Journal of Civil Rights and Economic Development

Volume 11
Issue 3 *Volume 11, Summer 1996, Issue 3*

Article 10

June 1996

Privacy Protection on the Information Superhighway

Barbara S. Wellbery

PRIVACY PROTECTION ON THE INFORMATION SUPERHIGHWAY

BARBARA S. WELLBERY*

The agency that I work for is the National Telecommunications and Information Administration (NTIA) in the Department of Commerce. We serve as the President's principal advisor on telecommunications and information matters and have been actively involved in the "Information Superhighway"[1] and the issues that it raises.

Rather than discussing an issue that creates clear liability in cyberspace[2] today, I will ask you to consider how privacy issues should be addressed in cyberspace.

The Information Superhighway creates serious implications for privacy. The ability to compile, to transmit, and to distribute information rapidly and inexpensively qualitatively changes how personal information can be collected and used.[3] Previously, that

* B.A., S.U.N.Y. Binghamton; J.D., Stanford Law School. Barbara S. Wellbery is the Chief Counsel of the National Telecommunications and Information Administration (NTIA). In this capacity, Ms. Wellbery deals with issues pertaining to the National Information Infrastructure and the Global Information Infrastructure, including telecommunications and information law and policy.

Prior to joining NTIA, Ms. Wellbery was Vice President and Deputy General Counsel of Discovery Communications, Inc., where she was responsible for international joint ventures, as well as regulatory, entertainment, trademark, and copyright aspects of the cable programming business. Before being employed by Discovery, Ms. Wellbery was the Deputy General Counsel and Director of Copyright at the Public Broadcasting Service (PBS), where she handled entertainment, copyright, and communications law matters, as well as general corporate issues.

Ms. Wellbery began her legal career as an associate at Wilmer, Cutler & Pickering.

[1] When the Administration talks about the Information Superhighway, we mean all aspects of telecommunications and information services, including among others, the Internet, cable, broadcast, wireless, and telephone services. *See, e.g.*, George H. Friedman & Robert Gellman, *An Information Superhighway "On Ramp" For Alternative Dispute Resolution*, 68 N.Y. ST. B.J. 38, 39 (June, 1996) (noting that term "Information Superhighway" describes use of computer networks for economic, social, governmental, and other activities).

[2] *See, e.g.*, WILLIAM GIBSON, NEUROMANCER 51 (1984). The term "cyberspace" was made popular by this work.

[3] *See, e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L.J. 195, 197-98 (1992) (stating that gathering and disseminating personal information is possible through sophisticated data collection methods, corporate outsourcing of data processing, and information service providers).

information was stored in file cabinets and compiling consumer profiles took a great deal of time and much expense. Now it is fairly easy and inexpensive.

Software exists that allows the places where you click on the Internet, so-called "mouse droppings," to be tracked and collected.[4] So a stop, for example, at a gay chat room, can be recorded. If you stop at the Democratic National Party's chat room or bulletin board, that can be recorded also. If you add to that the fact that every time you go to a store, your purchases can be scanned into a computer and tracked, you realize that a large amount of very detailed information can be compiled about you. It is not surprising that a recent consumer survey showed that about 84% of Americans were very concerned about their privacy in cyberspace.[5]

A few years ago, NTIA started to reexamine the question of privacy.[6] We distributed a Notice of Inquiry and asked industry and public interest groups to identify potential privacy issues and to suggest the manner in which such issues should be addressed. We surveyed privacy law and discovered that no comprehensive law dealing with privacy exists in the United States.[7] This is unlike the situation in many European countries where privacy laws apply to all industry sectors.

Indeed, in the United States, there is not even one law that deals with privacy in the entire telecommunications and cyberspace area. The laws that do exist are very sector-specific. For example, the Cable Communications Policy Act of 1984 governs

[4] *See, e.g.*, Larry Irving, *Progress Report on the Information Superhighway*, MACWORLD, Mar. 1, 1996, at 260 (stating that "mouse droppings" allow unauthorized online service providers to collect personal data, with some providers selling such information to private industry for marketing purposes).

[5] *Cf., e.g.*, Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1644 (1995) (discussing Harris survey in which 84% of Americans are concerned about privacy and 78% of Americans felt that they lost control over personal information).

[6] NTIA had been very involved in privacy issues in the late 1970s and early 1980s. It led United States efforts to negotiate voluntary privacy guidelines with the Organization for Economic Cooperation and Development and spearheaded their adoption by many American companies.

[7] *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (reasoning that specific rights guaranteed in United States Constitution create zones of privacy); *see also* Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1107-08 (1969) (asserting that privacy relates to control of flow of information about individuals); Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 205 (1890) (arguing that privacy is "right to be let alone").

how cable operators may use subscribers' personal information,[8] the Video Privacy Protection Act of 1988 governs how video rental stores may use the personal information of those renting videos,[9] and the Telecommunications Act of 1996 governs how telephone companies may use subscriber information.[10] The provisions of the 1984 Cable Act are fairly strict and limit the extent to which cable operators can collect and use information that they have about you in ways that are unrelated to the their providing business and service to you.[11]

The scope of these laws, however, is very limited. For example, while the Cable Act obviously applies to video programming provided by cable operators, it does not expressly apply to video carriage by Direct Broadcast Satellite (DBS) or wireless cable operators.[12] If Local Exchange Carriers (LECs) provide video programming on a common carrier basis, it is not clear that any law governs the personal information of their subscribers that they collect. The very limited scope of these laws means that they may not apply to new communications services as they are developed.

In a report entitled "Privacy in the NII: Safeguarding Telecommunications Related Personal Information," NTIA analyzed one kind of personal information, transactional information. This information includes, for example, to whom, from whom, and when a message was sent and, if applicable, the subject of the message. It is the information that appears "above the line" on an E-mail or on the itemized list of long distance calls that consumers receive each month. It is also the kind of information that you can get from "mouse droppings," or from a supermarket scanner.

Transactional information can be very revealing of one's personal habits when compiled and collected from many sources.[13] For example, it is possible to infer a person's political or sexual leanings from the places they visit on the "Web," and to know

[8] The 1984 Cable Act, 47 U.S.C. § 551 (1994).

[9] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994).

[10] Telecommunications Act, Pub. L. No. 104-104, 110 Stat. 56, 148-49 (1996) (governing use of personal information by telecommunications carriers and limiting use of information without customer approval).

[11] 47 U.S.C. § 551(c).

[12] *See* Definition of a Cable Television System, 5 F.C.C. Rcd. 7638, 7638 (1990).

[13] *See, e.g.*, David Charbuck, *Computer's New Frontier*, FORBES, Nov. 26, 1990, at 257, 260 (detailing how airlines gather ticket receipts and maintain information on laser disks for future image processing).

when they are home and/or awake, and to discover who their friends and relatives are from the transactional information on a long distance bill. What foods people eat and what books they read can be gleaned from looking at records compiled from supermarket scanners.

In surveying privacy law, we discovered that there are minimal consumer protections. As a result, we proposed a self-regulatory framework that would apply to telecommunications companies and to on-line service providers and would require notice to consumers and an opportunity for them to consent before information was used in ways other than to provide service.[14] Because expanding privacy protections will expand consumer demand for facilities and services in cyberspace, and these benefits can be produced with minimal costs to business, NTIA expects that the private sector will have strong incentives to implement privacy practices voluntarily. Indeed, there are many companies that provide notice and an opportunity to consent already, such as Prodigy and America Online.

NTIA is meeting with companies throughout industry to determine whether they have policies in place, how they enforce those policies, what kind of monitoring of company practices exists, and whether dispute resolution exists and if so how it works.

Adoption of a European Union Directive by the European Union in October 1995, provides a great deal of urgency to the issue of privacy protection in the United States.[15] The directive must be implemented by member states by October 1998. It gives each of the countries in the European Union the ability to halt trans-border data flows to non-member states, such as the United States, if they determine that the United States does not provide adequate data protection. Thus, an American company that does business in Europe and sends the information back to the United States to be processed, which, in fact, is the process of a number of bank card companies, might not be able to continue that process if the

[14] *Cf., e.g.*, Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 1019-20 (1996) (advocating more protection in collection and disclosure practices rather than regulating devices and practices that will change with technology).

[15] *See* Reidenberg, *supra* note 3, at 199 (noting that number of foreign governments have prohibited transmission of personal information to countries seen as lacking adequate privacy protections). *See generally* ADRIANA C.M. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC (1990).

European Union member states were to decide that its privacy protections were not adequate.

NTIA and the State Department are meeting with the European Union to begin a dialogue with them and to educate them about American privacy protections. The fact that we do not have an omnibus privacy law does not mean that there are no privacy protections. As noted above, many companies and trade associations have privacy policies. We are working to avoid a situation in which the European Union decides that United States privacy laws are not adequate. We will continue to meet with European Union officials to continue this dialogue and this education about American privacy law.