Volume 41 | Issue 1 Article 2

1996

Can Privacy Be Regulated Effectively on a National Level - Thoughts on the Possible Need for International Privacy Rules

Robert M. Gellman

Follow this and additional works at: https://digitalcommons.law.villanova.edu/vlr

 Part of the Computer Law Commons

Recommended Citation

Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level - Thoughts on the Possible Need for International Privacy Rules*, 41 Vill. L. Rev. 129 (1996).
Available at: https://digitalcommons.law.villanova.edu/vlr/vol41/iss1/2

This Symposia is brought to you for free and open access by Villanova University Charles Widger School of Law Digital Repository. It has been accepted for inclusion in Villanova Law Review by an authorized editor of Villanova University Charles Widger School of Law Digital Repository.

CAN PRIVACY BE REGULATED EFFECTIVELY ON A NATIONAL LEVEL? THOUGHTS ON THE POSSIBLE NEED FOR INTERNATIONAL PRIVACY RULES*

ROBERT M. GELLMAN**

TABLE OF CONTENTS

I. INTRODUCTION

IN the last twenty years, privacy regulation has become a growth industry. Collection, maintenance, use and disclosure of personal data are recognized as significant public policy concerns in much of the world. Many laws have been enacted, oversight agen-

* This Article is available at the *Villanova Law Review* home page at http://vls.law.vill.edu/academic/jd/journals/law-review/Volume_41/.

** Privacy and Information Policy Consultant, Washington, D.C.; former Chief Counsel and Staff Director of the Subcommittee on Information, Justice, Transportation, and Agriculture of the House Committee on Government Operations; B.A., 1970, University of Pennsylvania; J.D., 1973, Yale Law School. The author thanks Paul Schwartz, Colin Bennett, David Johnson and Joel Reidenberg for their suggestions and criticism of earlier drafts, and Isabel Lopez for research assistance.

Published by Villanova University Charles Widger School of Law Digital Repository, 1996

cies established and codes of conduct adopted. With the notable exception of the United States,[1] the institutionalization of privacy in the industrialized world continues to expand and to deepen its roots. Most privacy regulatory actions have taken place at the national level, although there have been local[2] and international[3] activities as well.

The purpose of this Article is to extend ongoing discussions about the scope and necessity of national privacy regulations. The question presented is a simple one, although the answer is complex and uncertain. Is it possible to provide effective privacy protections on a national level, or will it be necessary to have international rules to have meaningful protections? Framed more precisely, are modern information technology and multinational business activities combining to outstrip the ability of individual countries to regulate the use of personal information about their citizens?

For several reasons, this is presented as a question and not as a thesis. First, it is almost presumptuous for an American to suggest the need for international privacy regulation, because the United States is now significantly behind much of the Western industrialized world in addressing private sector privacy issues. In other countries, the most common approach to privacy is through the passage of omnibus laws defining privacy principles applicable to government and private sector records.[4] The United States approach to privacy is sometimes termed "sectoral," with separate and uncoordinated laws applying to some personal records, and no laws applying to other records.[5] For example, the United States has a

1. *See generally* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993) (examining lack of comprehensive data protection authority in United States).

2. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 22 (1989) (noting that first data protection law was passed in 1970 in German State of Hesse). In North America, the Canadian province of Quebec is the only jurisdiction with a comprehensive privacy law regulating the private sector. *See* Act Respecting the Protection of Personal Information in the Private Sector, S.Q., ch. 17 (Supp. 1993) (Can.).

3. For a discussion of international efforts at privacy regulation, see *infra* notes 84-129 and accompanying text.

4. There are, increasingly, hybrid systems that rely on general, legislated privacy standards with specific sectoral regulations. The European Union Data Protection Directive ("E.U. Directive") expressly encourages the use of sectoral codes of conduct. Council Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 27, 1995 O.J. (L 281) 31 [hereinafter Directive]. For an analysis of the E.U. Directive, see Rosario Imperiali d'Afflitto, *European Union Directive on Personal Privacy Rights and Computerized Information*, 41 VILL. L. REV 305 (1996).

5. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S.*

federal law protecting the privacy of video rental records.[6] More basic records of human existence (such as health, insurance and employment), however, are either not subject to any privacy controls, or are subject to occasional and uneven state laws.[7] Colin Bennett describes the private sector in the United States as "virtually unregulated" for privacy.[8]

Second, despite rapid advances in the last two decades, it remains unclear whether the privacy movement will stall as we move into the twenty-first century. Data protection authorities in some countries have moved beyond the first blush of growth and are becoming institutionalized and bureaucratic. This is neither terrible nor unexpected, but time and compromise take their toll. It remains to be seen whether these bureaucracies and their legislatures will have the energy for further expansion, modernization and coordination.[9]

Third, information technology is advancing so rapidly that privacy controls may, as a practical matter, become harder to draft and to enforce. Existing policies may lose their effect as computer networks make distance and national borders irrelevant to communications, information disclosures and economic transactions.

Private Sector, 80 IOWA L. REV. 497, 500 (1995) ("Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector.").

6. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710 (1994)).

7. *See, e.g.*, Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 300-09 (1995) (outlining data processing and privacy issues in health care arena).

8. COLIN J. BENNETT, CANADIAN STANDARDS ASSOCIATION, IMPLEMENTING PRIVACY CODES OF PRACTICE 8 (1995). Bennett excepts the credit reporting industry, which is subject to the Fair Credit Reporting Act (FCRA). *Id.* There are some other federal privacy laws in the United States. *See, e.g.*, Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)-(d) (1994) (providing that subscribers must be notified about personal data collected; providing that subscribers have right to inspect and to correct personal data; restricting disclosure of personal data); Family Educational Rights and Privacy Act of 1974 ("Buckley Amendment") § 513, 20 U.S.C. § 1232g (1994) (stating that students and parents may inspect and correct student data; restricting disclosure of student data); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (1994) (defining interception and disclosure of digitized communications and electronic mail as illegal, and establishing due process procedures for governmental access); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (1994) (requiring Federal Communications Commission to issue regulations to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object). Most personal records maintained by federal agencies are subject to the Privacy Act of 1974, 5 U.S.C. § 552a (1994). For a further discussion of the FCRA, see *infra* notes 48-61 and accompanying text.

9. For a discussion of how data protection authorities change over time, see FLAHERTY, *supra* note 2, at 385-91.

Traditional distinctions between types of records and classes of record keepers are fading. The world may have neither the will nor the ability to write privacy rules that can keep pace with the results of changing technology. It is interesting and relevant, but not crucial to this inquiry, whether current national laws are good or bad, adequate or inadequate, pro-privacy or anti-privacy. The borders of the possible can be profitably identified and discussed without making any decisions about the immediate desirability or necessity of crossing those borders.

Before moving ahead, a word about terminology is in order. In the United States, privacy can be an issue of broad and almost unbounded dimension. It encompasses everything from control over personal information to personal reproductive rights to limits on government intrusion into the home. The term "data protection" comes from Europe. It offers a more precise way of referring to privacy values that arise concerning the collection, use and dissemination of personal information.[10] When used in this Article, the term "privacy" should be understood to mean the same thing as "data protection."

II. A THUMBNAIL HISTORY OF PRIVACY: TECHNOLOGY AND ENFORCEMENT THEMES

A modern legal history of privacy must begin with the famous 1890 law review article by Louis Brandeis and Samuel Warren.[11] This article established technology as a strong and consistent privacy theme for the twentieth century:[12]

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what

10. FLAHERTY, *supra* note 2, at 11 ("Under the broad rubric of ensuring privacy, the primary purpose of data protection is the control of surveillance of the public, whether this monitoring uses the data bases of governments or of the private sector.").

11. Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). There is, of course, an earlier American privacy tradition that is reflected in constitutional guarantees against unreasonable searches and seizures, against self-incrimination, and for freedom of association and religion. *See* DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND (1967); Alan F. Westin, *Privacy Rights and Responsibilities in the Next Era of the Information Age*, *in* TOWARD AN INFORMATION BILL OF RIGHTS & RESPONSIBILITIES 71 (Charles M. Firestone & Jorge Reina Schement eds., 1995).

12. For a recent scholarly discussion of the importance of technological developments to privacy, see COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 3 (1992).

> Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[13]

Brandeis and Warren were concerned that advances in photography allowed a picture to be taken surreptitiously. Previously, a photograph required a formal sitting, allowing an individual to avoid being recorded. In the modern era of live television coverage of criminal trials, crimes in progress and even hostile military operations, this concern seems refreshingly quaint.[14]

It may be no coincidence that interest in privacy revived in the 1960s when computers began to take a prominent place in public awareness.[15] In many ways, the growth of privacy as a public policy concern in the last thirty years parallels the growth of computer usage and the emergence of the so-called Information Age.[16] When the executive branch proposed the establishment of a computerized federal data center in the United States in the mid-1960s, it sparked wide-ranging congressional hearings that continued for years, exploring different aspects of privacy.[17] These hearings ultimately resulted in the passage of the Privacy Act of 1974,[18] a law

13. Brandeis & Warren, *supra* note 11, at 195 (citations omitted).

14. *Cf., e.g.*, United States v. Cusumano, 67 F.3d 1497 (10th Cir. 1995) (holding that use of thermal imager to monitor exterior of house to detect heat sources within house violated subjective expectation of privacy in "waste heat"). For an examination of privacy issues as they relate to multimedia sound and image processing, see Joel R. Reidenberg, *Multimedia As a New Challenge and Opportunity in Privacy: The Examples of Sound and Image Processing, in* 22 MATERIALIEN ZUM DATENSCHUTZ 9 (1995). Professor Reidenberg argues that multimedia technology offers an opportunity to enhance individual interests by merging fair information practices with other concepts (such as intellectual property law) for the protection of personal information. *Id.*

15. Alan Westin refers to the "privacy crisis of the 1960s" when new physical, psychological and data surveillance technology applications transformed privacy into an issue that affected average consumers. Westin, *supra* note 11, at 80.

16. For a discussion of the fear of "Big Brother" and the development of concerns about private sector activities, see Joel R. Reidenberg, *Information Flows on the Global Infobahn, in* THE NEW INFORMATION INFRASTRUCTURE: STRATEGIES FOR U.S. POLICY 254-57 (William J. Drake ed., 1995).

17. For a history of the early legislation and congressional hearings, see PRISCILLA M. REGAN, LEGISLATING PRIVACY 71-86 (1995). For a bibliography of hearings since 1972, see HOUSE COMM. ON GOVERNMENT OPERATIONS, A CITIZEN'S GUIDE ON USING THE FREEDOM OF INFORMATION ACT AND THE PRIVACY ACT OF 1974 TO REQUEST GOVERNMENT RECORDS, H.R. REP. NO. 104, 103d Cong., 1st Sess. app. 3, 43-46 (1993).

18. 5 U.S.C. § 552a (1994).

that regulates the collection, maintenance, use and disclosure of personal information by federal agencies.

A second major privacy theme is the search for effective enforcement methods. Brandeis and Warren proposed the use of common-law tort remedies as a response to invasions of privacy. This typical American response is not necessarily characteristic of privacy enforcement in other countries. Regardless, the extent to which lawsuits provide practical relief for the average individual is open to question. The classic privacy torts[19] were developed and defined before the computer era and before the growth in maintenance and use of personal information by third-party record keepers.

The Privacy Act of 1974 ("Privacy Act"), one of the world's first (and now most outdated[20]) national privacy laws, relies on individual enforcement through litigation under statutory standards.[21] As part of the Privacy Act, Congress established the Privacy Protection Study Commission ("Privacy Commission") as a temporary organization to review and to report on public and private sector privacy issues.[22] The Privacy Commission's 1977 report included a recommendation for the establishment of an independent permanent privacy agency.[23] Congress never seriously considered the recommendation.[24]

---

19. *See* RESTATEMENT (SECOND) OF TORTS, §§ 652B (Intrusion upon Seclusion), 652C (Appropriation of Name or Likeness), 652D (Publicity Given to Private Life), 652E (Publicity Placing Person in False Light) (1977).

20. For a critical review of the Privacy Act of 1974, see HOUSE COMM. ON GOVERNMENT OPERATIONS, WHO CARES ABOUT PRIVACY? OVERSIGHT OF THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS, H.R. REP. NO. 455, 98th Cong., 1st Sess. (1983); FLAHERTY, *supra* note 2, at 359-61 (discussing impact and effectiveness of Privacy Act of 1974).

21. For a discussion of enforcement of privacy laws, see *infra* notes 140-48 and accompanying text.

22. Privacy Act of 1974, Pub. L. No. 93-579, § 5, 88 Stat. 1896, 1905 (1974). Because the Commission was temporary, § 5 of the Privacy Act was never codified; most of the remainder of the Privacy Act is codified, as amended, at 5 U.S.C. § 552a (1994).

23. *See* PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 37 (1977) (outlining functions of proposed privacy commission).

24. For a history of American proposals to establish a permanent government privacy agency, see Gellman, *supra* note 1, at 203-08. The only formal attempt to create a privacy agency in recent years came in 1994 when Senator Paul Simon offered an amendment to establish a Privacy Protection Commission. 140 CONG. REC. S5129-31 (daily ed. May 4, 1994). The amendment was offered to S.783, the Consumer Reporting Reform Act of 1994. *Id.* at S5129. There was only a brief debate, and the amendment was opposed by the floor manager of the bill largely on jurisdictional grounds. *Id.* at S5132. The amendment was tabled by a vote of 77-21. *Id.* at S5133.

The United States was an early leader in privacy. David Flaherty, a Canadian data protection scholar, wrote that the United States invented the concept of a legal right to privacy.[25] A 1976 book by a British privacy expert asserted that America was the country with the most highly developed law of privacy.[26] The United States lost that leadership, however, as the 1970s progressed. While the federal government has continued to enact privacy laws from time to time,[27] policy leadership clearly has moved to Europe. Beginning in the 1970s, European countries enacted comprehensive data protection laws governing both public and private sectors, and established formal data protection authorities to oversee and to enforce the laws.[28] Other countries have also tended to follow the European model of substantive law combined with a privacy oversight and enforcement agency.[29] The institutionalization of privacy through the establishment of permanent governmental authorities is the most significant administrative development of the past twenty years. These privacy authorities offer a different and probably more effective model of privacy enforcement and oversight. The failure of the United States to have a privacy agency has much to do with its loss of leadership and its frequently ineffective privacy laws.[30]

III. JURISDICTIONAL CONFLICTS

The question of national versus international regulation is primarily about the best and most appropriate governmental level for addressing privacy issues. Jurisdictional battles are familiar in the

25. FLAHERTY, *supra* note 2, at 306.

26. PAUL SIEGHART, PRIVACY AND COMPUTERS 11 (1976).

27. *See generally* REGAN, *supra* note 17, at 77-86 (discussing congressional hearings and overviewing enactment process for early privacy laws).

28. For example, Sweden passed the Data Act of 1973 establishing a Data Inspection Board; West Germany passed the Federal Data Protection Act in 1977 establishing a Data Protection Commissioner; France passed the Law on Informatics, Data Banks and Freedoms in 1978 establishing a National Commission on Informatics and Freedoms. Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 474-77 (1995) (citing DATA PROTECTION IN THE EUROPEAN UNION: THE STATUTORY PROVISIONS (Spiros Simitis et al. eds., 1994)). The first data protection law was passed in 1970 in the German State of Hesse. See FLAHERTY, *supra* note 2, at 22. For a list of data protection laws in countries belonging to the Organization of Economic Cooperation and Development (OECD), see BENNETT, *supra* note 12, at 57 tbl.1.

29. *See* Schwartz, *supra* note 28, at 474 (analyzing laws of Belgium, Denmark, Germany, Netherlands, Portugal, Spain and United Kingdom).

30. *See* FLAHERTY, *supra* note 2, at 305 ("The United States carries out data protection differently than other countries, and on the whole does it less well, because of the lack of an oversight agency . . . .").

United States, as state and federal governments have long fought over power and over which offers the most appropriate forum for legislation.[31] The Civil War, the states' rights movement and federalism can all be noted in passing without further comment.

Current debates over American privacy legislation illustrate different aspects of multi-level regulation, and focus on two major issues: (1) the level at which legislation should be passed, and (2) whether the laws should be exclusive or overlapping. The purpose of this discussion is not to decide at what level privacy should be legislated. Rather, it is to illustrate tensions that result when there is the prospect or the reality of conflicting rules and multiple jurisdictions. The same tensions can arise with private self-regulatory activities and with overlapping national and international privacy rules.

A. *Health Records*

There is no general federal statute that regulates the privacy of health records in the United States. It is largely a matter of state law, and none of the fifty states has identical laws.[32] States may have as many as three dozen or more laws that bear on the collection, maintenance, use or disclosure of health records.[33] There may be laws covering physicians, hospitals, insurers, public health authori-

31. Jurisdictional differences are not unique to the United States. In Canada, provincial legislation has given rise to different and stronger privacy rules for the private sector in Quebec than in the rest of Canada. Bennett describes Canada as the only country in which the scope of privacy protection in a local jurisdiction exceeds that of the federal government. BENNETT, *supra* note 8, at 10. Quebec argues that it is the only political entity in North America that meets the adequacy standards of the European Union. *Id.*

International demand for adequate privacy laws might someday encourage American states to pass their own laws in the hope of attracting business from abroad. There is no evidence of such activity yet. In Germany, a controversy over the census during the early 1980s found national and local data protection authorities on opposite sides of the issue. Schwartz, *supra* note 28, at 494-95.

32. In 1985, the National Conference of Commissioners on Uniform State Laws proposed a Uniform Health-Care Information Act in an attempt to stimulate uniformity among states on health care information management issues. Uniform Health-Care Information Act, 9 U.L.A. 475 (1988 & Supp. 1995). Only a few states enacted the uniform act in whole or in part. Having been proposed before the era of health maintenance organizations, outcomes research, cost containment, telemedicine, health database organizations and computer networks, the uniform act is now out-of-date.

33. A 1979 study by the National Commission on the Confidentiality of Health Records found that the number of laws relevant to health record confidentiality varied from 7 (in Vermont) to 39 (in Hawaii). NATIONAL COMMISSION ON CONFIDENTIALITY OF HEALTH RECORDS, HEALTH RECORDS CONFIDENTIALITY LAWS IN THE STATES 17, 54 (1979). A similar review today would surely find even more relevant laws.

ties, peer reviewers and others. In addition, there may be different laws covering general health records, AIDS records, mental health records, genetic records and other categories of health information.

Health records maintained by federal agencies are covered by the Privacy Act of 1974 in the same manner as other federal records about individuals.[34] This law does not apply to recipients of federal funds; therefore, most medical practitioners are not covered. Treatment records for alcohol and drug abuse are covered by other federal laws if the records are maintained by a person who receives federal funds.[35] The drug and alcohol laws apply to more of the health treatment community, but the limited coverage of the laws makes them inapplicable to most health records.

The result is a legal, political and practical mess. Protections for health records are inadequate, inconsistent and incomplete.[36] Practitioners and patients are largely ignorant of the laws that apply to health records and of their rights and responsibilities. Many studies and legislative reviews have sharply criticized the current legal structure.[37]

---

34. Privacy Act of 1974, 5 U.S.C. § 552a (1994). The law can apply to government contractors who are performing agency functions. *Id.* § 552a(m). There is one special provision relating to medical records that permits agencies to establish special procedures for disclosure of medical records to the subject of the records. *Id.* § 552a(f)(3). The significance of this authority has been called into question by *Benavides v. U.S. Bureau of Prisons*, 995 F.2d 269 (D.C. Cir. 1993).

35. *See* 38 U.S.C. § 7332 (1994) (providing confidentiality for information maintenance in connection with substance abuse programs conducted or assisted by United States department or agency); 42 U.S.C. § 290dd-2 (1994) (same).

36. There are ethical rules that define confidentiality responsibilities for physicians and other health care professionals. These rules are also incomplete and out-of-date. *See generally* Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255, 266-80 (1984) (discussing inadequacy of guidelines for physicians determining whether to disclose patient information). Also, professional ethical rules do not apply to everyone who obtains access to health records. For example, computer operators, claims processors and insurance companies may not be subject to ethical codes. *See generally* Schwartz, *supra* note 7, at 310-13 (discussing lack of consistency in utilizing confidential records).

37. HOUSE COMM. ON GOVERNMENT OPERATIONS, FEDERAL PRIVACY OF MEDICAL INFORMATION ACT, H.R. REP. NO. 832, Pt. I, 96th Cong., 2d Sess. 29 (1980) (report to accompany H.R. 5935) ("It is fair to conclude that most States do not have well defined, modern laws on the confidentiality of medical records."); WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, REPORT TO SECRETARY OF U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (1992). The Workgroup for Electronic Data Interchange (WEDI) report stated:

> Myriad laws and regulations require providers to maintain health information in a confidential manner. These legal parameters are difficult to catalog because confidentiality has historically been addressed at the state level, with each state crafting its own unique approach. The state rules

Until sometime in the second half of the twentieth century, the patchwork quilt of health record confidentiality rules was not perceived to be a significant problem. The two principal reasons for heightened concern about inconsistent confidentiality laws are the expansion of third-party payors for health care,[38] and the increasing computerization of health treatment[39] and payment[40] records. These factors have turned health care into an interstate business,

---

are superimposed on a federal regulatory framework. The result: a morass of erratic law, both statutory and judicial, defining the confidentiality of health information.

Id. at 5 app. 4; *see also* OFFICE OF TECHNOLOGY ASSESSMENT, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION 12-13 (1993) ("The present system of protection for health care information offers a patchwork of codes; State laws of varying scope; and Federal laws applicable to only limited kinds of information, or information maintained specifically by the Federal Government."); INSTITUTE OF MEDICINE, HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 15 (Molla S. Donaldson & Kathleen N. Lohr eds., 1994) ("Existing ethical, legal, and other approaches to protecting confidentiality and privacy of personal health data offer some confidentiality safeguards, but major gaps and limitations remain."); HOUSE COMM. ON GOVERNMENT OPERATIONS, HEALTH SECURITY ACT, H.R. REP. NO. 601, pt. 5, 103d Cong., 2d Sess. 83 (1994) (report to accompany H.R. 3600) ("Current legal protections for health information vary from State to State and are inadequate to meet the need for fair information practices standards.").

38. In 1950, individuals paid 65.5% of personal health care expenditures with their own personal funds. Private health insurance or government paid the remainder. By 1993, only 20.1% was paid out-of-pocket. DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH UNITED STATES 1994 229 (1995). In 1993, 17.3% of the population under the age of 65 was not covered by private health insurance or by Medicaid. *Id.* at 240. These statistics show that for most people, a third party pays most personal health bills.

39. Computerization of patient information is commonplace today. *See generally* Schwartz, *supra* note 7, at 300-06 (noting expanding role of data processing in health care). Major efforts to establish standards for computerized patient records are underway. A 1991 report by the Institute of Medicine recommended the formal establishment of uniform national standards for future computer-based patient records. INSTITUTE OF MEDICINE, THE COMPUTER-BASED PATIENT RECORD 147-48 (1991). This report identifies the lack of privacy and confidentiality standards as a problem for deploying new computerized patient information systems. *Id.* at 144. Extensive efforts to move toward this goal have already been undertaken and are ongoing. *See, e.g.*, WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, TOWARD A NATIONAL HEALTH INFORMATION INFRASTRUCTURE (1993) (discussing proposed strategies to improve quality and efficiency of computer systems in health care). The Computer-based Patient Record Institute is one of many organizations involved in the effort.

40. There is increasing demand for better and more uniform standards for the transfer of payment data. In 1991, at the request of the Secretary of Health and Human Services, an industry-led Workgroup for Electronic Data Interchange (WEDI) was established to provide the basis for the routine use of electronic data interchange (EDI) as the means of processing health transactions between providers and payors. WEDI found that electronic communications standards were lacking, and that over 400 different electronic formats were in use. WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 37, at 4. WEDI estimated that the adoption of uniform EDI standards and other related administrative changes would produce savings of 4 to 10 billion dollars. *Id.* Identified barriers to a uni-

and this is one reason for the recognition that state health record privacy laws are impediments.

Today, there are few, if any, participants in health care treatment or payment activities who do not operate in interstate commerce. Interstate commerce was the basis for proposed federal legislation to establish fair information practices standards for health information. The legislation became part of the Clinton administration's unsuccessful health reform effort in 1994. The legislative report accompanying a bill approved by a committee of the House of Representatives included this finding:

> The use, maintenance, and disclosure of health information affects interstate commerce because of the movement of individuals, health care providers, and health information across State lines; access to and transfer of health information from automated data banks and interstate telecommunications and computer networks; the exchange of health information through the mail; and the provision of and payment for health care through interstate means.[41]

With only limited exceptions, there is a broad consensus that favors replacing state privacy laws with a uniform federal law.[42] This, however, was not the case as recently as 1980. When Congress considered the Federal Privacy of Medical Records Act[43] during the 96th Congress, major elements of the health care establishment strongly opposed federal preemption. For example, the American Hospital Association (AHA) was opposed to federal legislation, preferring to leave the issue to state regulation.[44] By 1994, the AHA had completely changed its position and supported federal preemption, finding the argument for federal preemption to be

---

form, electronic payments system are different, and possibly conflicting, state laws on confidentiality. *Id.* at app. 4.

41. HOUSE COMM. ON GOVERNMENT OPERATIONS, HEALTH SECURITY ACT REPORT, H.R. Rep. No. 609 pt.5 at 83 (1994).

42. During consideration of H.R. 4077 in the 103rd Congress, there was some disagreement about the extent to which a new federal law should preempt stronger state and federal laws limiting disclosures of health records about AIDS, mental health, and alcohol and drug abuse treatment. This was never clearly resolved before the legislation was shelved.

43. H.R. 5935, 96th Cong., 2d Sess. (1980). Earlier versions appear at H.R. 2979, 96th Cong., 1st Sess. (1979) and H.R. 3444, 96th Cong., 1st Sess. (1979).

44. *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before a Subcomm. of the House Comm. on Government Operations*, 96th Cong., 1st Sess. 1088 (1979) (statement of the American Hospital Association).

"compelling."[45]

During consideration of health privacy legislation in the 103rd Congress, groups representing different interests were able to agree on the need for uniform federal legislation because no one benefitted from the existing diversity and inconsistency. Civil liberties groups supported federal legislation because it represented improved privacy protection.[46] Privacy protections under state laws or under common law are generally weak, and it may be easier to effect change through a single federal statute than through fifty state legislatures. Hospitals, doctors and insurers supported federal legislation because the modern system for medical treatment and payment requires greater efficiency, computerization and uniformity.

The purpose of this discussion is not to make the case for a federal health record confidentiality statute. Rather, the point is to illustrate the emergence of support for uniform national health privacy regulation. Diverse state laws governing the privacy of health records are generally recognized as a significant barrier to patient rights, fairness, efficiency and the modern practice of medicine. However, the interests of privacy advocates and industry with respect to uniform national privacy regulation do not always coincide in this fashion.[47]

B. *Fair Credit Reporting Act*

The first modern American privacy law, the Fair Credit Reporting Act (FCRA),[48] was a response to the growth and importance of third-party record keeping about consumers. Consumer reporting agencies (credit bureaus) held files on over 110 million individuals by 1969, and the files were principally used by credit grantors to evaluate the credit worthiness of consumers.[49] Problems with confidentiality, accuracy, relevance and fair use of information grew along with the size and importance of the industry. Following me-

45. *The Fair Health Information Practices Act of 1994: Hearings on H.R. 4077 Before the Information, Justice, Transportation, and Agriculture Subcomm. of the House Comm. on Government Operations*, 103d Cong., 2d Sess. 222 (1994) [hereinafter *Hearings*] (testimony of Fredric Entin, Senior Vice President and General Counsel, American Hospital Association).

46. *See, e.g., Id.* at 451-63 (testimony of Janlori Goldman, Director, American Civil Liberties Union, Privacy and Technology Project).

47. Some of the support in the privacy community for a uniform federal health privacy law that developed during the 103d Congress may have weakened during the 104th Congress. As of this writing, it is difficult to assess changes in position. In any event, the details are beyond the scope of this Article.

48. 15 U.S.C. §§ 1681-1681t (1994).

49. SENATE COMM. ON BANKING, HOUSING, AND URBAN AFFAIRS, THE CONSUMER REPORTING REFORM ACT OF 1994, S. REP. NO. 209, 103d Cong., 1st Sess. 2 (1993).

dia attention, consumer frustration and congressional hearings, Congress passed the FCRA in 1970 to regulate the collection, use and disclosure of consumer credit information.

In the last twenty-five years, the credit reporting industry has changed significantly. While credit reporting was once characterized by small, local credit bureaus, there are now three main national consumer reporting agencies.[50] The industry maintains 450 million credit files on individual consumers, and processes almost two billion pieces of data per month.[51] Without any doubt, credit reporting is an interstate business, for which a nationwide market exists.[52]

The FCRA has changed little since it was originally enacted. In the late 1980s, Congress began serious consideration of amendments to the law.[53] There was widespread recognition that the law was out of date and that change was required.[54] In 1993, a lobbyist for a public interest organization called the FCRA "a piece of prehistoric junk."[55] Legislative proposals were actively considered during the 101st, 102nd and 103rd Congresses. Disagreements over some legislative proposals were so sharp, however, that they prevented final passage of legislation in the 103rd Congress, even though both the House and the Senate passed generally similar bills.[56]

---

50. *Id.*

51. *Id.* at 2-3.

52. *See, e.g., The Consumer Reporting Reform Act of 1993 — S.783: Hearing on S.783 Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 103d Cong., 1st Sess. 68 (1993) [hereinafter *1993 Senate FCRA Hearing*] (testimony of Robert Hunter, Executive Vice President, Chase Manhattan Bank on behalf of American Bankers Association, Mastercard, VISA and others).

53. The first hearing was held in 1989 by a House Banking Subcommittee. *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance, and Urban Affairs*, 101st Cong., 1st Sess. (1989) [hereinafter *House 1989 FCRA Hearing*].

54. Support for specific legislative proposals waxed and waned during the course of several Congresses. Groups that supported one bill in one House opposed differently drafted proposals in another bill. The legislative dynamics over the course of three Congresses were complex. Changes in industry practice that were instituted in response to congressional attention resulted in some shifting in support for legislation. *See, e.g.*, SENATE COMM. ON BANKING, HOUSING, AND URBAN AFFAIRS, THE CONSUMER REPORTING REFORM ACT OF 1994, S. REP. NO. 209, 103d Cong., 1st Sess. 37-38 (1993) (statement of Senators Shelby and Domenici) (touting 20 new credit reporting industry policies, adopted on August 1, 1993, which exceeded existing legal requirements).

55. *1993 Senate FCRA Hearing, supra* note 52, at 25 (testimony of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group).

56. *See* 140 CONG. REC. H9797-9815, H9842 (daily ed. Sept. 27, 1994); 140 CONG. REC. S5136-46 (daily ed. May 4, 1994). In the 102d Congress, FCRA amendments reached the floor of the House of Representatives. 138 CONG. REC. H9400

One of the principal areas of disagreement during legislative debates was the degree to which the federal government should preempt the states from enacting legislation regulating consumer reporting.[57] Federal credit reporting legislation has been in place for twenty-five years, and no one opposes federal regulation; indeed, industry strongly supported a total federal preemption of state laws.[58] Compliance with different, overlapping and inconsistent laws presents an obvious problem for reporting agencies, their information providers and their customers, all of whom operate in an interstate environment.[59]

Consumer groups and state officials, however, have opposed preemption of state laws.[60] Consumer advocates support a federal legislative floor, but they have found that they have been able to obtain stronger standards through some state legislatures. The disagreement over this issue proved to be irreconcilable, at least over the course of three different Congresses.

On both sides of the credit preemption issue, there were strategic and tactical concerns. The credit industry initially opposed any change in the FCRA, preferring to continue existing law rather than to risk stronger federal requirements. The attention focused on credit reporting by congressional debates pressured industry to make voluntary changes in practice.[61] Eventually, industry came to favor legislative change as a way of institutionalizing the new prac-

(daily ed. Sept. 24, 1992). The key vote was on an amendment that would have removed federal preemption language, and the proponents of federal preemption won by four votes. *Id.* The bill was then pulled by its sponsors, who opposed federal preemption, and the bill died.

57. A survey of state laws by the National Consumer Law Center shows that 16 states have their own credit reporting statutes. WILLARD P. OGBURN, NATIONAL CONSUMER LAW CENTER, FAIR CREDIT REPORTING ACT 149-57, app. B (2d ed. 1988).

58. *See, e.g., 1993 Senate FCRA Hearing, supra* note 52, at 63 (statement of Barry Connelly, Executive Vice President, Associated Credit Bureaus) (expressing "compelling need for uniformity").

59. Industry had long opposed state laws and used other methods to avoid them. In *Equifax Services, Inc. v. Cohen*, 420 A.2d 189 (Me. 1980), *cert. denied*, 450 U.S. 916 (1981), a credit reporting agency challenged the Maine Fair Credit Reporting Act on a variety of grounds. *Id.* at 194. The challenge was successful in part, but overall failed, because not all provisions of the Maine law that conflicted with the federal law were overturned. *Id.* at 210-16.

60. *See, e.g., 1993 Senate FCRA Hearing, supra* note 52, at 59-61 (Resolution on Financial Privacy and Credit Reporting adopted by National Association of Attorneys General on March 28-30, 1993).

61. *See* ASSOCIATED CREDIT BUREAUS, SETTING THE STANDARD: IMPLEMENTATION GUIDE FOR CONSUMER INITIATIVES IN THE CREDIT REPORTING INDUSTRY (1994) (noting new policies and procedures of credit bureaus in areas of privacy, consumer relations and accuracy).

tices and preventing additional legal requirements, but the price for this support was a demand for federal preemption.

Preemption was not initially a high priority for industry. Because existing law was on their side, preemption was not an original concern of consumer groups either. When industry demanded preemption, consumer groups naturally took the opposite, pro-consumer position. In this fight, the battle line was drawn on a secondary front, but that did not diminish the intensity of the confrontation. Additionally, the battle over preemption is even more striking when contrasted with the consensus for uniform federal health records legislation.

C. *Self-Regulation*

Self-regulatory privacy codes offer examples of a different type of jurisdictional conflict that may arise with privacy regulation, and there is growing interest outside the United States in the use of industry privacy codes to implement statutory privacy rules.[62] It is therefore only a matter of time before conflicts are likely to arise over the scope and applicability of these self-regulatory activities.

One reason for the likely conflict is the sheer diversity of self-regulatory[63] activities that are available. Self-regulatory efforts may be focused at individual companies, at sectors (banking), at functions (marketing), at technologies (computer networks) or at professionals (doctors). For example, TRW Information Systems & Services (TRW), one of three leading credit bureaus in the United States, has established and published a set of "Fair Information Val-

62. For example, the Netherlands data protection law permits private organizations to voluntarily establish codes of conduct to further self-regulation. Additionally, the E.U. Data Protection Directive encourages the use of industry privacy codes. Directive, *supra* note 4, art. 27. The Privacy Commissioner of Canada recently came to the conclusion that voluntary privacy codes are inadequate and recommended that the Canadian Privacy Act be extended to cover the private sector. *See* Annual Report from the Privacy Commissioner of Canada (1994-95), *available at* http://infoweb.magi.com/privcan.

63. The term "self-regulation" is often used loosely. When regulatory authority is delegated by government to a private entity, then the term is used appropriately. When a private entity establishes its own rules without any government delegation, there is no real regulation. In the absence of governmental enforcement, the term "voluntary standards" may be more appropriate. *See* Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation as a Regulatory Technique*, 47 ADMIN. L. REV. 171 (1995) (concluding that, within specific limits, experience has shown that audited self-regulation is useful technique which should be considered in systematic fashion by government agencies when formulating regulatory policies). This distinction, important in other contexts, is not crucial here, and the term "self-regulation" is used here to cover self-regulatory activities, whether delegated by government or otherwise.

ues" that are intended to "form the foundation of [TRW] practices in information handling and privacy".[64] At the same time, TRW is a member of the Direct Marketing Association (DMA), which has adopted a code of fair information practices not binding on its members.[65] TRW is also a member of the Information Industry Association (IIA), a trade association representing the interests of creators and packagers of information content. IIA also has adopted fair information practices guidelines which, like the DMA code, are not binding on its members.[66] There may be other industry sponsored, self-regulatory activities to which TRW is a party.[67] In addition, individual members of the TRW staff may be subject to professional ethics codes, such as the Hippocratic Oath or the rules of bar associations.[68]

The result is that there a reasonable likelihood of a responsible company finding potential or real conflicts, or overlaps even at the voluntary level. A hypothetical example makes the point more clearly. For purposes of discussion, assume that there are privacy codes for the banking, direct marketing and insurance industries in a given country. Assume further that a bank is a member of all

64. *Fair Information Values*, TRW, July 1994 (brochure).

65. *See* DIRECT MARKETING ASSOCIATION, FAIR INFORMATION PRACTICES MANUAL (1994) (on file with author). The Direct Marketing Association (DMA) code can be contrasted with that of its Canadian counterpart, the Canadian Direct Marketing Association (CDMA). The CDMA privacy rules are binding on its members, and the association has enforcement procedures. *See* CANADIAN DIRECT MARKETING ASSOCIATION, CODE OF ETHICS AND STANDARDS OF PRACTICE, at I & J (undated) (on file with author). The CDMA recently announced its support for federal privacy legislation. John Gustavson, President & C.E.O., Canadian Direct Marketing Association, Address at the Insight Conference on Ensuring Privacy Protection on the Information Highway (Oct. 5, 1995) (Toronto, Canada) (on file with author).

66. INFORMATION INDUSTRY ASSOCIATION, FAIR INFORMATION PRACTICES GUIDELINES (Feb. 26, 1994). The diversity of the guidance issued by TRW, IIA and DMA is worthy of note. TRW's document is a short brochure that identifies broad values and general goals that are largely defined in terms of what consumers expect and what they do not expect. IIA's guidelines encourage companies to establish fair information practices policies and offer somewhat more direction, but few details. The IIA guidelines are four pages long, including a one page fair information practices checklist. The DMA's guidelines are much longer and are found in a fancy three-ring binder with even more details, information and guidance. DMA also includes a 39-page checklist. In each case, however, it is not apparent how these documents have affected behavior.

67. *See, e.g.*, ASSOCIATED CREDIT BUREAUS, INC., SETTING THE STANDARD: IMPLEMENTATION GUIDE FOR CONSUMER INITIATIVES IN THE CREDIT REPORTING INDUSTRY (1994). The privacy and other policies set out in this document "must be adhered to" by members of the Associated Credit Bureaus. *Id.* at 2.

68. None of the existing codes, policies or principles may actually be in conflict at this time. Voluntarily adopted policies may be sufficiently general in nature to avoid this problem. It is fair to ask, however, whether such general codes offer any effective protections to consumers.

three industry associations that promulgated the codes. Which code applies when the bank sells insurance through direct mail? Which code applies to corporate activities of the bank holding company that operates the subsidiaries that have promised to comply with applicable industry codes? If all codes are general or identical, then there may be no problem. But if the codes have different standards or procedures, then jurisdictional conflicts will occur.[69]

A second level of conflict is foreseeable as well for a company that operates internationally. If, for example, national privacy codes for the banking industry have different substantive or procedural rules in different countries, international bankers will face conflicts. As national industry codes for privacy spread around the world, this type of conflict is likely to arise.[70] The European Union Data Protection Directive refers to the possibility of community codes of conduct, but the process for approval and the effect of these codes is not clearly described.[71]

D. *Legal and Technological Overlaps*

Conflicts, overlaps and gaps in regulation can also arise within the same level of government because of changes in technology[72] and the way in which laws are drafted. This is not the same type of conflict as discussed earlier in this section, but it illustrates another way that data controllers and consumers can be significantly affected by inconsistent privacy policies.

An example comes from two laws that attempt to protect the

69. *See* Reidenberg, *supra* note 5, at 528 ("The U.S. standards-setting approach also defies current industry practices. The narrow, dispersed approach assumes that the processing of personal information will be limited to one context within a particular industry or company. Today, companies' information practices challenge this sectoral thinking because there is widespread, cross-sectoral use of personal information." (footnote omitted)).

70. It is possible that conflicts or potential conflicts may actually lead to the adoption of stronger privacy rules. Companies may prefer to comply with the strongest applicable code uniformly rather than accept weaker but different local rules. In Canada, where credit reporting is regulated at the provincial level, Equifax Canada, a dominant credit reporting company, takes the position that, as a matter of policy, it follows throughout all of Canada the strictest provincial law. *See* BENNETT, *supra* note 8, at 11.

71. Directive, *supra* note 4, art. 27.3.

72. The alternatives provided by technology are important because in many ways, the technology can direct policy choices. The architecture of computer networks may create problems that policy makers must confront (*e.g.*, global interconnections) and may foreclose options by not making them available (*e.g.*, use of high level encryption). *See generally*, Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 289 (1993) (arguing that "international data flows require complex standards, including overlapping regulation, rather than isolated one-dimensional rules").

privacy of consumers of movies and television programming. The Video Privacy Protection Act[73] limits businesses that sell or rent videotapes to consumers from disclosing some information about the interests of customers. The Cable Communications Policy Act of 1984[74] places limits on the collection and use of information concerning the viewing habits of cable subscribers. The details of these laws are not important here. What is notable is that both laws attempt to protect consumers from commercial exploitation of transaction information resulting from the consumption of video services.

A recent report from the National Telecommunications and Information Administration points out that the protections of the Video Privacy Protection Act may not extend to video programming transmitted through telecommunications networks.[75] Similarly, the privacy provisions of the law do not expressly apply to video carriage by direct broadcast satellite or wireless cable service operators. A broader look at rules governing the use of consumer information regarding consumption of information products and services reveals that there are no federal privacy laws that protect customers of libraries[76] or purchasers of books or magazines. The result is that essentially identical activities are subject to different privacy rules. Both consumers and merchants suffer from these differences, and there may eventually be a demand for equal treatment. The Electronic Communications Privacy Act of 1986[77] was passed in part because changes in technology created new forms of communications that were not protected by existing privacy laws.[78]

As long as the United States approach to privacy is sectoral,

73. 18 U.S.C. § 2710 (1994) (providing that "video tape service providers" may not knowingly disclose to any person, "personally identifiable" information about consumers).

74. 47 U.S.C. § 551 (1994) (prohibiting cable operator from collecting "personally identifiable" information concerning any subscriber, or from disclosing any "personally identifiable" information without written or electronic consent).

75. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE, PRIVACY AND THE NII 16 (1995).

76. When the Video Privacy Protection Act was proposed, an attempt was made to extend protection to library records, but the language was dropped because of opposition from law enforcement agencies. *See* SENATE COMM. ON THE JUDICIARY, VIDEO PRIVACY PROTECTION ACT OF 1988, S. REP. NO. 599, 100th Cong., 2d Sess. 8 (1988). Many states, however, have laws that protect the privacy of library records.

77. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.) (making interception of electronic communications and unauthorized access to stored electronic information unlawful).

78. *See* REGAN, *supra* note 17, at 129-37.

with separate, uncoordinated legislation applying to separate record systems and separate industries, these problems are certain to arise. The omnibus approach adopted by European countries establishes privacy standards that are independent of technological and market considerations. By establishing broadly applicable standards, the Europeans ensure that privacy is considered in the planning stages of new technology or activities, rather than at a less efficient and less effective point in the process. The United States is rarely, if ever, able to anticipate technology with privacy laws or policies.

E. *Analysis*

There are several lessons to be drawn here. First, for both health and credit records, pressures of technology and interstate commerce are important driving forces of industry support for federal preemption. The computerization and concentration that made it easier for credit reporting companies to operate without regard to state boundaries also made it more difficult to comply with differing state laws. For example, consider a credit application from a customer who has a business in Maryland and who resides in Pennsylvania. The application is received by a California bank that orders a credit report from credit bureaus headquartered in Georgia, Illinois and Ohio, and the application is ultimately rejected by a bank subsidiary in South Dakota. It may not be immediately apparent which state credit reporting law applies to the processing of this application. The same degree of interstate activity and computerization in the health treatment and payment process appears to provide the principal motivation for industry support for federal preemptive health privacy legislation.

Second, support for federal preemption is not always determined by core federalism principles. Interest groups are result-oriented, supporting preemption when federal action is more likely to produce a better result for their goals, and opposing preemption when the states are more likely to pass more favorable legislation.[79] The ACLU, for example, supported federal preemption for health records, but opposed it for credit records. This demonstrates a strong conviction for privacy, but an indifference to federalism. The business community does not uniformly favor federal preemptive legislation either. While there is no currently active federal legislative issue that illustrates this point directly, the life insurance

79. *See Privacy Laws—State or Federal*, PRIVACY & AM. BUS., May-June 1995, at 4-5.

industry has a history of opposing federal privacy legislation.[80]

Third, another factor in federalism battles is the extent to which state regulators may lose power if existing state laws are preempted. Some states have been active in overseeing credit reporting laws, and this has prompted opposition to federal preemption from state attorneys general who might have lost their authority over credit reporting activities in their states. While there was no visible opposition to federal preemption from the states in the health arena, this may have been due to a lack of active regulation or oversight of health privacy by state agencies, so no existing power center felt threatened by federal preemption.[81]

Finally, conflict between private regulators also seems possible. Sponsors of overlapping self-regulatory codes, such as trade associations, may compete for membership, influence or revenues, by establishing differing codes. This could raise a different level of forum shopping for record keepers and add to the overall confusion about privacy rules.

Extrapolating from national to international jurisdictions, one may speculate that American industry demand for international uniformity of regulation is likely to depend in part on the extent to which business activities routinely involve the transfer of personal information across national borders. Information and communications technologies are playing an increasingly important role in shaping the nature of international business, and the pressures of technology and commerce are likely to push toward uniformity.[82]

---

80. The American Council of Life Insurance supports the National Association of Insurance Commissioners' model state insurance information and privacy protection law, and opposes federal insurance privacy legislation. *See House 1989 FCRA Hearings, supra* note 53, at 475-501; *Confidentiality of Insurance Records, Hearings on H.R. 5646, H.R. 6518 and H.R. 7052 Before a Subcomm. of the House Comm. on Government Operations*, 96th Cong., 1st & 2d Sess. (1979-80) (testimony of Robert R. Googins, American Council of Life Insurance). One reason that the insurance industry has opposed federal regulation is that it has been traditionally regulated entirely at the state level.

81. The United States is not the only country with federal/state conflicts over privacy regulation. In Canada, for example, the province of Quebec has passed a comprehensive private sector data protection law that establishes higher standards than the federal government. *See* Colin J. Bennett, The European Union Data Protection Directive: Lesson for the Protection of Privacy in Canada, Address at the Industry Canada Workshop 13 (Aug. 31, 1995) (unpublished manuscript, on file with author); *see also* Paul-Andre Comeau & Andre Ouimet, *Freedom of Information and Privacy: Quebec's Innovative Role in North America*, 80 IOWA L. REV. 651 (1995) (discussing Quebec's implementation of laws that embrace "democratic openness," while maintaining confidentiality of personal information).

82. *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 554 (1995) ("In a world of international data transmissions, where global information sharing takes

While there may be many in the business community who favor no regulation, differential, incomplete or inconsistent regulation may be less welcome than comprehensive, yet rational, regulation. Additionally, other interest groups might be able to advance their privacy agendas with more favorable (stronger or weaker) rules at the international level. Of course, if more favorable rules are likely at the national level, then they will likely oppose international rules. Finally, conflicts among national regulators also will play an important role in shaping international regulation.[83]

IV. GLOBAL PRIVACY ENVIRONMENT

Technical and corporate infrastructures that permit routine international collection, maintenance, use and disclosure of personal information are already in place and are expanding. On the technical side, computer networks support routine international interconnections, and there is high level political support for continued expansion. A recent United States government policy document about the global information infrastructure included this vision of a seamless international web of computer networks, with connections to every nation and, perhaps, every person in the world:

> Multiple networks composed of different transmission media, such as fiber optic cable, coaxial cable, satellites, radio, and copper wire, will carry a broad range of telecommunications and information services and information technology applications into homes, businesses, schools, and hospitals. These networks will form the basis of evolving national and global information infrastructures, in turn creating a seamless web uniting the world in the emergent Information Age. The result will be a new information marketplace, providing opportunities and challenges for individuals, industry, and governments.[84]

The changes caused by computer networks—local, domestic and international—are also having a significant impact on privacy,

place involving a tremendous amount of personal data referring to individuals, the protection of individual privacy presents a critical regulatory challenge.").

83. There is clear evidence on this last point. *See, e.g.*, Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 449 (1995) ("Experience has shown that the primary interest of the member states is not to achieve new, union-wide principles, but rather to preserve their own, familiar rules.").

84. INFORMATION INFRASTRUCTURE TASK FORCE, THE GLOBAL INFORMATION INFRASTRUCTURE: AGENDA FOR COOPERATION (Feb. 15, 1995) (version 1.0), *available through* http://www.iitf.doc.gov (under *documents*).

increasing the decentralization of information processing and the surveillance of individuals:

> At the beginning of the 1990s, information processing was decentralizing even within large corporations as networks replaced mainframe computers. Today, in the mid-1990s, the decentralization of information processing has made omnipresent surveillance possible by organizations and even individuals. This decentralization enables any network participant to centralize data, for although bits of information are scattered throughout the network, they are accessible from any place on the network. This, however, is not the extent of decentralization's effects. Sophisticated information providers and intelligent networks already enable combinations of audiovisual images and sounds with other interactive services. Further, decentralization of information processing in the United States dramatically broadened the role of private-sector data processing and shifted power from the federal government to private-sector organizations. These private organizations now have exclusive control over the decisions regarding the collection and use of personal information.[85]

In the United States, exploitation of personal information for business purposes is a well-developed domestic activity, and American companies are intensifying their international activities. It is not possible nor necessary here to explore in depth the international interconnections among companies that traffic in personal data. A few examples will illustrate the trends.

An excellent illustration of routine global exchanges of personal data comes from TRW, a leading American credit reporting company. In June 1995, TRW announced an agreement with a Japanese credit bureau to allow access in Japan to the American credit records of United States citizens living in Japan. The agreement also will make available Japanese credit records for Japanese citizens living in the United States.[86] There is obviously enough rou-

85. Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 111-12 (1995) (addressing privacy issues created by expanding information infrastructure of emerging networks, and concluding that for greater congruence between network values and legal rules to occur, domestic and international pressure is needed).

86. TRW COMMUNICATIONS DEPARTMENT, TRW AND JAPANESE CREDIT BUREAU TO OPEN WAY FOR LENDER ACCESS OF "HOMELAND" CONSUMER CREDIT DATA (Press

tine transfer of individuals between the two countries to warrant a regular interconnection between separate national credit reporting systems.

Another United States credit reporting company with extensive international operations is Equifax, Inc. According to the company, its subsidiary in Canada is the largest provider of risk management information to the insurance industry, and operates Canada's largest credit reporting network and debt collection service.[87] Equifax Europe operates the second largest credit network in the United Kingdom. Another subsidiary, Transax, is the largest check guarantee company outside the United States, with operations in the United Kingdom, Ireland, France, Australia and New Zealand.[88] Overall, the company employs more than 14,000 people in North and South America, the United Kingdom and continental Europe.[89]

Another American company with large, data-intensive international operations is Reader's Digest. The company may be best known for its magazine, but the publication represents only a fraction of its business activities. The company is establishing a computerized customer information management system to support its extensive worldwide direct marketing operations. This will be a global information system, with major data centers in North America, Europe and the Far East.[90] The company is reported to have a database of 100 million households, half in the United States and half abroad.[91]

These examples only begin to suggest the extent to which personal data is used, exchanged and exploited in a global marketplace. Companies that operate across national borders increasingly face the prospect and the reality of compliance with different national privacy laws. Routine international transfers of personal data

---

Release, June 19, 1995), *available at* http://www.trw.com/news/releases/95—06—19—ISSJapan.html.

87. This information was retrieved in September 1995 from Equifax, Inc. *at* http://www.equifax.com.

88. *Id.*

89. EQUIFAX, INC., EQUIFAX BROADENS EUROPEAN MARKET, SIGNS JOINT VENTURE FOR CREDIT REPORTING IN PORTUGAL (Press Release, July 20, 1995), *available at* http://www.equifax.com/headline/july95/portugal.html.

90. Johanna Ambrosio, *Honing in on Target Customers: Reader's Digest Overhauls Flagship Database for Direct Mail Marketing Efforts*, COMPUTERWORLD, Feb. 10, 1992, at 97.

91. Richard S. Teitelbaum, *Reader's Digest; Are Times Tough? Here's an Answer*, FORTUNE, Dec. 2, 1991, at 101 (discussing use of computer databases by Reader's Digest to better understand and thereby provide better services and products to customers).

will place additional pressures on national privacy regulators to determine how to apply their laws to data transferred in other countries. International conflicts over national privacy regulation can only grow in importance as international data activities expand.

V. TENTATIVE STEPS AT INTERNATIONAL COORDINATION

Some common international data protection rules and policies have already been established. Consistent with general European privacy policy leadership, European institutions have been at the forefront of these efforts. In the past twenty years, a remarkable international consensus has been achieved regarding the broad objectives of privacy policy.[92] Many controversies and differences still remain, of course. Also, technological developments are creating new threats to privacy as well as creating new options for the protection of privacy interests. Finally, there are still sharp disagreements about implementation details and enforcement.

A. *The Organization for Economic Cooperation and Development and the Council of Europe*

The Organization for Economic Cooperation and Development (OECD) is an international organization that promotes economic and social welfare, and stimulates and harmonizes efforts on behalf of developing nations.[93] Along with nearly all industrialized free market countries, the United States is a member of the OECD. In the late 1970s, the OECD began work on guidelines for protecting privacy in transborder flows of personal data.[94] Final guidelines were adopted in 1980.[95]

The Council of Europe promotes a greater degree of collaboration among the democratic states of Europe than does the OECD, especially in the area of law and human rights. Questions about the effects of technology and privacy came under review at

92. *See generally* BENNETT, *supra* note 12, at 133-40 (citing Council of Europe and OECD as examples of international consensus).

93. THE STATESMAN'S YEAR BOOK 1981-82 38-39 (John Paxton ed., 1982).

94. For a brief history of the OECD Guidelines, see BENNETT, *supra* note 12, at 136-40.

95. Organization for Economic Cooperation and Development: Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980) [hereinafter OECD Guidelines], *reprinted in Data Protection, Computers, and Changing Information Practices: Hearing Before the Government Information, Justice, and Agriculture Subcomm., House Comm. on Government Operations*, 101st Cong., 2d Sess. (1990).

the Council of Europe beginning in the late 1960s.[96] Eventually, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention") in February 1980.[97]

As they were developed in concert,[98] a good deal of similarity exists between the OECD Guidelines and the Council of Europe Convention. Both documents, for example, are based on the general principles of fair information practices.[99] Colin Bennett has described how privacy policies around the world have converged around the notion of fair information practices,[100] and the work of

96. For a brief history of the Council of Europe's activities, see BENNETT, *supra* note 12, at 133-36.

97. 20 I.L.M. 317 (1981) [hereinafter *Council of Europe Convention*], *reprinted in Data Protection, Computers, and Changing Information Practices: Hearing before the Government Information, Justice, and Agriculture Subcomm., House Committee on Government Operations*, 101st Cong., 2d Sess. (1990).

98. BENNETT, *supra* note 12, at 137.

99. There is no formal code of fair information practices per se, but most formulations, including the OECD Guidelines and the Council of Europe Convention, center on these eight principles:

> (1) The Principle of Openness, which provides that the existence of record-keeping systems and databanks containing data about individuals be publicly known, along with a description of main purpose and uses of the data.
>
> (2) The Principle of Individual Participation, which provides that each individual should have a right to see any data about himself or herself and to correct or remove any data that is not timely, accurate, relevant or complete.
>
> (3) The Principle of Collection Limitation, which provides that there should be limits to the collection of personal data; that data should be collected by lawful and fair means; and that data should be collected, where appropriate, with the knowledge or consent of the subject.
>
> (4) The Principle of Data Quality, which provides that personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete and timely.
>
> (5) The Principle of Use Limitation, which provides that there must be limits to the internal uses of personal data and that the data should be used only for the purposes specified at the time of collection.
>
> (6) The Principle of Disclosure Limitation, which provides that personal data should not be communicated externally without the consent of the data subject or other legal authority.
>
> (7) The Principle of Security, which provides that personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure. Sufficient resources should be available to offer reasonable assurances that security goals will be accomplished.
>
> (8) The Principle of Accountability, which provides that record keepers should be accountable for complying with fair information practices.

HOUSE COMM. ON GOVERNMENT OPERATIONS, HEALTH SECURITY ACT REPORT, H.R. Rep. No. 601, pt.5, 103d Cong., 2d Sess. 81-82 (1994).

100. *See generally* BENNETT, *supra* note 12.

the OECD and Council of Europe institutionalized the harmonization that was already well underway.

Despite the broad policy similarities, there are some significant differences in scope and application.[101] The Convention applies only to automated processing of personal data, while the OECD Guidelines are not limited to automated data. Also, the Convention is legally binding[102] for countries that have ratified it, while the OECD Guidelines are not. Neither document offers specific details on practical application of the established standards, and both contain very general provisions on enforcement. The OECD Guidelines provide that data controllers[103] should be accountable for compliance.[104] The Convention requires signatories to establish appropriate sanctions and remedies for violations of data protection laws.[105] Countries can meet these general requirements by adopting enforcement methods that are suitable for their culture and legal system.

Adoption of common privacy principles is an important step toward uniformity. However, there can be less to professed adherence with voluntary guidelines, like those of the OECD, than meets the eye. In the early 1980s, the Reagan administration encouraged private American companies to adopt voluntarily the OECD Guidelines. The National Telecommunications and Information Administration (NTIA) of the Department of Commerce supported the OECD privacy effort by encouraging voluntary adoption of the OECD Guidelines by American companies. By 1983, 182 major U.S. multinational corporations and trade associations had endorsed the OECD Guidelines.[106] The United States officially trumpeted these activities as evidence of a commitment to privacy.

Considerable doubt exists, however, about the sincerity and effect of the NTIA effort. There is evidence that the NTIA's purpose was to avoid embarrassment and possible limitations on the transfer

101. For a detailed comparison of the two agreements, see Craig T. Beling, Note, *Transborder Data Flows: International Privacy Protections and the Free Flow of Information*, 6 B.C. INT'L & COMP. L. REV. 591, 614-16 (1983).

102. The Convention does not directly impose binding norms on signatories, but it requires nations to establish domestic data protection legislation. *Council of Europe Convention*, *supra* note 97, art. 4.1; *see also* Schwartz, *supra* note 28, at 471-72.

103. The OECD Guidelines, Council of Europe Convention and the E.U. Data Protection Directive all use the term "controller" or "data controller" to refer generally to the person who determines the purpose and means of processing personal data. *See* BENNETT, *supra* note 12, at 136-40. A more familiar, but less precise, American equivalent would be "record keeper."

104. OECD Guidelines, *supra* note 95, at pt. 2, para. 14.

105. *Council of Europe Convention*, *supra* note 97, art. 10.

106. Gellman, *supra* note 1, at 230.

of personal data to the United States that were being widely discussed under the banner of transborder data flows.[107] Further, there is little evidence that the endorsements of the OECD Guidelines by American companies resulted in changes in actual privacy practices.[108]

The Clinton administration has continued to pay lip service to the OECD Guidelines in developing privacy principles for the National Information Infrastructure (NII).[109] These NII privacy principles were intended to be consistent with the spirit of the OECD Guidelines.[110] Following the pattern set during the Reagan administration, however, no steps have been taken to change federal or corporate privacy policies. The Clinton privacy principles were not binding on anyone, not even the federal government. A recent report from the NTIA on privacy and telecommunications continues the familiar pattern of threatening government intervention if industry does not take steps on its own to address privacy needs.[111] These threats seem rather hollow when there have already been years of inaction.[112]

---

107. *Id.* at 231; *see also* HOUSE COMM. ON GOVERNMENT OPERATIONS, INTERNATIONAL INFORMATION FLOW: FORGING A NEW FRAMEWORK, H.R. REP. NO. 1535, 96th Cong., 2d Sess. (1980) (asserting that United States needs effective coordinating mechanism for development and implementation of policy with respect to emerging debate over international structure of communications and data flows).

108. Gellman, *supra* note 1, at 231-32.

109. INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (June 6, 1995) (Privacy Working Group, Information Policy Committee), *available through* http://www.iitf.doc.gov (under *IITF committees*).

110. *Id.* at 3 ("Finally, the Principles are intended to be consistent with the spirit of current international guidelines, such as the OECD Guidelines, regarding the use of personal information." (citation omitted)).

111. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION 27 (1995). In an indirect way, this report supports the conclusion that the earlier NTIA effort to collect endorsements from American companies of the OECD Guidelines resulted in few changes in actual practice. The report identifies the lack of uniformity in privacy protections for telecommunications-related personal information. *Id.* at 17. Also, the report urges industry to voluntarily adopt adequate notice and customer consent procedures. *Id.* at 19-27. Had industry actually been voluntarily complying with OECD Guidelines—as NTIA contended in the early 1980s—the 1995 report would have reached a different conclusion and would not have included a threat of government intervention if industry does not act voluntarily.

112. The Clinton administration's stance can be compared with the statement of Bruce Phillips, the Privacy Commissioner of Canada who stated: "The protection of privacy cannot be left to the whims of the marketplace." ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS 69 (1995).

B. *European Union Data Protection Directive*

In July 1995, the Council of Ministers of the European Union adopted a Data Protection Directive ("E.U. Directive") on "the processing of personal data and on the free movement of such data."[113] A major purpose of the E.U. Directive is to establish a common, high level of protection for personal data in all member states in order to remove obstacles to flows of personal data within the European Union.[114] This is consistent with the European Union's goals of abolishing internal frontiers and of establishing an economic and monetary union.[115] Differences in data protection laws among E.U. member states' laws were viewed as an obstacle to the flow of personal data that is a part of that internal European market.[116] The E.U. Directive seeks harmonization rather than uniformity of laws. "Harmonization" is a European Union term that calls for increased standardization.[117]

The first version of the E.U. Directive was proposed in 1990,[118] and it took five years and several drafts before final approval. The length of time that the E.U. Directive was in process is a measure of the amount of controversy that it attracted. There are some rough parallels between the debate on the E.U. Directive and the debate in the United States over reform of credit reporting laws. Privacy advocates, industry, data users and regulators were all actively engaged in trying to shape the E.U. Directive to suit their own agendas.[119] Like the credit legislation in the United States, the E.U. Directive was "declared dead" more than once.[120]

---

113. Directive, *supra* note 4.

114. *Id.* at cl. 1.

115. *See* Treaty Establishing the European Economic Community [Treaty of Rome], art. 146, *amended by* Treaty on European Union, Feb. 7, 1992, art. G, 31 I.L.M. 247, 256 (1992). Professor Colin Bennett writes that the Directive "reflects a belief that the single European market relied not only on the free flow of capital, goods and labour, but also of information." Bennett, *supra* note 81, at 2. Professor Spiros Simitis emphasizes the European Union's duty to guarantee the fundamental rights of its citizens as an important purpose of the Directive. Simitis, *supra* note 83, at 447-48 ("[T]he commission expressly declared its 1990 proposals to be an immediate consequence of the European Community's duty to guarantee the fundamental rights of its citizens.").

116. Directive, *supra* note 4, art. 7.

117. Schwartz, *supra* note 28, at 481.

118. Commission of the European Communities, Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) final at 188 [hereinafter Commission Proposal for a Council Directive].

119. *See* BENNETT, *supra* note 12, at 250.

120. Bennett, *supra* note 81, at 7. A detailed analysis of the complex politics of the Directive's adoption process can be found in Simitis, *supra* note 83.

A major area of interest and controversy involved the European Union rules on the transfer of personal data to third countries.[121] The original draft provided that personal data could be transferred only if the third country "ensures an adequate level of protection."[122] The final version contains new language that adds interpretative guidance and offers a considerable amount of flexibility on third country transfers.[123] Several specific conditions have been included in the E.U. Directive that justify some transfers to third countries even when there is no adequate level of protection.[124] Importantly, the E.U. Directive expressly provides a procedure for preventing the transfer of personal data to countries with inadequate protections.[125] An elaborate notice procedure applies when a member state or the Commission of the European Communities determines that a third country does not ensure an adequate level of protection.[126] There is considerable uncertainty about how these provisions will be interpreted and applied. It is unclear, for example, whether the E.U. Directive permits a sector-by-sector or company-by-company assessment of the adequacy of laws, or whether a country must be assessed in total.[127]

---

121. By contrast, neither the OECD Guidelines nor the Council of Europe Convention require restrictions on transfer to third countries with non-conforming laws. Graham Greenleaf, *The 1995 EU Directive on Data Protection — An Overview*, 3 INT'L PRIVACY BULL. 16 (Apr.-Jun. 1995). For an extended discussion of restrictions on transborder data flows, see Schwartz, *supra* note 28, at 473 (surveying various European restrictions on flows of personal information and distinguishing between adequacy and equivalency standards).

122. Commission Proposal for a Council Directive, *supra* note 118; *see also* Greenleaf, *supra* note 121, at 16.

123. Directive, *supra* note 4, art. 26. The Directive provides:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Id. art. 26.2. Whether the flexibility is a positive or negative feature remains to be determined.

124. *Id.* art. 26. The transfer must be: (1) consensual; (2) necessary for the performance of a contract in response to a data subject's request; (3) necessary for the performance of a contract in the interest of the data subject; (4) an important public interest or in connection with legal claims; (5) necessary to protect the vital interest of the data subject; and (6) made from a public register. *Id.*

125. *Id.* art. 25.4. Professor Schwartz uses the term "data embargo" to refer to this authority. See Schwartz, *supra* note 28, at 488.

126. Directive, *supra* note 4, arts. 25, 26.

127. Greenleaf, *supra* note 121, at 17-18 (arguing that better view is that sectoral compliance is possible). Colin Bennett suggests that both the standards

The "third country" provisions illustrate the difficulty of maintaining personal data protections when other jurisdictions do not have similar laws or practices. A term sometimes applied to a third country that deliberately avoids having privacy regulations is a *data haven.* If personal data from a country with privacy regulations can be freely transferred to a data haven where there are no privacy rules, then the legal protections available in the source country may be lost. The controller in the data haven may have no legal obligations or restrictions on use, and the data subject may have no enforceable rights.

The "third country" problem is not trivial, and the United States is a major reason. The United States does not have any general private-sector privacy laws that are equivalent to most European data protection laws. For example, if a company transfers a personnel file for its employee from an E.U. member state to the United States, that file will have no federal statutory privacy protections in the United States, and some limited protection in a few states. There is no set of fair information practices that is equivalent to the protection routinely available in Europe. The same is true for many other types of personal records. Another difference is the absence in the United States of an oversight or enforcement mechanism, such as a data protection agency. As a result of these differences, it remains unclear whether the European Union will find that U.S. privacy policies and practices meet the standard of adequacy either in whole or in part.

Because of the central importance of the United States in the world economy, this is a high stakes issue. If the United States is found to meet the adequacy test in the E.U. Directive despite its resistance to modern, comprehensive privacy laws,[128] then the credibility of the E.U. Directive may be undermined. A broad ban on data flows to the United States, however, would be disruptive, expensive and, seemingly, unlikely.[129] The exceptions that permit

("a high and common level of protection") and the methodology of applying it to third countries are unclear. Bennett, *supra* note 81, at 9. He calls it a "complex task that obviously requires empirical evaluation of practice, rather than a simple reading of the 'black letter' of the law." *Id.* The Directive itself does call for consideration of sectoral laws and professional rules in assessing adequacy, but ambiguity remains. *See* Directive, *supra* note 4, art. 25.2.

128. *See generally* Gellman, *supra* note 1, at 199 (examining U.S. data protection law).

129. International trade rules may also make it difficult to implement some limits of the transborder flow of personal information. *See* Reidenberg, *supra* note 16, at 258-59 (noting that some commentators view implementation of standards for fair information practice as form of trade protectionism). Professor Reidenberg further states that privacy was discussed as a possible trade barrier dur-

transfers to third countries, notwithstanding inadequate privacy laws, may be invoked to lessen the disruptions. Other intermediate steps might be taken to minimize the economic impact, including the possibility of allowing the United States more time to put its privacy house in order.

VI. PRACTICAL PROBLEMS OF NATIONAL PRIVACY REGULATION

The European Union has come the closest to confronting the problems of coordinating national privacy rules in an international environment. The E.U. Directive, however, is a complex and obscure document. Colin Bennett describes the difficulty of understanding and implementing the text:

> The EU Data Protection Directive is a complicated instrument. The text has been subject to much drafting and redrafting as compromises have been struck and restruck within the Commission, the Parliament and the Council. It is not a "user-friendly" document that individuals/consumers can use to ascertain and exercise their data protection right. Nowhere do we find a clear list of "fair information principles," as in most legislation and in the recent model code from the Canadian Standards Association (CSA). The reader is initially confronted with a series of legalistic "whereas" statements before the body of the directive that state intentions, place this Directive in the context of other values and policies, and pay lip service to the variety of interests that shaped its content. Nevertheless, the familiar set of "fair information principles" are present even though they take some unearthing and interpretation.[130]

We are several years away from the effective date of the E.U. Directive, and it is far from clear how the vague rules on international data transfers will be applied in practice. Relying on the familiar privacy themes of technology and enforcement, however, it is easier to describe the types of problems that may result from the lack of international rules for data protection and that are not squarely addressed in the E.U. Directive.

---

ing the Uruguay Round of General Agreement on Tariffs and Trade (GATT) and the negotiation of the North American Free Trade Agreement (NAFTA). *Id.* at 258.

130. Bennett, *supra* note 81, at 3.

A. *Technology and Conflicting Privacy Rules*

International data transfers, transactions and activities are already routine and are certain to increase. Computer networks, like the Internet, support routine communications without regard to geographical location or national boundaries. It is just as easy to send an electronic mail message around the world as it is to send one around the corner.

There is a defined set of rules regulating the international transfer of regular mail, and the risks and consequences are well understood. For electronic mail, however, the situation is more complex. As there are no fixed routes for electronic mail,[131] an electronic message from New York to Australia might pass through and be stored temporarily in several intermediary countries before it reaches its destination.[132] It is impossible to predict in advance what path the electronic message will take, and the path may be different each time a message is sent. The degree of privacy accorded to an electronic message may be determined by the countries through which the message passes or in which the message temporarily resides.[133] The United States, for example, enacted legislation[134] to afford a degree of substantive and procedural legal protection to electronic messages. Equivalent protections are not necessarily available in other countries connected to the Internet. As a result, there is a significant degree of uncertainty regarding the

131. Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349, 352 n.7 (1993).

132. It is possible that a message sent from one location in the United States to another location in the United States may pass through foreign countries as well.

133. Messages could theoretically be captured and stored for lengthy periods in intermediate countries. Consider a message that was sent to a computer in Country *A* to be transmitted to another computer closer to the destination. It is possible that a routine backup of the contents of the Country *A* computer could capture the message and store it for an indefinite period of time.

In perhaps the most famous use of backup tapes, incriminating messages from the White House computer system that had been deleted by Oliver North were reconstructed in their entirety from a tape backup system. *See* Charles R. Babcock & Don Oberdorfer, *Computer Detective Found Crucial Data; Intern's High-Tech Sleuthing Led to Files*, WASH. POST, Feb. 28, 1987, at A10 (explaining that interoffice communications were backed up on computer mainframe); *see also* HOUSE COMM. ON GOVERNMENT OPERATIONS, TAKING A BYTE OUT OF HISTORY: THE ARCHIVAL PRESERVATION OF FEDERAL COMPUTER RECORDS, H.R. REP. NO. 978, 101st Cong., 2d Sess. 9-10 (1990) ("The Iran-Contra Affair illustrates the importance of an electronic mail system as a repository for information . . . and the incident also illustrates the lack of attention that has been paid to the preservation of some computerized records.").

134. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848-73 (1986) (codified as amended at 18 U.S.C. § 2510 (1994)).

privacy rules governing electronic mail.[135]

International economic transactions are commonplace today. According to one privacy scholar, "[i]nformation sharing now takes place on an international scale and involves a tremendous amount of data referring to individuals."[136] Credit cards have been used internationally for many years, and information about credit transactions flows routinely from the country where charges are incurred to the country where the bill is ultimately sent.

An example illustrates the potential complexity of overlapping or conflicting regulation. Suppose that Country *E* prohibits the use of information from credit transactions for marketing purposes without the affirmative consent of the customer. Suppose further that Country *U* has no restrictions on the use of credit data for marketing. What rule applies when a citizen of Country *E* incurs a charge in Country *U*? There can be many players in the transaction, including the merchant, the merchant's bank or processing agent, a transaction clearinghouse and the credit card issuer. Some of the players are located in Country *E*, some in Country *U* and some could be located elsewhere. Can a company that has the transaction information in Country *U* use the data for marketing even though such use is prohibited in Country *E*? Can two companies that have the same information, as a result of the same transaction, be subject to different rules depending on the location where the information resides at any given moment? Can one company that operates in two different countries be subject to different rules at different times depending on the country in which the information is maintained? It is easy to develop even more complex and realistic examples with single transactions having a nexus with three, four or more countries.

Even if each country is determined to have "adequate" levels of data protection relative to a specific standard, there may still be differences between the rules that apply to specific record categories.[137] For example, two countries may have different procedural

135. The risks of legal interception of electronic mail must be distinguished from the risk of unauthorized or illegal interception by computer hackers or others. There are techniques, such as encryption, that minimize the consequences of interception. Government regulation of encryption, however, is a highly controversial constitutional, policy and political issue. *See, e.g.*, A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 712 (1995); *see also* Dorothy E. Denning & William E. Baugh, Jr., *Key Escrow Encryption Policies and Technologies*, 41 VILL. L. REV. 289 (1996) (outlining recent Clinton administration efforts at reforming U.S. encryption export policy).

136. Schwartz, *supra* note 28, at 471.

137. For a discussion of rules and rulemaking in the financial services indus-

requirements for disclosures, or one may require consumer consent before allowing unrelated uses of transaction data. One country may require affirmative consent (*opt-in*), while the other may permit negative consent (*opt-out*). Lacking affirmative consent, are marketing uses permissible in one country but prohibited in the other? Other procedural conflicts may involve notice, access and correction procedures, and rules for non-consensual disclosures.

Additionally, international marketing activities are certain to increase as computer networks expand. There is already a considerable amount of marketing activity on the Internet. Eventually, international marketing may be just as commonplace as, and just as indistinguishable from, domestic marketing. This will increase the routine transborder flow of consumer information and the pressures on privacy regulators. Even a casual connection through a World Wide Web page on the Internet can produce a remote record of an inquirer's electronic mail address and the subject of the inquiry. Those who engage in targeted marketing will find it interesting and profitable to be able to identify those who have used the Internet to seek information about specific consumer products and services, or about those who have shown an interest in a particular subject.[138]

An example shows how potential regulatory conflicts may arise from network activities. Assume that the collection and use of consumer transaction information with the consent of the consumer is lawful everywhere. In a country with a data registration or licensing requirement, a local merchant on the Internet will have filed the requisite forms with the country's data protection authority. A foreign Internet merchant, offering identical goods from an identical web page, may not be legally subject to the requirement. The consumer may not even be aware in what country the merchant resides or in what country the data will be maintained. A consumer who is knowledgeable about the privacy laws in his or her country may not even realize that the transaction was foreign, or that local legal protections for consumer information are not applicable.

---

try, see Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137 (1992).

138. There are already mailing lists being compiled and sold based on interests reflected in public postings on Internet usegroups. One mailing list vendor offers 250,000 electronic mail addresses in eleven different interest areas, including sports, computers, news, adult, investment, religion and pets. These lists are available from Marketry, Inc., in Bellevue, Washington. Another Internet service compiles public Internet postings in an online database that is searchable by keyword. This permits the retrieval of information about specified individuals. *See* http://www.dejanews.com.

The situation could be equally uncertain for the merchant. Must an Internet vendor comply with data protection laws in each country that is connected to the network? Does the vendor have to comply with the laws of a country only when there is a transaction that originated or is completed in that country? Depending on how data protection laws are structured, more interesting and more complex options and choices are possible. Suppose one country provides that registered data controllers are subject only to actual damages for privacy invasions. Suppose further that those who do business through the Internet from other countries who have not registered their data activities are subject to actual damages, punitive damages and liquidated damages. The merchant engaging in a normal transaction who uses transaction data in a manner that is lawful in the merchant's country but unlawful in the consumer's country may discover a potentially large legal liability as a result.[139]

Computer networks support transactions in which neither party is aware of the physical location or nationality of the other party. Neither party may be aware of the location at which transaction data is stored. Even the data controller may not be aware of where a computer service firm stores data under contract with the controller. It is possible, even likely, that data will be stored in multiple locations. In a sufficiently complex computer network, it may not even be apparent or predictable where data is maintained at any given time. National laws that depend on traditional jurisdictional hooks may be more difficult to apply in an environment characterized by international data transfers over computer networks. Applying privacy laws in this environment without broadly accepted, uniform international rules and procedures may be expensive, difficult or impossible.

B. *Enforcement*

Deciding what privacy rules, laws or standards may apply to any

139. An example of different liability rules can be found by comparing the Maine credit reporting law with the federal Fair Credit Reporting Act. The federal law includes immunity against an action by a consumer for defamation, invasion of privacy or negligence, except for false information furnished with malice or wilful intent. *See* 15 U.S.C. § 1681h(e) (1994). The Maine law, however, does not provide qualified immunity. *See* ME. REV. STAT. ANN. tit. 10, §§ 1311-1329 (West 1980). This could be a trap for the unwary credit reporting agency that was not aware that it was engaging in an activity that brought it within the scope of the Maine law. *See, e.g.*, Equifax Services, Inc. v. Cohen, 420 A.2d 189, 194 (Me. 1980) (examining differences between Maine law and federal law and holding that Maine law's failure to confer qualified immunity was not inconsistent with federal statute), *cert. denied*, 450 U.S. 916 (1981).

given set of data, consumers or merchants in an international environment is difficult enough. These jurisdictional difficulties are complicated further by problems with enforcement. What can aggrieved consumers do when their rights have been violated? How can a nation enforce its own privacy laws? Enforcement is a central concern for privacy statutes, and it presents some especially difficult problems in a transborder context.[140]

The basic privacy law for United States government records is the Privacy Act of 1974.[141] There is no centralized enforcement mechanism under the Privacy Act, but the Office of Management and Budget (OMB) has authority to issue guidelines and to provide assistance to, and oversight of, the Privacy Act by agencies.[142] Unfortunately, the OMB has traditionally shown very little interest in the law.[143] Additionally, individuals can bring lawsuits to enforce their own rights, but the former General Counsel to the Privacy Protection Study Commission testified that the Privacy Act was "to a large extent . . . unenforceable by . . . individual[s],"[144] primarily because it is difficult to recover damages and no injunctive relief is available.[145]

Enforcement of the Privacy Act is impossible for most foreigners as a matter of law. The Privacy Act only applies to citizens of the United States and to aliens admitted for permanent residence.[146] Even if foreigners were given rights under the Privacy Act, however, they would still face the same enforcement problems as Americans. In addition, they would encounter the added difficulty of managing a lawsuit in another country. This is a problem as well when enforcing privacy rights against private sector companies. The difficulty of private sector enforcement is compounded by the "scarcity of

140. Bennett sees the E.U. Data Protection Directive as pushing for convergence of enforcement and oversight mechanisms within Europe. Bennett, *supra* note 81, at 7. This will require considerable restructuring of national laws.

141. 5 U.S.C. § 552a (1994).

142. *Id.* § 552a(v).

143. *See* HOUSE COMM. ON GOVERNMENT OPERATIONS, WHO CARES ABOUT PRIVACY? OVERSIGHT ON THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS, H.R. REP. NO. 455, 98th Cong., 1st Sess (1983). David Flaherty described OMB's role as "passive." FLAHERTY, *supra* note 2, at 316.

144. OVERSIGHT OF THE PRIVACY ACT OF 1974: HEARINGS BEFORE A SUBCOMM. OF THE HOUSE COMM. ON GOVERNMENT OPERATIONS, 98th Cong., 1st Sess. 226 (1983) (testimony of Ronald Plesser, former counsel to the Privacy Protection Study Commission).

145. *Id.*; *see also* Schwartz, *supra* note 82, at 596 (noting that individuals seeking enforcement of their rights under Privacy Act "face numerous statutory hurdles, limited damages and scant chance to effect an agency's overall behavior").

146. 5 U.S.C. § 552a(a)(2).

legal rules."[147]

For those seeking to enforce privacy rules in countries with formal data protection authorities, alternatives to litigation may exist. Data protection authorities may accept and investigate complaints from individuals. This is not a practical remedy, however, for most consumers. The ability to file a complaint with the French data protection authority, for example, is a remedy that few, if any Americans, would welcome. It is difficult enough for an average individual to pursue an administrative or legal remedy within his or her own country. Expecting consumers to pursue remedies with additional barriers of distance and language is not realistic.

Data protection authorities also can initiate their own oversight and enforcement activities. It is not a simple task, however, to audit or to review activities of data controllers in other countries. The Commission of the European Communities is currently conducting a study to develop a methodology for assessing the adequacy of levels of protection of individuals with regard to the processing of personal data in third countries. When that study is completed, it may suggest approaches to the overall problem and offer some insight into how the European Union may enforce its data protection rules in other jurisdictions. It may be possible to establish effective incentives for self-enforcement of privacy rules. Meanwhile, the issue of transborder enforcement of privacy laws remains a largely unexplored subject,[148] and the E.U. Data Protection Directive offers little guidance.

VII. CONCLUSION

At the beginning of this Article, the issue of national versus international regulation of privacy was presented as an open question. While that question remains unanswered, some limited conclusions are possible. First, conflicting and overlapping international privacy laws and rules present unavoidable political, legal and policy problems. Agreement on general policy principles—such as those reflected in the OECD Guidelines and the

147. Reidenberg, *supra* note 5, at 531.

148. Professor Schwartz has begun to explore the subject with a review of the different authority of European data protection commissioners to embargo data. *See* Schwartz, *supra* note 28, at 488-92. He cites an example of how the French data protection authority used a contract in an attempt to extend its control over French data that was transferred to Italy, a country without a data protection law. *Id.* at 492. Schwartz's conclusion is that contractual solutions to international enforcement problems will be fated to "underenforcement." *Id.* Professor Reidenberg also offers an evaluation of the weaknesses of using contracts to enforce data protection laws abroad. *See* Reidenberg, *supra* note 5, at 545-48.

Council of Europe Convention—will not establish the common processes and procedures that are needed to implement common international privacy rules. General policies do not inform data controllers of their specific responsibilities or record subjects of their rights. Implementation requires additional rules. Whether those rules come from national laws, self-regulatory codes or company activities, differences across nations and industries seem inevitable.

One should keep in mind, though, that these differences are not, by themselves, necessarily bad policy. Applying common policies in varying ways to diverse categories of personal information is a potential strength of privacy regulation. Nevertheless, procedural and substantive rules can determine whether an average individual will, as a practical matter, be able to pursue substantive rights. As differences proliferate, meaningful remedies for aggrieved individuals will be difficult at best and practically or legally unavailable at worst.

Data controllers face the same problems. For example, a standard providing that record subjects should have access to their files will be implemented differently for different records. Health records require a more detailed and elaborate set of access rules and due process rights than pizza delivery records. When an access policy is prescribed by national regulators or through industry codes, rules may vary to reflect local priorities, cultures, industries and needs. These differences are certain to produce conflicts when records and people cross borders.[149] Neither national legislation nor voluntary action by record keepers will avoid the complexities of adapting general standards to specific classes of personal information.

Second, a government that has an investment in an existing data protection law may be more reluctant to coordinate with other countries. The tortured process by which consensus was achieved in the E.U. Data Protection Directive is evidence of the problem. Even though the European Union has a substantial commitment to common positions on difficult policy and legal matters, it took years to achieve general and vague agreement on data protection. Add more countries to the mix, and substantive international agree-

149. One striking example of a cultural difference comes from a comparison of the treatment of tax information in Sweden and the United States. In Sweden, an individual's net income and tax deductions are public information. FLAHERTY, *supra* note 2, at 146. Conversely, in the United States, federal tax records are protected from public disclosure by law. *See* 26 U.S.C. § 6103 (1994) ("Returns and return information shall be confidential.").

ments at a level more detailed than general policies will be even more difficult. The fight over Fair Credit Reporting Act amendments, discussed earlier, illustrates the same point.

The E.U. Directive goes beyond the Council of Europe Convention and the OECD Guidelines in providing more specificity about the obligations of member states. Nevertheless, the problems of consistency are hardly avoided by its adoption. Professor Spiros Simitis, the first data protection commissioner in the German State of Hesse, sees existing national laws as a significant obstacle to common regulation.[150] Professor Simitis also sees the political pressures for accommodating existing laws as a threat to a high level of protection and to the scope of common regulations. Extensions beyond existing national laws were too difficult to achieve in the E.U. drafting process.[151] In effect, existing national laws may create a straightjacket that can stifle creativity, responses to new technology and willingness to conform to new international rules.

Third, information technology is eroding traditional jurisdictional theories used to apply laws to individuals, corporations and data. None of the international privacy activities directly recognizes current computer network technology. The OECD Guidelines and the Council of Europe Convention were adopted in 1980 and 1981, long before computer networks were commonplace. The E.U. Directive is more recent, but it too fails to address network issues. The E.U. Directive offers pre-network solutions, and these are not necessarily translatable directly in a networked environment. Technology has overwhelmed some traditional approaches to privacy protection and some legal assumptions upon which the approaches rely.

Fourth, the United States will likely be the major impediment to any attempts to standardize privacy regulation, whether for traditional or networked records, whether through governmental or other mechanisms. There is no substantial political support in the

150. Simitis, *supra* note 83, at 449. Professor Simitis writes:

> However, while at first the national laws may appear to be a valuable aid in establishing a common regulation, in reality they constitute a serious handicap. Experience has shown that the primary interest of the Member States is not to achieve new, union-wide principles, but rather to preserve their own, familiar rules. A harmonization of the regulatory regimes is, therefore, perfectly tolerable to a Member State as long as it amounts to a reproduction of the State's specific national approach.

Id.

151. *Id.* at 449-52. Professor Simitis comments that the "likelihood that the Commission's proposals will be adopted rests not on their originality but upon the ability of Member States to identify in these proposals many elements of their own regulation." *Id.* at 449.

United States business community for even the appearance of privacy regulations, let alone substantive protections. American industry is likely to continue this resistance, perhaps until it finds itself closed out of foreign markets for lack of domestic privacy rules. There are some American companies—especially those that operate internationally and under foreign data protection laws—that may be more amenable to privacy rules. They are, however, a distinct minority.

Finally, if governments are unwilling or unable to address the details of international privacy regulation in an effective or timely manner, other options are available.[152] The private sector may find it appropriate and necessary to develop and to adopt voluntary international privacy codes without the direct participation of governments.[153] Additionally, the international standards movement may offer another alternative. While many traditional standards activities are aimed at technical issues, there are standards for quality management and quality assurance developed by the International Organization for Standards.[154] These standards focus on process management and control and on the infrastructure of quality system support processes.[155] Fair information practice standards present similar management and procedural problems, so the standards process may be compatible with privacy regulation.[156] For example,

152. One way to minimize privacy problems is to avoid collecting personal information at all. New use of information technology—including public key cryptography, digital signatures, blind signatures and digital pseudonyms—may permit some activities to continue anonymously. Anonymity is not likely, however, to offer a complete solution. *See generally* INFORMATION AND PRIVACY COMMISSIONER (ONTARIO, CANADA) & REGISTRATIEKAMER (THE NETHERLANDS), PRIVACY-ENHANCING TECHNOLOGIES: THE PATH TO ANONYMITY (1995).

153. Another approach is to build into network operating systems protocols and procedures that define and perhaps even enforce the rights of participants. For example, some degree of privacy might be assured if the network automatically provided encryption of all communications and transactions. Network protocols can establish rules of practice that are the same as or perhaps even stronger than formal legal restrictions because it can be impossible for network users to avoid or evade the rules.

154. The International Organization for Standardization (ISO) is a private international agency headquartered in Switzerland and dedicated to voluntary standardization. It has published thousands of standards, including some that are not strictly technical in nature. *See* NATIONAL RESEARCH COUNCIL, STANDARDS, CONFORMITY ASSESSMENT, AND TRADE 46-48 (1995). *See also* Bennett, *supra* note 8, at 93-94. The ISO Committee on Consumer Policy has established a working group to assess whether there should be international standards for the protection of personal data and privacy. *See* S. Spivak, Address to the 17th ISO General Assembly (Sept. 1994) (Nice, France) (on file with author).

155. *See, e.g.*, CANADIAN STANDARDS ASSOCIATION, PLUS 900 HANDBOOK: THE ISO 9000 ESSENTIALS 11 (1994).

156. A generalized approach to implementation of the ISO 9000 manage-

the Canadian Standards Association developed a model code for the protection of personal information.[157]

Standards alone, however, without common procedures or effective enforcement, including realistic remedies for aggrieved consumers, will not be adequate.[158] The experience in the United States with the OECD Guidelines shows some practical shortcomings of general standards. Many companies agreed to the OECD Guidelines, but few changed their practices or policies. There was no external pressure or enforcement, as the government was uninterested, and individual consumers were unable or unwilling to push for compliance. By contrast, a manufacturer might effectively be pressured by customers to comply with quality control principles.

A step beyond standards is a detailed voluntary international privacy code adopted jointly by merchants and consumers. A *cooperative privacy code* may offer some solutions to conflicts that would be difficult to achieve through governmental organizations, or through the traditional standards process. For example, merchants and consumers might agree upon a set of cooperatively developed privacy standards and procedures for Internet or other international computer network transactions. The rules would set out basic fair information practices for the collection, maintenance and use of personal information transmitted through network activities and transactions. This would include uniform rules for notice, individual participation, use and disclosure, security, and accountability.

An effective cooperative privacy code would have to include two elements. First, there should be substantive and procedural details that go beyond general principles. Specific responsibilities of merchants and networks service providers would have to be adequately described. Second, there should be an enforcement mechanism that offers both oversight of the activities of record keepers

---

ment standards includes the following: management decision and commitment; project planning and assignment of responsibility; training key resources; initial assessment of existing practices and procedures; documentation development; implementation of procedures; internal auditing or preassessment; independent assessment; and achievement. *Id.* at 16-17. This same approach would appear to be appropriate for implementation of privacy standards. *See also* Alan F. Westin, *Managing Consumer Privacy Issues—A Checklist*, TRANSNAT'L DATA & COMM. REP. 34 (July/Aug. 1991) (advocating use of consumer privacy policies and procedures).

157. CANADIAN STANDARDS ASSOCIATION, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION (1995) (Final Draft). *See generally* Bennett, *supra* note 8.

158. Standards could form the basis for a voluntary privacy code. With sufficient details, the standards could be the code as well.

and a practical remedy for individuals. This might include independent[159] auditing[160] and electronic dispute resolution.[161] Adjudication could be accomplished through a private service based on mediation or arbitration rather than litigation. Companies engaged in international privacy-affecting transactions could support both the development of rules and the operations of an oversight/dispute resolution entity. The dispute resolution entity could be completely independent of its supporters, collecting a fee from subscribing vendors and a filing fee from complaining consumers.

Much, if not all, of the dispute resolution process could be accomplished electronically, reducing the cost to all participants. Consumers would benefit from the availability of a practical, inexpensive process. To offer equivalent benefits to merchants, the remedies available to consumers could be limited. For example, damage awards might be limited to actual damages and punitive damages would not be available.

Internet merchants and network service providers might welcome the certainty and uniformity of the process. They have an interest in establishing workable rules that they and their customers would find acceptable, practical and responsive to existing and future problems. Consumers would welcome uniform, realistic and accessible remedies that are available without regard to borders. Those offering goods and services through international networks who agree both to comply with a privacy code and to use the enforcement mechanism, could include notices on their network postings. This would inform and reassure consumers about their privacy rights. Because current Internet users appear to have stronger concerns about privacy than the public at large, vendors who subscribe to a cooperative privacy code might attract more business than those who do not.

159. Independence is a critical attribute of a data protection authority. The E.U. Directive requires "complete independence" for the supervisory authority. Directive, *supra* note 4, art. 28. It will be necessary for a significant degree of independence to be established for privacy auditors or adjudicators, or else the entire scheme will be viewed as nothing more than a wholly owned subsidiary of its corporate sponsors. For more on the politics of the independence requirement in the E.U. Directive, see Simitis, *supra* note 83, at 462-63; *see also* FLAHERTY, *supra* note 2, at 391-94 (noting that problem lies in creating "a necessary system of governmental oversight for a data protection agency, that is compatible with the legitimate exercise of its responsibilities").

160. ISO 9000 standards call for audits as a condition of registration. This provides independent assurance that the standards have been met. *See, e.g.*, CANADIAN STANDARDS ASSOCIATION, *supra* note 155, at 22.

161. For a discussion of modes of dispute resolution in an electronic environment, see Perritt, *supra* note 131, at 388-95.

A cooperative scheme might well result in more than one privacy code. Just like industry codes apply common principles differently to different record environments, multiple codes might develop in the networked environment. Rules that might be suitable for a system that provides electronic mail services might not be appropriate for electronic commercial transactions. There could even be competition among codes, with some merchants adopting strict privacy codes as a way of attracting privacy-sensitive customers. Conflicts would not be totally eliminated, but because each network transaction or event would come with a set of privacy rules and remedies, the consumer and the merchant would know their respective rights and responsibilities for each transaction or event.

If large global companies took the lead in developing and implementing cooperative privacy codes along with appropriate consumer representatives, national governments and international organizations might be encouraged or pressured to conform disparate laws to those codes.[162] For example, the European Union might find it convenient to determine that a suitable cooperative privacy code for the Internet meets the adequacy test for network data transfers to third countries. It would certainly offer a way to avoid problems of third-party enforcement that will be difficult to address in other ways. There is clear support for industry codes in the E.U. Directive and in some national laws, so this is not an unreasonable expectation. Cooperative privacy codes could even be adopted domestically in the United States as a way of avoiding the development of conflicting state rules or unwelcome federal rules. If privacy problems are solved or significantly diminished through private means, pressure for formal legislation may diminish.

Cooperative privacy codes are not a panacea. Computer networks may make it relatively easier to develop and to apply cooperative codes, but the barriers will be higher for other, more traditional, types of activities. Also, even when consumers and merchants can agree to solutions among themselves, the presence and needs of government cannot be completely ignored. Coopera-

162. There is precedent for the development of private law. *See, e.g.*, Michael T. Medwig, Note, *The New Law Merchant: Legal Rhetoric and Commercial Reality*, 24 LAW & POL'Y INT'L BUS. 589, 589-90 (1993). The author comments:

> The law merchant is spoken of under a number of names, including international, transnational, or supranational commercial law; international customs or usages; general principles of international commercial law; and *lex mercatoria*. Regardless of the label, the same phenomenon—a set of rules encompassing the trading practices of the international merchant community—is being described.

Id. at 590 (citations omitted).

tive privacy codes would have to consider the possibility of demands for information and surveillance from law enforcement, national security and other government agencies. Still, the possibility that there will be other demands for information does not prevent consumers and merchants from addressing their own activities and resolving their own disputes. Both sides must recognize and accept outside restrictions.

Privacy was a public policy issue long before the invention of the computer and computer network. Modern technology has moved privacy issues from the local to the national and now to the international sphere. Those countries that are willing to address privacy concerns nevertheless may be unable to offer their own citizens assurances that personal information in an internationally networked environment will be fairly used in accordance with fair information practice standards. Additional efforts at internationalization and privatization of privacy policy and regulation may be necessary if privacy protections are to be maintained anywhere. Whether those efforts should be private or governmental, or will have any realistic chance of success, remains to be seen.