1995

The EU Data Protection Directive, Information Privacy, and the Public Interest

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

The EU Data Protection Directive, Information Privacy, and the Public Interest

*Fred H. Cate**

I. THE DATA PROTECTION DIRECTIVE

A. Introduction

The first serious international discussion of data protection law took place in 1968 at the United Nations International Conference on Human Rights. In the more than 25 years since that conference, data protection, privacy, and "fair information practices" have attracted widespread international and domestic debate and legislative action, particularly in Europe. The German state of Hesse enacted the first data protection statute in 1970; Sweden followed in 1973 with the first national statute.[1] Today, Austria, France, Germany, Ireland, Luxembourg, Sweden, and the United Kingdom, among other countries, have broad statutes that provide a general set of privacy rights applicable to both public and private sectors.[2]

Enactment of data protection laws by individual European nations has been paralleled and, in some cases, anticipated by collective, multinational action. In 1980 the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD) issued *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Guidelines).[3] The Guidelines outline basic principles for both data protection and the free flow of information among countries that have laws conforming with the protection principles. The Guidelines, however, have no legal force and permit broad variation in national implementation.[4]

One year after the OECD issued its Guidelines, the Council of Europe promulgated a convention *For the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention).[5] The Convention, which

---

* Associate Professor of Law and Faculty Advisor to the Federal Communications Law Journal, Indiana University School of Law-Bloomington; Senior Fellow, The Annenberg Washington Program; and Of Counsel, Fields & Director, P.C. Professor Cate convened the Annenberg Washington Program forum, Information Privacy and the Public Interest, on which this issue is based.

1. Peter Blume, An EEC Policy for Data Protection, 11 Computer/L.J. 399, 401 (1992).
2. *See generally* David H. Flaherty, Protecting Privacy in Surveillance Societies (1989).
3. OECD Doc. C 58 final (Oct. 1, 1981).
4. *See generally* Blume, supra note 1, at 404-05.
5. Jan. 28, 1981, Europ. T.S. No. 108.

took effect in 1985, is similar to the Guidelines, although it focuses more on the importance of data protection to protect personal privacy. The Convention requires each of the member countries to enact conforming national laws, although it too permits broad variances among national regimes. Only ten countries have ratified the Convention,[6] while eight have signed without ratification.[7] Finland, Liechtenstein, Malta, San Marino, and Switzerland have neither signed nor ratified the Convention.[8]

As a result of the uneven application and great variation among national laws permitted by both the Guidelines and the Convention, in July 1990 the Commission[9] of the then-European Community published a draft *Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data.*[10] The Directive is part of the ambitious program by the countries of the European Union (EU)[11] to create not merely the "common market" and "economic and monetary union" contemplated by the Treaty of Rome,[12] but also the political union embodied in the Treaty on European Union signed in 1992 in Maastricht.[13]

The shift from economic to broad-based political union brought with it new and more urgent attention to the protection of informational privacy. On March 11, 1992, the European Parliament[14] amended the Commission's proposal to eliminate the distinction between public and private sector data protection and then overwhelmingly approved the draft Directive. On October 15, 1992, the Commission issued its amended proposal. On February 20, 1995, the Council of Ministers[15] adopted a

---

6. Austria, Denmark, France, Germany, Ireland, Luxembourg, Norway, Spain, Sweden, and the United Kingdom.

7. Belgium, Cyprus, Greece, Iceland, Italy, Netherlands, Portugal, and Turkey.

8. For an excellent discussion of both the Guidelines and the Convention, see Joel R. Reidenberg, The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services, 60 Fordham L. Rev. S137, S143-48 (1992).

9. The European Commission is the administrative body of the European Union which oversees and implements the requirements of EU foundational treaties. The Commission has 17 members, two each from France, Germany, Italy, Spain, and the United Kingdom, and one from each of the other Member States. European Community Law: An Overview 44 (3d ed. 1993)[hereinafter European Community Law].

10. *See* Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (92) 422 final at 30 (the amended version was submitted by the Commission on Oct. 16, 1992).

11. The 16 current members of the EU are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, and the United Kingdom.

12. Treaty Establishing the European Economic Community, art. 2 (as amended 1987 and 1992).

13. Treaty on European Union, Feb. 7, 1992, O.J. (C 224/01) (1992), C.M.L.R. 719, *reprinted in* 31 I.L.M. 247 (1992).

14. The European Parliament is the legislative body of the EU and is composed of 518 members, who are elected through direct voting by party, not country. European Community Law, supra note 9, at 23.

15. The Council of Ministers is composed of ministers from each member country; it may

Common Position with a View to Adopting Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive).[16] Formal adoption of the Directive by the Council is certain, perhaps even by the end of 1995.

B. Terms

1. Scope and Definitions

The draft Directive is extraordinarily comprehensive. It will require each of the sixteen EU member states to enact laws governing the "processing of personal data."[17] The Directive defines "processing" broadly as "any operation or set of operations," whether or not automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[18] "Personal data" is defined equally broadly as "any information relating to an identified or identifiable natural person."[19] As a practical matter, the Directive excepts only the "processing of personal data" that is performed by a "natural person in the course of a purely personal or household activity."[20]

2. Basic Protections

National laws enacted in compliance with the Directive must guarantee that "processing of personal data" is accurate, up-to-date, relevant, and not excessive. Personal data may be used only for the legitimate purposes for which it was collected, and kept in a form that does not permit identification of individuals longer than is necessary for that purpose.[21] Personal data may be processed only with the consent of the data subject, when legally required, or to protect "the public interest" or the "legitimate interests" of a private party, except where those interests are trumped by the "fundamental rights and freedoms of the data subject . . . ." [22] The processing of data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union member-

---

accept or reject, but not modify, measures proposed by the Commission. Id. at 40.

16. European Parliament and Council Directive 95/— on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (C 93) 1 [hereinafter Directive]. The text of the Directive is reprinted in the Appendix to this issue of the *Iowa Law Review.*

17. Directive, supra note 16, art. 1(1); *see* id. art. 2(b) (defining "processing of personal data").

18. Id. art. 2(b).

19. Id. art. 2(a). "[A]n identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Id.

20. Id. art. 3(2).

21. Directive, supra note 16, art. 6(1).

22. Id. art. 7(f).

ship . . . [or] concerning health or sex life" is severely restricted and in most cases forbidden without the written permission of the data subject.[23]

3. Disclosure to Data Subjects

Data processors must inform persons from whom they collect data of the purposes for the processing; the "obligatory or voluntary" nature of any reply; the consequences of failing to reply; the "recipients or categories of recipients" of the data; the data subject's right of access to, and opportunity to correct, data concerning her; and "the identity of the controller . . . ."[24] The processor must provide the same disclosure to individuals about whom data has been collected without their consent.[25]

4. Access to, and Opportunity to Correct, Personal Data

The Directive requires Member States to enact laws guaranteeing individuals access to, and the opportunity to correct, processed information about them. At minimum, those laws must permit data subjects to obtain "without constraint at reasonable intervals and without excessive delay or expense . . . confirmation as to whether or not data relating to him are processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed."[26] Member States may limit this right of access only to protect national security, defense, criminal proceedings, public safety, an "important economic or financial interest of a Member State or of the European [Community] . . .," or a similar interest.[27]

National laws under the Directive must also permit data subjects to correct, erase or block the processing of "incomplete or inaccurate" data,[28] and the opportunity to object at any time "on compelling legitimate grounds" to the processing of most personal data.[29] The Directive requires that data subjects be offered the opportunity to have personal data erased without cost before they are disclosed to third parties, or used on their behalf, for direct marketing.[30]

---

23. Id. art. 8(1).

24. Id. art. 10. The data "controller" is the person or organization who "determines the purposes and means of the processing of personal data." Id. art. 2(d).

25. Directive, supra note 16, art. 11(1). The processor need not provide disclosure of the obligatory or voluntary nature of any response nor the consequences of failing to reply to the person about whom the data is collected. Id.

26. Id. art. 12(1).

27. Id. art. 13(1)(a)-(g).

28. Directive, supra note 16, art. 12(2).

29. Id. art. 14(a).

30. Id. art. 14(b).

5. *Data Security*

The Directive also establishes basic requirements for protecting personal data from "accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access, . . . [and] all other unlawful forms of processing."[31]

6. *Registration of Data Processing Activities*

In keeping with most European data protection legal regimes, the Directive requires that data processors—called "controllers" in the Directive—notify the applicable national "supervisory authority" before beginning any data processing.[32] Member States' national laws must require that the notification include, at a minimum: the name and address of the controller; the purpose for the processing; the categories of data subjects; a description of the data or categories of data to be processed; the third parties or categories of third parties to whom the data might be disclosed; any proposed transfers of data to other countries; and a description of measures taken to assure the security of the processing.[33] Controllers must also notify the supervisory authority of changes in any of the above information.[34]

The Directive requires each supervisory authority to investigate data processing that are "likely to present specific risks for the rights and freedoms of data subjects . . . ."[35] For certain routine processing that does not pose a significant threat to individuals' rights, such as producing correspondence or consulting documents available to the public, the Directive permits Member States to simplify or even eliminate the notification requirements.[36] Each supervisory authority is required to keep and make available to the public a "register of [notified] processing operations . . . ."[37]

7. *Restrictions on Automated Decision Making*

In a significant departure from prior data protection laws, the Directive requires Member States to "grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."[38]

---

31. Id. art. 17(1).
32. Directive, supra note 16, art. 18(1). "Supervisory authorities" are discussed below. *See* infra notes 42-44 and accompanying text.
33. Id. art. 19(1).
34. Id. art. 19(2).
35. Id. art. 20(1).
36. Id. art. 18(2).
37. Directive, supra note 16, art. 21(2).
38. Id. art. 15(1).

In the *Explanatory Memorandum* issued with the amended Directive, the Commission offers three clarifications. First, the decision must be adverse to the individual; "the simple fact of sending a commercial brochure to a list of persons selected by computer" does not constitute an adverse decision.[39] Second, the Commission stressed that the provision applies only to decisions taken "solely" by automatic processing; "what is prohibited is the strict application by the user of the results produced by the system."[40] For example, national laws must forbid an employer from rejecting an applicant solely based on the results of a computerized psychological evaluation. Third, the provision applies to processing that uses "variables which determine a standard profile." The use of automated processing to determine facts about a specific individual and then make an adverse decision against her, for example, to determine an individual bank balance and then refuse to provide cash because the account holder is overdrawn, would not be forbidden.[41]

The Directive also requires that every data subject have the right to obtain "knowledge of the logic involved in any automatic processing of data concerning him . . . ."[42]

8. *Supervisory Authorities*

Under the Directive, each Member State must establish an independent public authority to supervise the protection of personal data.[43] Each "supervisory authority" must have, at minimum, the power to investigate data processing activities, including a right of access to the underlying data; the power to intervene to order the erasure of data and the cessation of processing, and to block proposed transfer of data to third parties.[44] The supervisory authority must also be empowered to hear complaints from data subjects and must issue a report on a regular basis that is made available to the public.[45]

9. *Liability and Remedies*

The Directive requires that Member States' laws provide for civil liability against data controllers for unlawful processing activities,[46] and provide "suitable" penalties for noncompliance with the national laws adopted pursuant to the Directive.[47] In addition to requiring the

39. Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, Explanatory Memorandum, COM (92) 422 final at 26.

40. Id.

41. Id.

42. Directive, supra note 16, art. 12(1).

43. Id. art. 28(1).

44. Id. art. 28(3).

45. Id. art. 28(5).

46. Directive, supra note 16, art. 23(1).

47. Id. art. 24.

supervisory authority to enforce those laws and to hear complaints by data subjects, the Directive mandates creation of a "right of every person to a judicial remedy for any breach of the rights guaranteed by the [Directive]."[48]

10. *Restrictions on Transborder Data Flow*

Perhaps the most controversial provision in the Directive is the requirement that Member States enact laws prohibiting the transfer of personal data to nonmember states that fail to ensure an "adequate level of protection."[49] The Directive provides that the adequacy of the protection offered by the transferee country "shall be assessed in the light of all the circumstances surrounding a data transfer," including "the nature of the data, the purpose and duration of the proposed processing," the "rules of law, both general and sectoral," in the transferee country, and the "professional rules and security measures which are complied with" in that country.[50] The prohibition is subject to exemptions when the transfer: (1) has the consent of the data subject, (2) "is necessary to the performance of a contract between the data subject and the controller," (3) is necessary for performance of a contract made in the best ineterest of the data subject, (4) is necessary to serve an "important public interest," (5) is necessary to protect "the vital interests of the data subject," or (6) "is made from a register which according to laws or regulations is intended to provide information to the public . . . ."[51] The Directive forbids Member States from restricting the flow of personal data among themselves because of data protection or privacy concerns.[52]

II. THE DEBATE OVER THE DIRECTIVE

A. *The "Adequacy" of U.S. Privacy Law*

The prohibition on data transfers to other countries found to offer inadequate data protection is the cause of great concern for all businesses who operate in Europe and countries outside the EU, and particularly to U.S. businesses. While most European countries have afforded significant, detailed protection to individual privacy rights, particularly in the context of electronically stored and processed information, the United States and many other countries have no comparable system of data protection. Although the United States Supreme Court claimed in *Whalen v. Roe* to recognize a constitutional interest "in avoiding disclosure of personal matters,"[53] no Court decision has ever reversed a legislative or administra-

48. Id. art. 22.
49. Id. art. 25(1).
50. Directive, supra note 16, art. 25(2).
51. Id. art. 26(1).
52. Id. art. 1(2).
53. 429 U.S. 589, 599 (1977).

tive action based on that supposed right. Moreover, such a constitutional right—even if vindicated by a court—would apply only against governmental action. Federal statutes addressing private actions touching on personal privacy, although numerous, offer little effective protection to individuals.[54]

As a result, American businesses with interests in personal data collected, stored or processed in Europe, and particularly American businesses with operations in Europe, fear that they will be unable to move that data legally—even if they "own" it—to the United States. David Flaherty, Data Protection Registrar in British Columbia, writes:

> The European data protectors view the current situation as an excellent opportunity to put pressure on Canada and the United States for improved data protection. They anticipate blocking the movement of personal data from European branches of multinationals to Canadian or American branches, because equivalent data protection does not exist. For various reasons, including nationalistic ones, they are very serious about this. . . .
>
> . . . The American private sector, accustomed as it is to no government regulation for data protection, is especially exercised about the potential impact of the draft Directive on the data handling activities of American-controlled multinationals and has made predictable approaches for protection to the Department of State and the Office of the International Trade Representative.[55]

U.S. businesses have good reason to be worried. The first prohibition on transnational data transfer by the British Data Protection Registrar under national law[56] forbade a proposed sale of a British mailing list to a United States direct mail organization.[57] France, acting under French domestic law,[58] has prohibited the French subsidiary of an Italian parent company from transferring data to Italy because Italy did not have an omnibus data protection law.[59] The French Commission nationale de

---

54. *See, e.g.*, Fair Credit Billing Act of 1974, 15 U.S.C. § 1666 (1988); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t (1988); Fair Debt Collection Practices Act of 1977, 15 U.S.C. §§ 1692b(2), 1692c(b); Equal Credit Opportunity Act of 1974, 15 U.S.C. §§ 1691b(2), 1691c(b) (1988); Electronic Funds Transfer Act of 1978, 15 U.S.C. §§ 1693-1693r (1988); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2520, 2701-2709 (1988); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1988); Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b)(1); Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009. *See generally* Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195 (1992) (asserting that the American legal system does not respond adequately to privacy issues raised by information processing activities in the business community).

55. David H. Flaherty, Telecommunications Privacy: A Report to the Canadian Radio-Television and Telecommunications Commission 72-73 (1992).

56. Data Protection Act, 1984 (U.K.), *reprinted in* A.C.M. Nugter, Transborder Flow of Personal Data Within the EC 365 (1990).

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

58. Loi du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés (Fr.) [Law No. 78-17 of Jan. 6, 1978, concerning data processing, records, and freedom], *reprinted in* Nugter, supra note 56, at 353.

59. Déliberation no. 89-78 du 11 juillet 1989, *reprinted in* Commission nationale de

l'informatique et des libertés has required that identifying information be removed from patient records before they could be transferred to Belgium,[60] Switzerland,[61] and the United States.[62]

And the comments of at least one senior EU data protection expert, Professor Dr. Spiros Simitis, formerly Data Protection Commissioner in the German state of Hesse and Chair of the Council of Europe's Data Protection Experts Committee, suggest that there may be little room for compromise:

> [C]ontrary to most other documents and nearly for the first time in the history of the Community, the Commission in its draft said that the need for the Directive is based on the need to protect human rights within the Community. This is why, when we speak of data protection within the European Union, we speak of the necessity to respect the fundamental rights of the citizens. Therefore, data protection may be a subject on which you can have different answers to the various problems, but it is not a subject you can bargain about.[63]

B. The Importance of Information

The debate over the Directive's restrictions on transborder data flow is only intensified by the extraordinary importance of information in the U.S. and global economies. Although figures vary, information services and products are either the first or second largest sector of the U.S. economy, accounting for between ten and twelve percent of Gross Domestic Product.[64] Taken together, telephone companies, information service providers, communications equipment manufacturers, and computer hardware and software companies account for more than 4.5 million U.S. jobs.[65] This significance of information was forcefully recognized in the Clinton Administration's recent *National Information Infrastructure Agenda for Action:*

---

l'informatique et des libertés, 10e Rapport au president de la Republique et au Parlement 1989, at 32-34 (1990) [hereinafter CNIL Rapport].

60. Déliberation no. 89-98 du 26 septembre 1989, *reprinted in* CNIL Rapport, supra note 59, at 35-37.

61. Reidenberg, supra note 8, at S163 (citing an interview with Ariane Mole, Attachée Relations internationales, Direction juridique de la Commission nationale de l'informatique et des libertés, Paris, France (June 6, 1991)).

62. Id.

63. Professor Spiros Simitis, Unpublished Comments at the Annenberg Conference on Information Privacy and the Public Interest (Washington, D.C., Oct. 6, 1994).

64. *See* Brown Lists Clinton Administration's Advisors on Information Infrastructure, Daily Rep. for Executives, Jan. 7, 1994 [hereinafter Brown], *available in* LEXIS, News library, NWSLTR file at *3 (referring to remarks of Commerce Secretary Ronald H. Brown at the Museum of Television and Radio, stating that the information sector accounts for more than 10% of the gross domestic product); Transcript of Remarks by Vice President Albert Gore at National Press Club, U.S. Newswire, Dec. 22, 1993, [hereinafter Gore], *available in* LEXIS, News library, NWSLTR file at *12 (stating that the information sector accounts for more than 12% of the gross domestic product).

65. Brown, supra note 64, at *3.

"Information is one of the nation's most critical economic resources . . . . In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic importance to the United States."[66]

Even these figures do not represent the real importance of information and, therefore, the real significance of the information infrastructure in the United States. "Information," Anne Branscomb, author of *Who Owns Information?*, has written, "is the lifeblood that sustains political, social, and business decisions."[67] Noncommunications businesses rely as much on information services and products as do telephone companies and computer manufacturers. During the 1980s, U.S. business alone invested $1 trillion in information technology.[68] Between one-half and two-thirds of U.S. workers are employed in information-based jobs.[69]

The EU data protection Directive threatens U.S. leadership in the information economy and is heightening U.S. concern over protecting that so-called dominance. Some critics see the Directive as merely the newest in a series of European attacks on profitable U.S. information and programming industries. After all, it was only five years ago that the European Community promulgated an equally controversial directive—the *EC Council Directive Concerning the Pursuit of Television Broadcasting Activities* (Broadcasting Directive)[70]—that required Member States to ensure that "where practicable and by appropriate means," a majority of broadcast transmission time, excluding time occupied by news, sports, games, advertising and teletext, is reserved for "European works."[71]

---

66. Information Infrastructure Task Force, National Information Infrastructure Agenda for Action 5 (1993).

67. Anne W. Branscomb, Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition, 36 Vand. L. Rev. 985, 987 (1983).

68. Howard Gleckman, The Technology Payoff, Bus. Week, June 14, 1993, at 57.

69. Gore, supra note 64, at *11; Information Infrastructure Task Force, supra note 66, at 5. *See generally* Fred H. Cate, The Future of Communications Policymaking, 3 Wm. & Mary Bill of Rts. L.J. 1 (1994) (discussing the impact of information technology and the importance of developing effective federal information policy).

70. EC Council Directive Concerning the Pursuit of Television Broadcasting Activities, 1989 O.J. (L 298) 23 [hereinafter Broadcasting Directive]. *See generally* Fred H. Cate, The First Amendment and the International "Free Flow" of Information, 30 Va. J. Int'l L. 371 (1990).

71. Broadcasting Directive, supra note 70, art. 4. The Broadcasting Directive defines "European works" as programming originating from Member States or other European states which are parties to the Convention. "European works" must also meet one of three conditions: (1) they are made by producers "established" in Member States, (2) producers established in Member States actually control and supervise the production, or (3) no co-producer outside the European Community may provide the majority of financing for each production. Id. art. 6.

"European works" may also include programming originating from European states which are neither Member States nor adherents to the Convention, but is produced by producers established in Member States or by producers in European countries which will agree to abide by the Treaty of Rome, provided that the production must be "mainly made" with authors and workers residing in European countries. Id.

Programming which meets none of the definitions above, can still be considered a

C. *Privacy in the Electronic Information Age*

Privacy advocates, on the other hand, see the privacy Directive as the source of significant, new opportunities. As important as information may be, more and more people in the United States and elsewhere are expressing growing concern about the threat of information technologies to personal privacy. The proliferation of digital technologies—massive databases and networks, high speed data transmission, cellular telephones, facsimiles, and powerful, affordable computers—has sparked growing concern over personal privacy and heightened interest in domestic data protection and privacy law. According to the 1992 Equifax survey by Louis Harris & Associates and Alan F. Westin, seventy-six percent of Americans report feeling that they have lost control over personal information about themselves and seventy-nine percent are concerned about threats to personal privacy.[72] The Directive has the potential to play an important role in stimulating greater legal protection for personal privacy, and more responsible behavior by U.S. corporations regarding the collection, use, dissemination, and retention of personal data.

The protection of personal privacy, and the impact of the Directive, are only heightened by the inherently global characteristics of information, particularly in the growing web of electronic networks. Information increasingly does not respect boundaries. According to Professor Joseph N. Pelton:

> We are not talking about a modest proposition here. Telepower in its various forms—telecommunications, electronic entertainment, computer and information services, robotics, artificial intelligence, and expert systems—is already reshaping the global economy, internationalizing labor, and shifting jobs in space, time, and concept. Some would argue it is rendering the nation state obsolete.[73]

Whether in a wire (or optical fiber) or beamed from a satellite or microwave dish, information—particularly electronic information—is ubiquitous. Unlike a truckload of steel or a freight train of coal, television and radio signals, telephone, facsimile and modem communications are difficult to pinpoint and almost impossible to block, through either legal or technological means. As the Clinton Administration and the G-7 leaders focus attention on the Global Information Infrastructure, resolving privacy

---

European work "to an extent corresponding to the production of the contribution of European co-producers to the total production costs", provided that the production is made "mainly" with authors and works residing in European countries. Id.

72. Louis Harris & Assocs., Harris-Equifax Consumer Privacy Survey 126 (1992).

73. Joseph N. Pelton, The Globalization of Universal Telecommunications Services, Ann. Rev. of the Inst. for Info. Stud. 141, 143 (1991). *See generally* Fred H. Cate, Global Information Policymaking and Domestic Law, Ind. J. of Global Leg. Stud. 467 (1994) (stating that the self-interest of the United States requires multinational cooperation and global information standards).

issues raised by electronic information technologies and avoiding regulatory hurdles to transborder data flows are both of heightened priority.

Most importantly, all of the affected parties recognize the important opportunity presented by the Directive for meaningful consultations between U.S. and European business and government leaders. These contacts can improve the text of the draft Directive, avoid unnecessary regulation, identify potential trouble spots for compliance, and further an open exchange of ideas about the importance of protecting personal privacy while preserving the commitment of the United States and of European nations to the freedom of information.

III. INFORMATION PRIVACY AND THE PUBLIC INTEREST

The Annenberg Washington Program in Communications Policy Studies of Northwestern University sought to take advantage of this opportunity for consultation by bringing together government and business leaders from both sides of the Atlantic for far-ranging, frank discussions about the important issues surrounding the Directive and the protection of personal privacy. The Program, which provides a neutral, nonpartisan forum for addressing pressing issues of communications and information policy, works to help bridge the gaps that often divide business and government, academia and practice, and the United States and other nations. At Information Privacy and the Public Interest, senior government officials from Canada, France, Germany, and the United States, met in Washington on October 6, 1994, with executives from American Express, Bell Atlantic, Citicorp, Dun & Bradstreet, IBM, J.P. Morgan, Readers Digest, TRW, and U.S. West, public interest advocates, and leading academics from both sides of the Atlantic to be brought up-to-date about the pending Directive, define common objectives, and address differences about how those important objectives are to be realized.

This issue of the *Iowa Law Review* is the product of their efforts. It reflects not only the substantive presentations, but also the wide-ranging discussion, and the diversity of perspectives on these pressing issues. The Program is grateful to each of the participants and to each of the contributors, particularly Professor Spiros Simitis, from the Research Center for Data Protection at Goethe University; Professor Paul Schwartz, from the University of Arkansas School of Law; and Professor Joel R. Reidenberg, from Fordham University School of Law. These individuals gave generously of their extraordinary knowledge and experience to plan and execute the forum. The Program also gratefully acknowledges the editors of the *Iowa Law Review*, whose skill, flexibility, and commitment have made this issue possible.

Scholarly journal issues, such as this one, play a vital role in expanding and refining the debate over information privacy in the United States, Europe, and throughout the world. They help both generate and disseminate thoughtful perspectives on these important issues, and they

dramatically expand the audience for face-to-face discussions such as those at Information Privacy and the Public Interest. The Annenberg Washington Program is delighted to join with the *Iowa Law Review* in presenting this timely contribution to the growing debate about protecting privacy in the information age.