest in doing business with infomediaries.[458] In other words, infomediaries can help in the development of "privacy price discrimination."[459] This term indicates a differentiation by data processing companies among individuals with varying preferences about the use of their personal data.[460] A default norm of minimum data disclosure will thereby end a personal information subsidy to information processing companies.[461] The next Section will explore the idea of the information subsidy at greater length; here, the emphasis is only how ending this assistance to industry will cause a net social gain by allowing individuals to personalize their privacy levels around standards that promote democratic self-rule.

### 2. Industry Knows Best: Self-Regulatory Mechanisms

While self-regulation remains the favored policy alternative for privacy on the Internet, it is as improbable a candidate for success as the privacy market. Nevertheless, Vice President Gore, the Commerce Department, and the United States Government Working Group on Electronic Commerce all strongly endorse privacy protection

---

458. *See* Reidenberg, *supra* note 68, at 588 ("Policymakers must emphasize the creation of an incentive structure both that encourages new developers to design technologies with information flow flexibility and that offers incentives for the implementation of technologically mediated information policy rules.") (footnote omitted).

459. The standard definition of price discrimination is that under it a seller sets "different prices to different purchasers depending not on the costs of selling to them, but on the elasticity of their demand for his product." POSNER, *supra* note 416, at 281.

460. My development of a concept of "privacy price discrimination" has a close analogy in the law of intellectual property. In the context of computer software, in particular, the law has been highly attentive to price discrimination and the kinds of behavior that should be permitted among buyers and sellers of information goods. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449-50 (7th Cir. 1996) (describing price discrimination in sale of software); William M. Landes & Richard Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 328 (1989) (describing types of intellectual property where price discrimination may be possible); Robert Merges, *Comment: Of Property Rules, Coase, and Intellectual Property*, 94 COLUM. L. REV. 2655, 2666-67 (1994).

461. The danger of a subsidy from a traditional economic perspective is that it might lead to a wasting of resources, that is, companies will not use a good efficiently that they receive for less than market cost. *Cf.* Richard A. Epstein, *The Legal Regulation of Genetic Discrimination: Old Responses to New Technology*, 74 B.U. L. REV. 1, 17-18 (1994) (describing the cross-subsidization that results from the prohibition against genetic discrimination). This Article's critique of the information subsidy created by open disclosure is, however, different than the one that a traditional law-and-economics conception might offer. This Article proposes that a poor standard for privacy on the Internet will cause harm both to democracy and individual self-definition. *See supra* Parts II.A.-B.

through industry self-regulation.[462] The online industry has found this emphasis welcome, and in turn is emphasizing its sensitivity to information privacy issues. In the words of the Online Privacy Alliance, a lobbying organization representing a wide range of corporations and associations, "[t]he Online Privacy Alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce."[463]

This Article's analysis of privacy self-regulation begins by putting itself into the larger perspective of standard-setting. Apart from a sometimes significant governmental role in developing standards, companies engage in standard-setting through either competition or cooperation.[464] During a standards competition, companies promote dueling products in an effort to control the future technological standard.[465] An example of such a standards war is the losing battle that Sony fought in the late 1970s and the early 1980s to make the Betamax the leading format for video cassettes.[466]

In contrast, cooperative standard-setting involves negotiations between different enterprises to reach an agreement on one set of issues so these entities can concentrate on competition in other areas.[467] As two economists observe of such collaborative standard-setting, the "process should be thought of as forging an agreement on the rules of play—the size of the playing field, the type of ball used, and so on."[468] One example of a standards collaboration is the negotiation between Philips Electronics and Sony that led to the still accepted format for CDs.[469] A second example of such collaboration about standards is the current effort by Johnson & Johnson, Eastman Kodak, and Proctor & Gamble to develop uniform security-alarm

462. *See supra* text accompanying notes 199-205.

463. Online Privacy Alliance, *Mission* (visited Sept. 7, 1999) <http://www.privacyalliance.-com/mission/>.

464. MERGES, *supra* note 62, at 846-47; SHAPIRO & VARIAN, supra note 61, at 261-96; Joseph Farrell, *Standardization and Intellectual Property*, 30 JURIMETRICS J. 35, 41-42 (1989).

465. MERGES, *supra* note 62, at 847; SHAPIRO & VARIAN, *supra* note 61, at 278.

466. SHAPIRO & VARIAN, *supra* note 61, at 17. A more recent standards war concerned digital video disks and saw DVD triumph entirely over Divx, which was pulled from the market by its sole promoter on June 16, 1999. Steven V. Brull, *DVD and Conquer: Why One Technology Prevailed*, BUS. WK., July 5, 1999, at 34.

467. MERGES, *supra* note 62, at 847-48 (noting possibility of "joint development of industry standards by a number of firms").

468. SHAPIRO & VARIAN, *supra* note 61, at 306.

469. *Id.* at 261-62.

tags.[470] This trio has formed a consumer products manufacturers' consortium to set out a standardized shoplifting-alarm packaging system for products sold in grocery and drug stores.[471]

Thus, industry self-regulation about privacy is a negotiation about "the rules of play" for the use of personal data. In coming to agreement about these rules, however, companies are likely to be most concerned with one question: what revenues are at stake in the negotiation about standards?[472] The development of standardized formats for CDs increased revenues for hardware manufacturers and software providers by helping convince consumers that these new formats would become widely accepted. As a result, people were more willing to bear the switching costs associated with their adoption of these products.[473] In the case of the consumer products manufacturers' consortium, a standardized anti-theft system will benefit these companies uniformly by reducing losses from shoplifting and the obstruction of brand names on packages by retailers utilizing security tags in an ad hoc fashion.[474]

Revenues are also at stake in privacy standard-setting. These revenues are tied to the collection, analysis, and sale of the enormous amounts of personal data that individuals generate once online. For the current online industry, moreover, personal information largely has the quality of nonrivalrous consumption, which means that one firm's utilization of it does not leave less for any other company.[475] As a result, almost all major Internet enterprises and computer companies benefit from developing standards, including new technology,

---

470. *See* Tara Parker-Pope, *Consortium to Develop Security Tags for Items Sold in Groceries, Drug Stores*, WALL ST. J., Mar. 19, 1999, at B3.

471. *See id.*

472. SHAPIRO & VARIAN, *supra* note 61, at 293.

To point to this concern about revenue streams in an early and epochal collaborative standards negotiation, IBM had "sought out Gates in 1980 to develop an operating system for the IBM PC...." JAMES WALLACE, OVERDRIVE: BILL GATES AND THE RACE TO CONTROL CYBERSPACE 20-22 (1997). Gates did a better job than IBM, however, in understanding the nature of the revenues that were at stake. He licensed his operating system to IBM for a low, one-time fee that permitted use of the Microsoft operating system on as many personal computers as IBM sold while refusing to sell his software to IBM or to give it an exclusive license to his product. *See id.* at 20-22. As an entire industry grew around IBM's non-proprietary personal computer, Microsoft was able to reap the revenues associated with its control of the dominant operating platform for these devices. *See id.*

473. SHAPIRO & VARIAN, *supra* note 61, at 262.

474. *See* Parker-Pope, *supra* note 470, at B3.

475. *See* COOTER & ULEN, *supra* note 372, at 40 (noting that "consumption of a public good by one person does not leave any less for any other consumer").

that preserve the current status quo of maximum information disclosure.

In this view, unlike the commons of England, personal information cannot be overused and should not bear legal limits that restrict the ability of companies to collect and transfer it as they see fit.[476] Scott McNealy, chairman and chief executive of Sun Microsystems, summed up this aspiration in his blunt statement, "You have zero privacy anyway . . . get over it."[477] This is advocacy masked as description; its purpose, like that of the self-regulation movement, is to promote the financial interest of online business as it is currently configured. Yet, the way in which industry "consumes" personal data has considerable spillover.[478] In particular, promotion of the values of democratic deliberation and individual self-determination require limits on outside access to personal information to stop harms to democratic self-rule and individual self-determination.

The difficulty with self-regulation then is that within the present incentive structure, online industry will use collective action to lock in a poor level of privacy at a societal level. Part of this action by these entities takes the classic form of their lobbying government. Proof that online companies generally share interests regarding privacy came when nine leading Internet firms founded a Washington lobbying group.[479] The lobbying organization promised not to take positions on "issues that divide" the founding companies, "such as the current fight . . . over access to high-speed cable lines."[480] No such division was present, however, concerning information privacy.[481] Online industry also seeks to lock in a poor level of privacy through collaborative standard setting.

At present, industry action takes this route in proposals that center on two areas: (1) industry-wide privacy codes of conduct for

476. On the notion of the overuse of public goods, the so-called "tragedy of the commons," see Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1390 (1993); *see generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968).

477. Polly Sprenger, *Sun on Privacy: 'Get Over It,'* (visisted Jan. 26, 1999) <www.wired-com/news/print_version/politics/story/17538.html?wnpg=all>.

478. Spillover or "external" costs cause the individual's self-interest to diverge from social interests. *See* COOTER & ULEN, *supra* note 372, at 188. For a discussion of spillover costs in a transnational context, see Goldsmith, *supra* note 68, at 1210-12.

479. *Top Internet Firms, With Eye on Policy, Form Lobbying Group*, WALL ST. J., July 12, 1999, at 20.

480. *Id.*

481. The Wall Street Journal termed this one of the "top issues" for this new lobby-ing entity. *Id.*

Web sites, and (2) technology that allows individuals to express their privacy preferences in their browser. In both areas, industry plans fall far short of the fair information practices advocated in this Article. To begin with the creation of codes of conduct, industry action has generally focused on only two of the four fair information practices. The two practices that industry has largely ignored are the need for an effective fabric of obligations, such as data minimalization, and for limited procedural and substantive rights, such as rights of access and correction. As for the fair information practices that industry emphasizes, it has presented incomplete versions of these two standards and has failed to convince Web sites to follow even these weak guidelines.

In place of the full range of fair information practices, industry codes of conduct concentrate on transparent processing systems and the establishment of external oversight. In industry's model of online privacy self-regulation, however, significant problems exist with the initial conception and actual expression of both standards. To begin with transparency, industry views it as fulfilled by incomplete privacy statements.[482] This concept, which is that any kind of notice equals privacy protection, is also capturing the larger policy debate. For example, in July 1999, the FTC released an Internet privacy study carried out on its behalf by Mary Culnan of Georgetown University's McDonough School of Business.[483] The Georgetown Internet Privacy Policy Survey reveals many problems in cyberspace. First, it shows that less than ten percent of surveyed sites provided even a subset of basic fair information practices.[484] Second, the study indicates that a high percentage of Web sites are collecting personal information.[485] Other potential problems were outside the study's scope. To begin

482. In particular, the Online Privacy Alliance has emphasized the value of posting any sort of privacy statement as a means of warding off governmental regulation. It advises Internet companies, "Government officials will be judging how successful self-regulation may be by how many companies have posted privacy policies on their web sites and how many have joined the Alliance and adopted its guidelines." Online Privacy Alliance, *Frequently Asked Questions* (visited Sept. 6, 1999) <http://www.privacyalliance.com/facts/>.

483. FTC, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (July 1999) [hereinafter FTC SELF-REGULATION REPORT] (available at <http://www.ftc.gov/opa/1999/9907/-report-1999.htm/>); GEORGETOWN INTERNET PRIVACY POLICY SURVEY (last modified: May 17, 1999) [hereinafter GEORGETOWN SURVEY].

484. GEORGETOWN SURVEY, *supra* note 483, at 9. The Survey refers to this finding in confusing terms as the percentage of the Web sites that "contained at least one survey element for notice, choice, access, security, and contact information." *Id.*

485. *Id.* at 3 (Appendix A, Table 2a).

with, the study did not examine whether Web sites offered procedural and substantive rights, such as redress or enforcement policies.[486] Moreover, as the Center for Democracy and Technology observed, the survey, like others of its ilk, provides no information about whether companies are actually following the privacy policies that they promised.[487] Finally, the Georgetown Survey does not consider whether Web sites are allowing individuals to limit release of their personal data to affiliated enterprises.[488] This last issue is of particular significance at a time when mergers and consolidations are almost daily events among Internet companies and between Internet and Real Space companies.[489]

Despite the Georgetown Survey's indications of weak privacy for personal information on the Internet and its own shortcomings, the FTC and the media were captivated by one of its findings. This empirical work indicated that 65.7 percent of the sites in the sample posted "at least one kind of privacy disclosure."[490] For many observers, including the Chairman of the FTC, Robert Pitofsky, this single development was solid proof of "real progress."[491] The FTC's Chairman assured Congress that the Georgetown study helped indicate that "self-regulation is working."[492] The FTC itself argued that "self-regulation is the least intrusive and most efficient means to ensure fair information practices online."[493] In contrast, FTC Commissioner Sheila Anthony stated that "[n]otice, while an essential

---

486. *Id.* at 8.

487. *See* Center for Democracy and Tech., *Behind the Numbers: Privacy Problems on the Web* (visited July 21, 1999) <http:www.cdt.org/privacy>.

488. *See* GEORGETOWN SURVEY, *supra* note 483,. at 11.

489. *See, e.g.*, Ted Kemp, *Behind the DoubleClick Merger: Buying behavior is Abacus' key asset*, 21 DMNEWS 1 (1999) (analyzing purchase by leading marketer of online advertisements of "a company that runs the biggest database of consumer catalog buying behvaior in the U.S.").

490. GEORGETOWN SURVEY, *supra* note 483, at 7; FTC SELF-REGULATION REPORT, *supra* note 483, at 7. For media reports, see Jeri Clausing, *Gain for On-Line Industry on Privacy Issue*, N.Y. TIMES, July 13, 1999, at A10; Jeri Clausing, *Gains Seen in Consumer Privacy on Internet*, N.Y. TIMES, May 13, 1999, at A20; Grant Lukenbill, *Privacy Laws Inappropriate at This Time, FTC Tells Congress*, 21 DMNEWS, July 19, 1999, at 1.

491. As a FTC Press Release quoted Pitofsky: "We continue to believe that effective self-regulation is the best way to protect consumer privacy on the Internet, and I am pleased that there has been real progress on the part of the online industry." FTC, *"Self-Regulation and Privacy Online," FTC Report to Congress* (visited July 13, 1999) <http://www.ftc.gov/opa/1999/-9907/report1999.htm> [hereinafter FTC Press Release]. A similar conclusion is found in the FTC's report to Congress. *See* FTC SELF-REGULATION REPORT, *supra* note 483, at 8.

492. FTC Press Release, *supra* note 491, at 1.

493. FTC SELF-REGULATION REPORT, *supra* note 483, at 6.

first step, is not enough if the privacy practices themselves are toothless."[494] At present, her judgment is decidedly in the minority.

AOL, the ISP for nineteen million Americans, offers a more specific, negative example in regard to notice. At different times, AOL has utilized smokescreen tactics to make it difficult to obtain information about its privacy practices, including its plans to modify how it uses personal data.[495] For example, while AOL provides notice of its *Web site's* privacy policy through the kind of hypertext link that this Article has described, it requires that one sign up for its ISP service before providing information regarding its privacy practices as *service provider*.[496] This practice seeks to promote lock-in by placing the burden of "switching costs" on the consumer who has initially chosen AOL as her ISP.[497] In addition, those who continue to interact with a Web site or utilize an ISP are generally considered to have granted consent to the posted policies.[498] As a result, a thin caricature of transparency is emerging as a cornerstone of industry's preferred mode of self-regulation.

The oversight that industry is proposing is also incomplete and likely to be ineffective.[499] The private sector has been resolute in opposing proposals for a governmental data protection agency. Instead, online industry is promoting nongovernmental "seal services"

---

494. *Prepared Statement of the Federal Trade Commission on "Self-Regulation and Privacy Online" Before the Subcommittee on Telecommunications, Trade, and Consumer Protection on the Committee on Commerce, U.S. House of Representatives* (visited July 13, 1999) <http://www.ftc.gov/os/1999/9907/pt071399anthony.htm> (statement of Comm'n Sheila F. Anthony) (concurring in part and dissenting in part).

495. *See* Schiesel, *supra* note 129, at D4 (noting that before AOL changed plans to sell telephone numbers, it had tucked its "only notice of the proposed policy shift in an obscure corner of the service").

496. *American Online, Inc.* (visited Sept. 6, 1999) <http://www.aol.com/info/privacy.html> ("The AOL Internet online service has a separate privacy policy for its members. If you are an AOL member, you can find that policy within our Terms of Service.").

497. On the critical nature of "switching costs" in the information economy, see SHAPIRO & VARIAN, *supra* note 61, at 11-13.

498. *See supra* Part III.C.1.

499. Moreover, this entire process travels down a path already taken. In Real Space, a strong negative example exists of a group of enterprises using the claim of self-regulation to construct a smokescreen of ineffective measures that obscures its true practices. The direct marketing industry has ardently promoted self-regulation. Its trade group, the Direct Market Association ("DMA"), has pointed to an industry code of conduct and a Privacy Task Force as the prime fruits of this self-regulatory effort. *See* SCHWARTZ & REIDENBERG, *supra* note 48, at 308-09. It has devoted less publicity to poor industry compliance with this code, including violations of its regulations by at least one enterprise that belonged to the Privacy Task Force. *Id.* The DMA is now playing an aggressive role in promoting self-regulation in cyberspace. *See* DMA, *The DMA's Privacy Promise* (visited Sept. 6, 1999) <http://www.thedma.org/pan7/main.shtml>.

that create "trusted privacy marks" to be placed on the Web sites that make use of them. These kinds of Trusted Third Parties differ from infomediaries; where the latter companies seek to stimulate development of a privacy market through development of direct relations with individual consumers, privacy seal companies offer a general branding trademark combined with audit services for companies.[500] A Web site's posting of such a privacy logo on its home page indicates that the site has posted a privacy statement and that the designated privacy seal service will audit compliance by monitoring the companies' data-handling practices.[501] The two leading such Trusted Third Parties are Truste and BBBOnLine.[502]

This approach is promising, but its current weaknesses are that the privacy seal companies: (1) certify standards that may fall short of this Article's proposed fair information practice, (2) are limited in their enforcement powers, and (3) have brands that are not widely recognized at present. These three shortcomings, unfortunately, all magnify each other. As the Center for Democracy & Technology has commented, "at the current time, the quality of privacy practices required of seal holders . . . varies substantially."[503] Should these companies find a violation of a posted privacy practice, their most effective action is forbidding a site from utilizing their respective privacy seal, which individuals will hardly miss.[504] The limited evidence available also suggests that these monitoring organizations have been far from aggressive in carrying out their duties. Most privacy violations involving Web sites are brought to public attention by the media and are not followed by a privacy-branding company's decisive enforcement action or revocation of a privacy seal.[505]

---

500. For a good introduction to the leading privacy seal service, see TRUSTE, *Frequently Asked Questions* (visited Sept. 6, 1999) <http://www.truste.org/webpublishers/pub_faqs.html>.

501. *See id.* at 2.

502. BBBOnline began offering its services later than TRUSTE. For information on it, see BBBOnline, *The BBBOnline Privacy Program* (visited Sept. 6, 1999) <http://www.bbbonline.-com/businesses/privacy/index.html>.

For criticism of BBBOnline for initial problems with bugs in its application and registration process, see Chris Oakes, *Better Business Bureau Offline?* (Apr. 5, 1999) <http://www.wired-com/news/print_version/business/story/18940.html>.

503. Center for Democracy & Tech., *supra* note 487, at 12.

504. Both companies, Truste and BBBOnLine, have emphasized their willingness to bring the activities of companies that violate their agreements with them to the FTC's attention. On the limits of the FTC's powers, see *supra* text accompanying notes 193-98.

505. For a recent incident following this pattern that involves Microsoft, one of the premier sponsors of Truste, see Jeri Clausing, *Privacy Watchdog Declines to Pursue Microsoft, a Backer*, N.Y. TIMES ON THE WEB 1 (visited Mar. 22, 1999) <http://nytimes.com/library/tech/99/03/-

Thus, significant shortcomings exist in the first element of industry self-regulation, which is the development of codes of conduct. The second element of industry self-regulation is a technological solution that seeks to allow each person to express the kind of fair information practices that she wishes. Here, the standard-setting process involves not only private corporations but also the World Wide Web Consortium ("W3C"), a nonprofit institution involved in Internet self-governance.[506] The W3C is developing a Platform for Privacy Preferences ("P3P"), which is a software protocol for allowing an individual to check whether a Web site's privacy practices match her wishes.[507] P3P is to be a platform that allows "individuals, markets, and regulatory frameworks" to "ultimately determine the [privacy] balance."[508] This technological solution follows a path similar to that of the "V-Chip," a filtering device that Congress has mandated that manufacturers build into television sets.[509] The V-Chip will allow parents to restrict the kinds of programs to which their children will be exposed.[510]

P3P has great potential to assist in the customization of individual wishes for information privacy. The difficulty, as already noted in the context of infomediaries, is that a lock-in of a poor level of privacy is likely to occur around a norm of maximum information disclosure. By itself, P3P will not cause change in the existing norm of maximum disclosure. Rather, Web sites will be able to use P3P to

---

cyber/articles/23privacy.html>; *Microsoft Off Truste's Hook*, WIRED.COM 1 (Mar. 22, 1999) <http://www.wired.com/news/print_version/chnology/story/18639.html?wnpg=all>.

506. *See* W3C, *Platform for Privacy Preferences (P3) Project* (visited Sept. 4, 1999) <http://-www.w3.org/P3/Update.html>.

507. *See id.*

508. *W3C, P3P and Privacy on the Web FAQ* (visited Mar. 15, 1999) <http://www.w3.org/-P3P/P3FAQ.html>; *see* Joseph Reagle & Lorrie Faith Cranor, *P3P in a Nutshell* (visited Sept. 4, 1999) <http://www.w3.org/P3P/nutshell.html>.

509. 47 U.S.C. § 330(x) (1994).

510. Such filtering technologies require a reduction of a universe of possible preferences to simple standards. *See* J.M. Balkin, *Media Filters, The V-Chip, and the Foundations of Broadcast Regulation*, 45 DUKE L.J. 1131, 1143 (1996). In the case of the V-Chip, for example, the FCC has approved a regulatery scheme in which television programs will be rated as belonging to one of seven categories, ranging from TV-Y (suitable for all Children) to TV-MA (designed to be viewed by adults and, therefore, perhaps unsuitable for children under 17). *See* F.C.C., Implementation of Section 551 of the Telecommunications Act of 1996: Video Programming Ratings, CS Docket No. 97-55, FCC 98-35, (Mar. 13, 1998).

P3P is seeking to develop a similar kind of privacy language; here, one proposal is for six pre-configured preference files ranging from "Access all Web sites" to "I want to be close to anonymous." Joseph Reagle, *P3 Prototype Script* (visited Sept. 4, 1999) <http://www.-w3.org/Talks/970612-ftc/ftc-mast.html>. Within these six files, more detailed choices will be preset, and an individual will have the possibility to fine-tune these values. *See id.*

close themselves off to individuals who seek the fair information practices that I have proposed. In other words, those who view the Internet through the filter of privacy-enforcing software may end up placing most of the Web off-limits to themselves. Their Hobson's choice will be sacrificing either their privacy or their access to the Internet.

This analysis indicates that the timing of strategic moves is critical for development of privacy norms. Technology can play an important role in constituting a multidimensional privacy territory on the Internet.[511] As Joel Reidenberg has argued, technological norms form part of the new Lex Informatica. Yet, the contribution of P3P technology will be most effective if made at the time when the data topography of cyberspace is first being established.[512] It is particularly troubling, therefore, that P3P's development has not only been slow, but also is stalled at present by a dispute about legal rights to the essential underlying intellectual property.[513] Even if P3P is finally made available, cyberspace privacy may have been permanently defined down by that time.

### 3. The Law's Domain

Both the market and self-regulation have important roles to play in privacy protection on the Internet. Yet, reliance on these forces alone will not create effective privacy standards for cyberspace.

---

511. *See* Reidenberg, *supra* note 68, at 586-87.

512. *See* SHAPIRO & VARIAN, *supra* note 61, at 15 (noting that lock-in can occur on a societal level).

513. The patent owner for a filtering technology similar to that of P3P, Intermind, is demanding "a minimum royalty of US $50,000 per year to a maximum of $2.5 million from companies implementing P3P." Chris Oakes, *Patent May Threaten E-Privacy*, (visited Nov. 11, 1998) <http://www.wired.com/news/print_version/technology/story/16180.html?wnp=-all>.

A report in the trade press recently quoted one anonymous member of the P3P working group as saying that this controversy surrounding Intermind's patent "has stopped P3P dead in its tracks." Connie Guglielmo, *Will Patent Pose Privacy Problem?*, INTER@CTIVE WK., Feb. 1, 1999, at 36. It is unsurprising, therefore, that the latest Internet browser to be released, Microsoft Internet Explorer 5.0, lacks P3P. *See id.*

Some slight positive movement regarding P3P has occurred, however, with the release by Microsoft of the "Privacy Wizard." Chris Oakes, *Click Here for a Privacy Policy*, (Apr. 10, 1999) <http://www.wired.com/news/print_version/technology/story/16180.html?wnpg=-all>. This software program allows sites te disclose their privacy policies and to have these privacy statements become part of a P3P infrastructure. *See id.* The modesty of this develop-ment is due to the lack of a complete P3P infrastructure; as *wired.com* explains, "the cart is leading the horse." *Id.* at 2. For a more enthusiastic reaction to P3P, however, and one that ignores almost all these issues, see *Developments in the Law: The Law of Cyberspace*, 112 HARV. L. REV. 1647 (1999).

The four fair information practices that this Article has developed should be expressed in federal legislation. Enactment of this law would be an ideal follow-up to congressional enactment in 1998 of the Children's Online Privacy Act.[514] This legislative imposition of fair information practices for cyberspace will lead to three significant benefits: (1) the prevention of a lock-in of poor privacy standards, (2) the creation of the preconditions for effective market and self-regulatory contributions to privacy protection, and (3) the ending of United States intransigence on the wrong side of ongoing negotiations with the European Union about trans-Atlantic transfers of personal data.

The timing of strategic moves in the Information Age is critical, and the likely result of delay in the expression of privacy standards will be to lock in the current privacy horror show in cyberspace. If we wait, American society may follow the path indicated by Scott McNealy and "get over" its loss of privacy on the Internet.[515] This path would be more than unfortunate because privacy rules are a critical means of constituting both individuals and community.[516] The promotion of cyberspace as a new arena for civic life and the maintenance of a populace capable of self-determination requires the right kind of restrictions on different kinds of access to personal information. The four fair information practices that this Article advocates, if expressed in law, will be the best first step in establishing the necessary data topography of Internet privacy. This legal expression of privacy norms will also promote democratic deliberation and individual self-determination in cyberspace.

A further benefit of a legislative expression of privacy norms, paradoxically, will be to heighten the effectiveness of the market and self-regulatory mechanisms. The Clinton Administration's policies in this area have largely encouraged a consensus in the industry around norms that do not benefit society as a whole. As the industry is currently configured, it benefits from standards that accomplish the following: promote maximum disclosure of personal data; establish a poor level of transparency; offer no effective procedural or substantive rights; and establish hollow oversight. In a similar fashion in the past, the legal system's deference to the direct marketing industry's

514. For a discussion, see *supra* text accompanying notes 206-08.
515. Sprenger, *supra* note 477, at 1.
516. See *infra* Parts II.A-B.

weak code of conduct has permitted it to stave off effective regulation.[517]

A legal expression of fair information practices would create an environmental shock to industry's privacy self-regulatory groups and its current consensus. The legislative enactment of fair information practices would prevent firms from viewing personal data as a public good; instead, companies would be forced to engage in privacy price discrimination.[518] Already, software and other Information Age companies have become highly sophisticated at capturing revenues by customizing their products and services to charge each customer the price that she is willing to pay, and no more.[519] Such price discrimination sometimes takes place by selling to different users at different prices, by letting users choose the version of a product they wish, and by making discounts available to certain groups.[520] Compared to this effort, companies do not generally seek privacy price discrimination because the law, technology, and social practices create an information subsidy in their favor. From this perspective, a legislative enactment of fair information practices would end a socially unproductive subsidy to online industry. In addition, greater industry interest in such Trusted Third Parties as infomediaries and privacy seal organizations would be likely to develop.

Finally, enactment of an online privacy protection law in the United States would help resolve a conflict with the European Union ("EU"). The stakes in this clash are high; at present, the Commission of the EU is threatening to block the flow of personal data to the United States.[521] European nations have spent decades in creating high levels of protection for personal data through legal regulations at the domestic and trans-European level.[522] In an age of international data flows, however, these measures would be doomed to failure if their reach ended at the borders of Europe.[523]

---

517. SCHWARTZ & REIDENBERG, *supra* note 48, at 309-12.

518. For a definition of this concept, see *supra* text accompanying notes 459-60.

519. SHAPIRO & VARIAN, *supra* note 61, at 55-68.

520. *See id.*

521. *See* SWIRE & LITAN, *supra* note 4, at 212; Gary E. Clayton, *Eurocrats Try to Stop Data at the Border*, WALL ST. J., Nov. 2, 1998, at A34 (discussing the ramifications of the European Directive 95/46 that prohibits the exportation of personal information by businesses unless the country that receives the information has adequate privacy protections).

522. *See* FLAHERTY, *supra* note 24, at 21-28, 93-103, 165-72.

523. Schwartz, *supra* note 417, at 483-88.

In response to this increase in extra-territorial activities involving the personal data of their citizens, many European nations have extended their domestic laws to regulate international transmissions of personal data.[524] At the trans-European level, moreover, the Member States of the EU enacted a Data Protection Directive that seeks both to harmonize their national data protection laws at a high level and to restrict transfers of personal data to third-party nations that lack "an adequate level of protection."[525] In cases where such adequate protection is not present, the Directive provides exceptions that permit transfers if, among other circumstances, the individual affected has "unambiguously" consented, or if the party receiving the data has agreed by contract to provide adequate protection.[526]

These national and European-wide measures for information privacy pose significant challenges to the free flow of personal data to the United States.[527] Whether or not the United States generally has "adequate" information privacy is a complex question. An answer to it requires examination of the protections available for a specific data transfer, including the safeguards offered by law and relevant business practices.[528] Nevertheless, the European view regarding United States privacy standards has been appropriately skeptical.[529]

---

524. *See id.*

525. Council Directive 95/46, art. 25, 1995 O.J. (L281) 1, 31 [hereinafter European Directive] (protecting of individuals with regard to the processing of personal data and on the free movement of such data). For a discussion, see SWIRE & LITAN, *supra* note 4, at 22-49; Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 463-66 (1995); Schwartz, *supra* note 417, at 473-88.

526. European Directive, *supra* note 525, at art. 26.

527. As Peter Swire and Robert Litan write,

> The Directive could have far-reaching effects on business practices within the United States and other "third countries" (countries that are not part of the European Union). Mainframes and Web sites in the United States might be cut off from data from Europe. Marketing and management practices that are routine in the United States might be disrupted.

SWIRE & LITAN, *supra* noto 4, at 3.

528. *See* European Directive, *supra* note 525, art. 25(2); *see also* WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, FIRST ORIENTATIONS ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES - POSSIBLE WAYS FORWARD IN ASSESSING ADEQUACY, XV D/5020/97-EN final WP4 1-5 (June 26, 1997).

529. For a report on the EU's views, see, e.g., Thomas Weyr, *US-Europe Privacy Truce Buys Time, But EU May Target Directive Violators Early*, DMNEWS INT'L, Nov. 9, 1998, at 1.

To make matters more complicated, the EU Directive's provisions on data transfers are enforced by the Member States, which makes their current views and future action of critical importance. *See* Schwartz, *supra* note 417, at 488-96; *U.S.-EC Deal on Data Privacy No Guarantee of Peace with Member States, Expert Says*, 67 U.S.L.W. 2367 (Dec. 22, 1998).

In response to EU pressure, Clinton Administration officials followed an initial period of inaction with the U.S. Commerce Department's drafting of weak "safe harbor" standards for privacy.[530] The Commerce Department's plan is to obtain EU agreement to waive sanctions against any American companies that follow these standards.[531] Yet, the "safe harbor" principles largely track the worst aspects of the industry codes of conduct that this Article has already criticized.[532] In addition, to the extent that the Commerce Department is attempting to move the American online industry in the direction of stronger fair information practices for European citizens, it faces opposition from business.[533] The American online industry is fearful of domestic precedential value if it agrees to provide European citizens who visit its Web sites with fair information practices superior to those given to Americans at these same sites.[534] One particular contentious area concerns improving the access to one's personal data that is collected in cyberspace.[535]

The EU's Data Protection Directive is only part of a larger international effort at privacy protection.[536] The United States

---

530. International Trade Admin., Electronic Commerce Task Force, *Safe Harbor Principles* (visited Sept. 4, 1999) <http://www.ita.doc.gov/ecom/menu.htm>.

531. For reports on these negotiations, see Thomas Weyr, *Crunch Time for US-EU Privacy Talks: Progress Made but No Resolution Yet*, DMNEWS INT'L., Dec. 14, 1998, at 1; Weyr, *supra* note 529, at 1; *see also* Edmund L. Andrews, *European Law Aims to Protect Privacy of Data: Some Trade with U.S. Could Be Disrupted*, N.Y. TIMES, Oct. 26, 1998, at A1.

532. The Draft International Safe Harbor Privacy Principles and comments on them are available on the Web site of the Department of Commerce's International Trade Administration, Electronic Commerce Task Force (visited Oct. 26. 1999) <http://www.ita.doc.gov/ecom/shprin.html>.

For a speech in favor of the U.S. approach by the chief American negotiator with the EU, see *Remarks of Ambassader David L. Aaron, Under-Secretary of Commerce for International Trade Before the French and American Business Community, American Chamber of Commerce Conference Center, Paris, France* (visited Jan. 25, 1999) <http://www.ita.doc.gov/media/privacy.htm>.

For criticisms of the safe harbor principles, see *Administration Diplomacy on Data Privacy May Not Satisfy FTC's Policy Expectations*, 67 U.S.L.W. 2331 (Dec. 9, 1998); Nadya E. Aswad, *Privacy Commentators Demand Clarity; Group Asks If Self-Certification Qualifies as Safe Harbor*, 3 Electronic Com. & L. Rep. (BNA) 1337 (Nov. 25, 1998); Robert Gellman, *Commerce Department's Safe Harbor Proposal Sinks at the Dock*, DMNEWS, Dec. 21, 1998, at 15.

533. Robert O'Harrow, Jr., *Companies Resist U.S. Proposals on Privacy*, WASH. POST, Mar. 16, 1999, at E1.

534. *See id.*

535. *See id.* at 2. The chief U.S. negotiator with the EU has been quoted as having reassured industry leaders "that efforts to comply with European rules have nothing to do with the privacy legislative debates in the United States." Id.

536. For example, countries in Latin America that are developing information privacy laws include Argentina, Brazil, and Chile. Alastair Tempest, *The Globalization of Data Privacy*, DMNEWS INT'L, Mar. 15, 1999, at 5. As part of the international effort at improving privacy in

government is not helping in this effort. Rather, it is increasing the problem by its intransigence in favor of industry self-regulation, which is an approach that will not work under current conditions.[537]

## CONCLUSION

This Article has depicted the widespread, silent collection of personal information in cyberspace. At present, it is impossible to know the fate of the personal data that one generates online. This state of affairs is bad for the health of a deliberative democracy. It cloaks in dark uncertainty the transmutation of Internet activity into personal data that will follow one into other areas and discourage civic participation. This situation also has a negative impact on individual self-determination; it makes it difficult to engage in the necessary thinking out loud and deliberation with others upon which choice-making depends. In place of the existing privacy horror show, we need multidimensional rules that set out fair information practices for personal data in cyberspace.

This Article has argued that the necessary practices must embody four requirements: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight. Neither the market nor industry self-regulation is likely, however, to put these four practices in place. In particular, despite the Clinton Administration's favoring of industry self-regulation, this method is an unlikely candidate for success. Industry self-regulation about privacy is a negotiation about "the rules of play" for the use of personal data. In deciding on these rules, industry is likely to be most interested in protecting its stream of revenues. It will therefore benefit if it develops norms that preserve the current status quo of maximum information disclosure.

This Article advocates a legislative enactment of its four fair information practices. This legal expression of privacy norms is the

---

cyberspace, Germany has enacted the Teleservices Data Protection Act of 1997. *See* PRIVACY LAW SOURCEBOOK, *supra* note 396, at 299-300.

537. As an example of the intransigence, Ira Magaziner, in his role as Senior White House Electronic Commerce Adviser, stated regarding the privacy negotiations with the EU, "[w]e won't have [the EU] impose an inefficient, nonworkable system on us." *U.S. Businesses Watchful, Not Worried by Specter of EU Data Protection Directive*, 67 U.S.L.W. 2307 (Dec. 1, 1998).

best first step in promoting democratic deliberation and individual self-determination in cyberspace. It will further the attainment of cyberspace's potential as a new realm for collaboration in political and personal activities. Enactment of such a federal law would be a decisive move to shape technology so it will further—and not harm—democratic self-governance.