TRANSBORDER DATA FLOW AND THE PROTECTION OF PRIVACY: THE HARMONIZATION OF DATA PROTECTION LAW

DAVID M. COOPER

Recent developments in computer and communications technologies have facilitated the flow of information across national borders. The ease of gathering and transferring data has raised serious questions regarding the protection of the individual from the compilation and misuse of personal information. Governments have an interest in restricting some information flow, but many businesses depend on the ability to send information freely across borders. In this article, David M. Cooper explores the complexity and variety of interests related to the problem of transborder data flow. He reveals how differing national interests in limiting the flow of data have led to the enactment of significantly different national data-protection and privacy laws in the United States and Europe. After surveying the developments in privacy legislation, Mr. Cooper reviews the recent attempts to harmonize these disparate national laws by implementing international guidelines and conventions. The author concludes by proposing several measures that can be taken by the United States to aid in efforts toward the harmonization of privacy law.

Over the past twenty years, the development of computer and communications technologies has dramatically altered the process of storing, retrieving, and transferring information. New computer and telecommunications capabilities have aided businesses, governments, and others by drastically reducing the costs of maintaining records on individuals. These new technologies have done more, however, than quantitatively increase the speed and capacity of record-keeping facilities. There has also been a qualitative change in the process of information storage — one that has significant implications for the maintenance of individual privacy.

In the past, data on an employee, for instance, was accessible only to a limited number of people without the allocation of a significant amount

---

David M. Cooper is a candidate for the MALD degree at the Fletcher School of Law and Diplomacy and is a programmer/analyst and consultant for Multiplications, Inc. in Cambridge, MA.

of resources to copy, mail, and distribute documents. The technology of the past placed natural barriers in the way of the unintended disclosure of personal information. With the advent of high-speed computer systems, which incorporate extensive video-display terminal networks, information on an individual can be recalled from a database at any time, by any number of people, with a trivial amount of resources per individual. Thus, data formerly held secure by the slowness and expense of copying and distribution, can, if not protected by suitable security mechanisms, today become accessible to large numbers of people. In addition, the development of extensive international communication systems involving microwave relays, undersea cables, and satellite links, combined with the development of modems and other mechanisms for the transmission of computer-readable data, has made possible the instantaneous transfer of this data across vast distances. Data can be recorded, transferred, or retrieved between nations as quickly as between adjacent offices.

This transfer of data across international borders by automatic means is termed transborder data flow (TDF). TDF has been defined as "the electronic movement of data between countries."[1] Unfortunately, this definition is too broad. Since a simple overseas telephone conversation is, in effect, a transfer of data by electronic means, some have distinguished TDF from other forms of modern international communication by requiring that "the technical process involve: (1) transmission, (2) storage, and (3) computation."[2] Computation in this sense does not refer to the manipulation of numeric quantities, but merely the use of electronic computers.

TDF has significant ramifications in the areas of legal as well as social, political, and economic policy. It poses a number of questions that have only begun to be resolved and about which a large body of literature is accumulating. The protection and creation of jobs, maintenance of control over sensitive domestic economic data, and differing concepts of the development of law, as well as the privacy of the individual, are all involved in this increasingly important issue.

I. Political and Economic Considerations

Data has traditionally been processed close to the site of its compilation. Now, however, advancing technologies have made it possible to centralize the processing of data far from the location of its acquisition. In addition, the development of data networks has often resulted in the concentration

1. William L. Fishman, "Introduction to Transborder Data Flows," *Stanford Journal of International Law* 16 (Summer 1980): 1.
2. Eric J. Novotny, "Transborder Data Flow Regulation: Technical Issues of Legal Concern," *Computer/Law Journal* III (Spring 1982): 106.

of high-paying technical jobs in the data processing state, leaving only low-paying, key-punch operations in the data-exporting state. As a result, many nations are beginning to regard the development of their own data processing and communications industries as a high priority — especially since the value of the world market for telecommunications is expected to reach $145 billion by 1985.[3]

This industry is clearly dominated by the United States: 56 percent of the world's largest data bases are located in the U.S.[4] American computer firms such as IBM dominate the international computer hardware market as well. Many nations have recognized U.S. dominance and have begun to take steps to change this situation. In Canada, the loss in foreign exchange to the U.S. for data services has been estimated at $300 million per year.[5] Elizabeth Kriegler of the Canadian Department of Communications expressed some of the concerns typically felt by the United States' trading partners:

> The sale of individual hamburgers may be . . . registered on a computerized cash register and transmitted hundreds of miles to another location for analysis . . . We must avoid a scenario wherein our young people might find jobs cooking and selling them, but are precluded from any attendant data processing, systems analysis, market research, or corporate decision-making functions.[6]

The Nora-Minc Report, commissioned by the French Government in the late 1970s, depicted the international competition over communications and computers as a "battle" with IBM in which France's current defenses are as useless as was the Maginot Line at the onset of World War II.[7] It suggested that "IBM is following a strategy that will enable it to set up an [international] communications network and control it."[8]

Some nations have also expressed concerns over the potential loss of national control resulting from the export of information. The Canadian Government's Clyne Report noted that, of all the developing technologies, computer and commmunications technologies "pose probably the most

3. John C. Lautsch, "Computers, Communications and the Wealth of Nations: Some Theoretical and Policy Considerations about an Information Economy," *Computer/Law Journal* IV (Summer 1983): 102.
4. W. Michael Blumenthal, "Transborder Data Flow and the New Protectionism," *Vital Speeches of the Day* 47 (15 August 1981): 552.
5. David F. Linowes, "Is There a Spy in the Sky," *Vital Speeches of the Day* 47 (1 July 1981): 667.
6. Joan Edelman Spero, "Information: The Policy Void," *Foreign Policy* 48 (Fall 1982): 147.
7. Simon Nora and Alain Minc, *The Computerization of Society, A Report to the President of France* (Cambridge, MA: The MIT Press, 1980), p. 69, 73.
8. Ibid., p. 6.

dangerous threat to Canadian sovereignty."[9] The Canadian Minister of Science and Technology stated that TDF "creates the potential . . . that industrial and social development will be largely governed by the decisions of interest groups residing in another country."[10] Sweden has also expressed a fear that transfer of information to a foreign country poses a threat to the control of strategic national information.[11]

In contrast to these national concerns, many corporations depend on the ability to send information freely across national frontiers in order to conduct business. Arthur A. Bushkin, a former U.S. delegate to the Organisation of Economic Cooperation and Development (OECD), asserted that "the ability to manage a company's internal information flows is as important as — and in some cases not so different from — the ability to manage a company's assets or its production."[12]

A variety of concrete measures has been imposed by some data-exporting states. Some nations have imposed restrictions on communications systems by requiring that data be sent through nationally owned telecommunications facilities rather than through privately leased lines. This imposes extra costs on the exporting organization and provides business for nationally owned networks.[13] Control Data Corporation and Tymshare, corporations based in the U.S., faced extensive prohibitions on the use of privately leased lines when they attempted to establish operations in Japan.[14] In addition to these recent measures, a significant threat to the free flow of data between countries lies in the development of inconsistent data protection and privacy laws.

II. Recent Privacy Legislation

The rapid proliferation of computer facilities and the conversion of paper files into computer data bases pose difficult questions regarding the protection of the individual from the compilation and misuse of private information. In the nineteenth century most of an individual's records could be found in the home.[15] Today, information on an individual is held by a large number of organizations and institutions. An average citizen of a developed nation is likely to have records pertaining to him or her in the data bases of employers, banks, various government agencies,

9. Fishman, "Introduction to TDF," p. 9.
10. Blumenthal, "New Protectionism," p. 552.
11. Fishman, "Introduction to TDF," p. 10.
12. Arthur A. Bushkin, "The Threat to International Data Flows," *Business Week* (3 August 1981): 11.
13. Spero, "Information," p. 141.
14. Ibid.
15. Fishman, "Introduction to TDF," p. 5.

educational and medical institutions, and credit agencies, among others. David Linowes, paraphrasing Alexander Solzhenitsyn, noted that

> As every man goes through life, he fills in a number of forms each containing a number of questions . . . there are thus hundreds of little threads radiating from every man. Millions in all. Whoever has access to those threads has the potential power to manipulate that person.[16]

The concept of privacy overlaps extensively with the concept of data protection. P. Sieghart of the United Kingdom's Data Protection Commission defined privacy as "the claim of the individual to decide for himself who shall know what about him, and what use they shall be entitled to make of that knowledge."[17] Used often in Europe, the term "data protection" is roughly synonymous with the concept of fair record practices in the United States. It refers to the protection of personal rights in the creation, use, and maintenance of records containing personal data. Data protection laws are intended to protect the individual from the creation and misuse of personal records. The concept of privacy protection in the United States, however, also includes the protection of persons from intrusions that do not generate stored records. The term "privacy protection" is most often used in common law countries, while nations with civil law traditions use "data protection." For the purposes of this article, privacy protection and data protection are used synonymously.

Most major privacy or data protection laws have been enacted since 1973. These laws were enacted to provide a form of "due process" to those about whom the data was collected (the data subject).[18] Western nations typically protect data in one of two ways: (1) the piecemeal approach taken by the United States, and (2) the omnibus approach often found in European laws. The U.S. has enacted privacy legislation on a sector-by-sector basis, while many European states have enacted data protection laws covering most public and private institutions.

One of the most important of the U.S. laws on privacy is the so-called Watergate legislation — the 1974 Privacy Act. The Privacy Act covers record-keeping activities of government agencies in relation to citizens. The legislation explicitly defines most of the privacy rights that other countries have attributed to persons.[19] Although the objectives of the

16. Alexander Solzhenitsyn as paraphrased in Linowes, "Spy in the Sky," p. 667.
17. P. Sieghart, "The Protection of Personal Data — Lacuna and Overlap," in Organisation of Economic Cooperation and Development, *Transborder Data Flows and the Protection of Privacy*, Proceedings of Vienna, Austria symposium, 20-23 Sept. 1977, p. 226.
18. Michael G. Epperson, "Contracts for Transnational Information Services: Securing Equivalency of Data Protection," *Harvard International Law Journal* 22 (Winter 1981): 161.
19. Ibid., p. 160.

Privacy Act are similar to most European data protection legislation, the law falls short in scope compared to its European equivalents. The Privacy Act fails to protect non-residents of the United States.[20] Many of the European data protection laws, on the other hand, protect all those within their territory.[21]

U.S. laws protect only natural persons in most cases, while some European laws extend protection to corporations, social clubs and other private organizations. These laws allow corporations to contact record-keeping organizations to insure that all information pertaining to them is accurate and is not improperly divulged. One commonly cited rationale for the greater scope of European laws is that, in the case of a small business, there is often little difference between the privacy rights of the shopkeeper and those of his or her individually-owned corporation.[22] Others criticize this concept, asserting that extending privacy law to corporations interferes with the "free circulation of information" in the marketplace.[23] Yet, even critics admit that, in the area of credit information, such protection might be necessary.[24]

The United States has also enacted privacy legislation covering fair credit reporting, educational records, bank records, electronic funds transfer systems, and a few other areas of private sector recordkeeping.[25] Except for these specific institutions covered by U.S. law, the private sector is essentially unregulated.

Critics of U.S. privacy law have noted that it is incumbent upon aggrieved individuals to seek to assert their rights through the courts.[26] U.S. law provides little in the way of *advance* safeguards against the improper collection, use, and dissemination of personal data. Rather than being aimed at the prevention of abuse, U.S. law provides only the remedy of litigation for damages after the violation has occurred. If an individual in the U.S. believes that his or her privacy rights have been violated by government authorities, there is no institution concerned with privacy protection to whom he or she can turn. The individual must contact the particular agency believed to be holding the records in question.[27] In many European countries, the affected individual may petition a single

20. Privacy Act of 1974, 5 U.S.C. Sec. 552a.
21. Rein Turn, "Privacy Protection and Security in Transnational Data Processing Systems," *Stanford Journal of International Law* 16 (Summer 1980): 72.
22. Andrew Lloyd, "UN Body Approves Data Protection Report," *Transnational Data Report* 6 (October/November 1983): 349.
23. Janice Wright, "The Protection of Corporate Privacy," *Transnational Data Report* 6 (June 1983): 233.
24. Ibid.
25. Turn, "Privacy Protection," p. 70.
26. Sieghart, "Lacuna and Overlap," p. 227.
27. Turn, "Privacy Protection," p. 76.

government agency to take investigative and prosecutorial actions. For example, in France, an individual can request that the National Commission on Data Processing and Liberties (CNIL) investigate any suspected infractions.[28]

However, in its defense, some have noted that U.S. privacy law does not restrict coverage specifically to computer-controlled records. Instead, U.S. law covers all documents independent of the media in which they are stored.[29] The most common criticisms of U.S. law are aimed at the lack of comprehensiveness and the loopholes afforded to data collectors.

Despite variations from country to country, European privacy laws have a number of common provisions. European laws often require the registration or licensing of data processing activities that involve personal data. In Sweden, for example, a license must be acquired from the Data Inspection Board prior to the establishment of a data base containing personal data.[30] Swedish law states that permission to export data should be granted "only if it may be assumed that release of the information will not cause undue encroachment on the privacy of anyone."[31] In one instance, the Swedish board objected to the creation of a data base in the U.K. that would contain information on most Swedish households.[32] At that time, the U.K. had yet to enact any legislation concerned with data processing privacy abuse. Other nations have not required licenses but have allowed data collectors to be self-regulating under the monitoring of the government data protection board.[33]

The approach of most European law reflects the civil law tradition that it is preferable to establish a law prior to the onset of the situation which the law addresses.[34] In addition, the civil law approach defines what is allowed instead of what is not, forbidding anything that is not specified as permissible. The German data protection law, for example, states that the processing of personal data is allowed if defined by statute or consented to by the data subject.[35] In common law countries such as the United States, law is usually formulated after problems have arisen, and anything not expressly forbidden is permitted.

In addition to this basic philosophical divergence, different countries

28. Law No. 78-17 of 6 January 1978 (France), Chapter II, Article 6.
29. Fishman, "Introduction to TDF," p. 5.
30. The Swedish Data Bank Statute (1973:289) of 11 May 1973, Section 3.
31. Ibid.
32. Turn, "Privacy Protection," p. 80.
33. Michael D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy," *Stanford Journal of International Law* 16 (Summer 1980): 39.
34. Blumenthal, "New Protectionism," p. 553.
35. Law for the Protection of Personal Data Against Misuse In Data Processing, German Federal Republic, 27 January 1977, Chapter 1, Section 3 (1) and (2).

identify different types of personal data as "sensitive." Australians view facts concerning family, friends, physical health, and sexual morality as being sensitive. French law, however, defines racial origin, political or religious affiliation, or union membership as sensitive, non-recordable data.[36] Australian Supreme Court Justice Kirby attributes the French perspective to European concern with political persecution following World War II.[37] Frits W. Hondius of the Directorate of Legal Affairs of the Council of Europe, in defending the basis of European data protection law, gives the example of the World War II fate of Anne Frank:

> Anne Frank was an innocent girl who, like millions of others, was deported. The authority who administered this sinister operation used personal records, although, thank God, not a computer. This is why Europeans today are so emphatic about protecting men, women, and children against data abuse.[38]

Differing national regulations on the creation, maintenance, and export of files containing personal data pose potential legal and economic problems. Once data have been transferred or exported from a state with stringent data protection laws to another state with less restrictive laws, the sending state's law could be circumvented. Although none of the European laws have flatly prohibited the transfer of data to states with less stringent data protection laws, the inability of data protection authorities to inspect foreign operations might make it difficult to obtain government approval for setting up a data bank.[39]

Already, incidents have occurred where this fear has led to the denial of permits or the refusal of access to data. A request by Burroughs Corporation to "dial into" the Canadian Government Computing System to aid in the repair of the system hardware was denied.[40] Even the threat of potential refusal of licenses might have an effect on the ability of data services in a less protective country to obtain valuable contracts. Therefore, some analysts feel that even if government data protection boards act in good faith, they represent a threat to the free flow of information.[41] In addition, transborder data flow licensing can be used as "a form of commercial extortion" according to American attorney David Farnsworth.[42] Farnsworth

36. Kirby, "Basic Rules," p. 49.
37. Ibid.
38. Fritz W. Hondius, Letter to the editor, *Transnational Data Report* 6 (November/December 1983): 353.
39. Epperson, "Contracts for Information Protection," p. 164.
40. Blumenthal, "New Protectionism," p. 553.
41. Epperson, "Contracts for Information Protection," p. 168.
42. David P. Farnsworth, "Data Privacy: an American's View of European Legislation," *Transnational Data Report* 6 (July/August 1983): 288.

suggests that data protection boards might be tempted to use the granting or withholding of licensing permission in order to influence corporate decisions in favor of their country's interests.[43]

Another legal problem in the transfer of personal data lies in the potential inability of individuals to have access to their records in a foreign country.[44] Due to the complexity of the computer and communication systems involved, potential problems are not limited to the simple two-state case. It is common for data to be transferred within a network of computers where the data spends milliseconds in a number of computers in a number of states, and for the time that the data resides in one of these states it may (depending on the specific capabilities of the system involved) be possible for the data to be copied or tampered with.

When differences in the approaches to data protection law are cited as reasons to hinder transborder data flow between the OECD states, it is usually the United States which is singled out as the state with the lax privacy law.[45] Though inconsistencies between European states are sometimes cited as a problem, some fear that this perceived deficiency of U.S. law may be used as a justification for measures aimed at diminishing U.S. dominance of the data processing hardware, software, and services market.[46] W. Spieker of the German Federation of Trade Unions, whose constituency may be threatened by U.S. dominance of the data processing and telecommunications industries, has called for "priority [to] be given to regulations preventing so-called 'data havens.' "[47]

III. Current Approaches to the Harmonization of Privacy Laws

In order to prevent what Harvard professor Oswald Ganley has called the "strangulation" of transborder data flows due to over-regulation,[48] a number of international organizations have moved toward the creation of treaties or less formal mechanisms for reconciling the differences between data record regulation in Western countries. These mechanisms aim to reconcile the legitimate need for protection of personal privacy with the need to maintain transnational recording and processing systems of personal

43. Ibid.
44. Turn, "Privacy Protection," p. 78-79.
45. Epperson, "Contracts for Information Protection," p. 164.
46. Fishman, "Introduction to TDF," p. 12.
47. W. Spieker, "Data Protection and the Trade Union," in Organisation of Economic Cooperation and Development, *Transborder Data Flows and the Protection of Privacy*, Proceedings of Vienna, Austria symposium, 20-23 Sept. 1977, p. 234.
48. Oswald Ganley, *Transborder Data Flow: Competition or Strangulation?* (Medford, MA: Edward R. Murrow Center of Public Diplomacy, 1979).

data. In the 1970s, the OECD, the Council of Europe, and the European Economic Community (EEC) began studies on the development of international norms for data protection. Despite differing legal mechanisms for the protection of personal rights of privacy in the United States and Western Europe, there has been "remarkable agreement" on the "ultimate content" of norms governing privacy protection.[49] That is to say that the objectives of U.S. and European law are roughly the same; only their scope, and the administrative and adjudicatory mechanisms designed to address the problem are different. There remains a need to devise regulations that might reduce potential problems with conflicting laws to a "manageable size."[50] Some have seen this as a problem of reconciling the loss of control of data when it is transferred to another country with the potential loss of economic benefits caused by the restriction of the data-holding entity.[51] The complexity and variety of interests involved in the problem have led different organizations to take different positions on the necessity for a binding international agreement.

The OECD was one of the major organizations to investigate the problem. A series of hearings, committee studies, and symposia held by the OECD led to the formulation of the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Guidelines).*[52] The *Guidelines* were formulated in order to "help to harmonise national privacy legislation" by serving as a "basis for legislation" in countries yet to enact privacy legislation and as principles that can be incorporated into existing national laws.[53] Created merely as recommended paths for future legislation, the *Guidelines* are not binding on OECD members. Some European representatives on the Expert Group on Transborder Data Barriers and the Protection of Privacy (Expert Group), the group which formulated the *Guidelines*, believed this would be insufficient. They favored, instead, the signing of a legally enforceable treaty rather than merely the adoption of common guidelines.[54] This legalistic approach was taken by the Council of Europe in concurrent negotiations on a data protection treaty.

Justice Kirby of Australia, Chairman of the Expert Group, described the central principle behind the privacy guidelines as the "golden rule" of data protection law: "The right of the individual, in general, and with some exceptions specifically provided for, to have access to personal data about himself."[55]

---

49. Sieghart, "Lacuna and Overlap," p. 230.
50. Ibid., p. 225.
51. Turn, "Privacy Protection," p. 79.
52. Organisation of Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1 October 1980.
53. OECD, *Guidelines*, Preface.
54. Kirby, "Basic Rules," p. 45.
55. Ibid., p. 29.

Sieghart sees the *Guidelines* as a means of avoiding what he calls "lacuna" problems (the potential for the creation of data havens, states with lax data protection laws) and "overlap" problems (the potential for the creation of inconsistent and overlapping legal systems) that would frustrate the legitimate transfer of data between countries.[56]

The *Guidelines* attempt to achieve an international consensus between the standards of privacy law and countries' willingness to allow the free flow of data across national boundaries. The most important part of the document is Paragraph 18, which limits interference with transborder data flow to instances involving data exported to a country which does not yet "substantially" observe the *Guidelines*. Nations are encouraged to consider the impact of their laws on the effectiveness of privacy protection in other countries. The *Guidelines* require, however, that countries avoid developing laws that exceed the requirements of privacy protection. Paragraph 18 is the *quid pro quo* which nations, such as the United States, receive in return for adapting domestic laws to meet the sensitivities of their data trading partners. U.S. support for the *Guidelines* is an admission that the free flow of information is not an absolute value.

The *Guidelines* establish eight basic principles to be embodied in national laws:

(1) *Collection Limitation:* Data should be obtained through "lawful and fair means" and limits placed on the type of data which may be collected.[57]

(2) *Data Quality:* Data should be accurate, complete, up-to-date, and "relevant to the purpose for which it was collected."[58]

(3) *Purpose Specification:* The intended purpose of the data should be specified to the data subject.[59]

(4) *Use Limitation:* Data should not be disclosed except with the consent of the data subject or by the authority of law.[60]

(5) *Security Safeguards:* Data should be protected against abuse through "reasonable security safeguards."[61]

(6) *Openness:* Data collectors should follow a general policy of openness with regard to the existence, purposes, and nature of a personal data file.[62]

(7) *Individual Participation:* Individuals should have the right to determine if data on them is held by a data collector, to obtain that data, to challenge the validity of that data, and to have such data deleted or corrected.[63]

---

56. Sieghart, "Lacuna and Overlap," p. 228.
57. OECD, *Guidelines*, para. 7.
58. Ibid., para. 8.
59. Ibid., para. 9.
60. Ibid., para. 10.
61. Ibid., para. 11.
62. Ibid., para. 12.
63. Ibid., para. 13.

(8) *Accountability:* The data collector should be accountable for complying with privacy law.[64]

The *Guidelines*' basic principles are generally vague. The collection limitation principle, for example, merely requires that data, where "appropriate," be acquired with the "knowledge or consent" of the data subject. No definition of "appropriate" is delineated. In addition, the *Guidelines* merely specify that limits be placed on the type of data, avoiding the question of what those limits should be. Furthermore, no position is taken in the *Guidelines* on the controversy over what constitutes sensitive data. Similarly, in the purpose specification principle, distinctions are not drawn between what is and is not acceptable use of collected personal data — the *Guidelines* requiring only that the data subject be informed of the purpose. In legislation under consideration in Australia, the intended purposes of data must also meet criteria of social acceptability.[65] The *Guidelines* also give little assurance to individuals that they may gain access or make changes to data held on them. The individual participation principle implies that a challenge to stored data can be denied, and though the *Guidelines* require that the individual may challenge this denial, no specific criteria upon which this denial can be based are outlined.

One significant principle of privacy law absent from the *Guidelines* is a sunset provision — a limit on the period of time certain types of data can be held. Effective sunset provisions previously have been enacted, such as in the U.S. Fair Credit Reporting Act, whereby records must be destroyed or erased after a specific period of time (usually 7 years).[66] With a few exceptions, such as for medical data, a similar sunset provision in the *Guidelines* would help ensure that inappropriate and outdated information would be automatically removed from files. Instead, the individual is responsible to seek out and have removed any data which is no longer up to date. Justice Kirby, in a summary of the principles he feels central to privacy law, asserted that personal data ought to be archived, destroyed, or modified so that the individual involved cannot be identified once the data's "purposes have expired."[67]

In order to protect against inadvertent or accidental disclosure of personal data, the *Guidelines* require that personal data be protected by "reasonable security safeguards."[68] Observers complain that there are no means of assuring absolute security in most of the circumstances common to transborder

64. Ibid., para. 14.
65. Kirby, "Basic Rules," p. 46.
66. 15 U.S.C. sec. 1681c.
67. Kirby, "Basic Rules," p. 58.
68. OECD, *Guidelines*, para. 10.

data flows.[69] The private use of increasingly sophisticated encryption techniques, which are the most common methods used to limit potential disclosure during the telecommunications phase of transborder data operations, have recently been threatened by government restrictions. Though international telecommunications are to some degree already protected by the International Telecommunications Convention of Malaga-Torremolinos (1973),[70] additional agreements on computer/communications security may be required in the future.[71]

The *Guidelines*' proposed principles reflect a compromise between European and American approaches to privacy law. The European approach is generally stricter than the U.S. law, extending privacy to both persons and corporate entities. The *Guidelines* are to be applied to "personal data, whether in the public or private sector."[72] Compared to this provision, existing U.S. law fails to meet the ideal proposed by the *Guidelines,* since not all American private data banks are covered by U.S. law. However, the *Guidelines* define "personal data" as data relating to an "identifiable individual," thus limiting coverage to natural persons — a distinct tilt toward the American approach.[73]

The *Guidelines* do not attempt to harmonize the implementation of these laws; no suggestions are made for common means of enforcement or common principles of individual redress. Instead, the *Guidelines* simply promote the self-regulation of data collectors, suggesting that member countries encourage the creation of codes of conduct. The implementation paragraphs clearly tilt toward the American approach, except for a requirement that there not be any "unfair discrimination against data subjects."[74] This statement could be interpreted as applying to the U.S. Privacy Act, because of its limitation of coverage to U.S. citizens and permanent residents.[75]

The increasing tendency toward the registration and licensing of data collectors is not addressed by the *Guidelines.* Many nations require the registration of each proposed data bank that will contain data on individuals, and nations such as Sweden require government approval before allowing the export of data to data banks based abroad.[76]

Other implementation questions such as the severity of sanctions imposed on data abusers are not addressed by the document. The U.S. Privacy Act limits penalties to civil action and fines up to $5,000 for U.S.

69. Turn, "Privacy Protection," p. 82.
70. *International Telecommunications Convention, Malaga-Torremolinos,* 25 October 1973, T.I.A.S. 8572, para. 22.
71. Turn, "Privacy Protection," p. 82.
72. OECD, *Guidelines,* para. 7.
73. Ibid., para. 1(b).
74. Ibid., para. 19(e).
75. Ibid., para. 19(e).
76. The Swedish Data Bank Statutes (1973:289) of 11 May 1973, Section 1.

government employees who willfully disclose unauthorized data.[77] Some European laws, however, apply harsher penalties for unauthorized disclosure, ranging from one to five years in jail.[78]

While the *Guidelines* were being drawn up, the Council of Europe drafted an international treaty also addressing the problem of data protection. The *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention)* was drafted in response to the perceived need for further clarification of the right of privacy outlined in Article Eight of the European Convention on Human Rights, because of the changes wrought by the new technologies.[79] The *Convention* has many elements in common with the *Guidelines*.[80] The essential difference between the two documents is that the Council of Europe *Convention* is intended to be adopted as binding by states. Unlike the *Guidelines*, it requires that signatories modify their national laws to meet its specifications.

There was a great deal of collaboration between the drafters of the two documents. Most of the principles found in the *Guidelines* can be found in the Council of Europe *Convention*. There are, however, a number of differences. The Council of Europe treaty allows signatories to extend their protection from natural persons to legal persons and other groups — a distinct tilt away from the U.S. approach toward that of some European legislation.[81] The Council of Europe *Convention* is more specific as to the types of data considered sensitive — it lists religious opinions, racial origins, health and sexual matters, and criminal convictions as data not to be recorded on file unless the domestic law provides sufficient safeguards.[82] The *Convention* does include the sunset data principle.[83] Lastly, the Council of Europe *Convention* does not require that measures be taken to alert the data subject that data is being collected — a significant departure from the human rights emphasis of the document.

In one aspect, the Council of Europe treaty is more specific than the *Guidelines* — requiring that signatories designate authorities to aid foreign residents in their pursuit of their privacy rights.[84] An individual of signatory A could request the aid of signatory B's designated authority in accessing

77. Privacy Act of 1974, 5 U.S.C. sec. 552a, (e) (1).
78. The penalties in the French law (78-17) range from 6 months to 5 years (Chapter VI); in Germany, from 1 to 2 years; and in Sweden, from 1 to 2 years. (Section 21).
79. European Convention on Human Rights, Rome, 4 November 1950, Article 8.
80. Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*, Strasbourg, 28 January 1981, as reproduced in International Legal Materials 20 (March 1981).
81. Council of Europe, *Convention*, art. 3(2) (b).
82. Ibid., art. 6.
83. Ibid., art. 5(e).
84. Ibid., arts. 13-17.

a record on that individual believed to exist in a data bank located in country B. No charges, other than those commonly applicable to citizens of country B, could be levied on the individual making the request. The designated authority of country B could only refuse to provide access if it contravened the standard sovereignty, security, public order, and rights-of-others clauses.

Since its approval in January 1981, the *Convention* has been ratified by two nations (Sweden and France). Entry into force may take place in 1984, if three more nations ratify the treaty (Norway, Luxembourg, Austria, and Iceland are in the process of ratification).[85]

Though the treaty is open to non-members of the Council of Europe by invitation, it is unlikely the United States will sign it. The Council of Europe *Convention* is far more stringent than existing U.S. law, and it seems unlikely that such a sweeping plan for regulation of the private sector would be approved by any American administration, especially the Reagan Administration, with its current emphasis on deregulation. Multinational corporations prefer the *Guidelines* to the *Convention* because of its direct promotion of the concept of self-regulation, and its common law "wait and see" attitude.[86] Though nine of the twenty-one members of the Council of Europe have signed the treaty,[87] it is likely to be of lesser importance than the *Guidelines* because of its failure to arrive at a consensus that might be supported and perhaps joined at some future date by the United States.

The policy of the United States during the past two administrations has been to support and promote the free flow of information. During the Carter Administration, National Security Advisor Zbigniew Brzezinski called for trade in information goods and services to be free of barriers, conducted in an atmosphere of mutual respect.[88] In January 1981, departing Commerce Secretary Philip Klutznick called on the U.S. private sector to take "appropriate affirmative action to implement" the *Guidelines,* warning that failure to do so might "increase the prospects for the imposition of conditions, limitations, and administrative difficulties" on U.S. corporations operating data banks with links abroad.[89] Incoming Secretary Baldridge noted that it was "in the interests of U.S. corporations" to follow and promote the *Guidelines.*[90]

---

85. Tom Riley, "Data Commissioners Review International Problems," *Transnational Data Report* 6 (December 1983): 417.
86. Ganley, "Competition," n.p.
87. Frank Kuitenbrouwer, "The Global Data War," *World Press Review* (November 1981), p. 54.
88. Fishman, "Introduction to TDF," p. 10.
89. Bushkin, "The Threat," p. 10.
90. Ibid., p. 11.

IV. Other Solutions and the U.S. Response

Are the *Convention* or the *Guidelines* the only possible solutions? Efforts toward legal harmonization are aimed at solving three problems: 1) ensuring the rights of privacy of those on whom records are kept, 2) reducing the incompatibility of differing domestic laws and thus reducing the costs borne by data collectors, and 3) preventing the use of privacy problems as a justification for the restriction of transborder flows of personal data. Only the second of these two problems, the cost of incompatible laws, seems to be presenting a serious problem at this time. The other issues seem to be of more potential concern in the future.

America's corporate concerns have tended to focus on how to provide the requisite features in new personal data systems to meet the differing requirements of European nations.[91] In testimony before a congressional subcommittee, a vice-president of Eaton Corporation estimated that such inconsistencies increase the cost of data processing operations by 30 percent. Many corporations support efforts toward harmonization of laws because of the resulting decreased cost of compliance with consistent laws. An Intergovernmental Bureau of Informatics (IBI) survey found strong support for harmonization among multinational corporations.[92]

Problems of legal inconsistency between the United States and civil law European nations in matters of data protection have not yet been the official cause of any restrictions on the transborder flow of data. At a recent meeting of data protection commissioners from seven European nations and Canada held in Stockholm, the main subject of concern was how data protection agencies would handle files on individuals maintained by such non-commercial organizations as Interpol and Amnesty International.[93]

Thus, outside of increased costs due to inconsistent data regulation between European countries, the essential issues of transborder data flows and privacy law harmonization lie in the area of heading off future disagreements, and ameliorating the problems faced by those whose privacy rights may be abused. There are several relatively small steps the United States could take to help prevent and lessen these potential problems.

There seems to be little reason why the Privacy Act of 1974 does not extend coverage to non-citizens of the United States. If the same rights currently attributed to citizens were given to non-citizens, with careful exceptions in the area of national security, a potential complaint of European privacy rights proponents could be eliminated. Thus one privacy-related justification for the termination or restriction of personal data flows between

---

91. Martin D. J. Buss, "Managing International Information Systems," *Harvard Business Review* 60 (September/October 1982): 155.
92. Riley, "Data Commissioners," p. 419.
93. Ibid., p. 417.

Europe and the United States could be eliminated. Limited gestures such as this would provide evidence that the United States has no intention of becoming a data haven and does respect the rights of citizens of other nations.

The U.S. administration should continue to promote self-regulation by corporations affected by this issue. If U.S. corporations carefully and visibly promote their own acquiescence to European laws and to the *Guidelines*, a source of future problems might be lessened. Already, a group of business executives who attended the Stockholm data protection commissioner's meeting were openly interested in promoting compliance with the Council of Europe *Convention* when it comes into force and curious about the application of data protection law to new videotext and electronic mail services.[94]

David K. Flaherty of the Privacy Project at the University of Western Ontario has proposed that the United States establish a Privacy Protection Commission, akin to the Civil Rights Commission, to conduct investigations and articulate privacy problems.[95] Again, such an approach might serve to indicate the United States' concern with the human rights aspects of the privacy protection issue. The research function of the proposed commission would serve as a means of detecting future issues before they become serious problems. Thus, some of the beneficial "preventative" aspects of the civil law approach could be realized in the United States without dramatically altering the U.S. legal framework for privacy protection.

Flaherty's plan envisions the scope of the Privacy Commission as limited to public sector oversight, but it seems that this is an unnecessary limitation. The Privacy Commission could also serve as a means of detecting potential sources of private sector problems as well. It might aid European data protection boards in their pursuit of the rights of foreign citizens, by persuading American companies to comply with reasonable European privacy requests. Though these proposed powers would not satisfy all the Council of Europe *Convention* requirements for a designated data protection authority, they would move considerably in that direction.[96] By meeting the Europeans half way, the United States could avoid European requests that the United States establish a more formal data protection board along the lines of the European licensing and registration boards. In a nation the size of the United States, with large numbers of private record-keeping systems, a licensing or registration scheme would be unworkable.

In return, the United States might suggest that some of the European nations relax their registration and licensing requirements. According to

94. Ibid.

95. David H. Flaherty, "The U.S. Needs a Privacy Protection Commission," *Transnational Data Report* 6 (September 1983): 341.

96. Council of Europe, *Convention*, art. 13.

Farnsworth, TDF registration and licensing requests can take as long as eight months to process, thus creating a clear disincentive to establishing data processing networks and systems that involve transborder data flow.[97] In addition, J. K. Williams of IBM United Kingdom, Ltd. notes that the significant costs of European data regulation have not come in the area of responding to data subject requests, but in the area of documentation to meet government regulations.[98] Williams proposes that registration be less concerned with minor details and limited to general subject areas of record-keeping.[99]

G. Michael Epperson suggests that, rather than relying simply on applying the *Guidelines* to their operations, corporations ought to utilize a contract approach to achieve "functional equivalency" between the laws of the data-exporting state and the U.S.[100] Such a contract would specify the rights and duties defined in the exporter's law. After approval by the data exporter's data protection board, the contract would give standing to the board to sue for breach of contract. However, this type of arrangement places the duty of enforcement on the exporter's board, forcing the board to undertake legal action in a foreign country at potentially burdensome costs. The expense involved might significantly restrict the board's legal challenges to only the most pressing concerns. Epperson also notes that U.S. courts might be unwilling to enforce foreign criminal sanctions.[101]

Generally speaking, major objections by Americans and some Europeans to sweeping data protection legislation and the immediate establishment of international conventions regulating TDF hinge on the feeling that too much has been done too soon. This view emphasizes that regulation ought to be implemented only after significant problems have been demonstrated. Only if such difficulties arise will there be sufficient experience to judge the pros and cons of such sweeping and restrictive legislation.

Though the United States may eventually become a party to a binding international agreement on the privacy issue, such an agreement at this time would be premature.[102] The danger of bureaucratic impediments to the development of efficient and beneficial technology is too great and our experience with the international law of privacy is too shallow. Yet the necessity for some kind of international privacy law remains; it is what Justice Kirby called "the price that has to be paid for the defense of important individual liberties."[103]

97. Farnsworth, "An American's View," p. 287.
98. J. K. Williams, "European Data Protection — a Business Viewpoint," *Transnational Data Report* 5 (April/May 1982): 156.
99. Ibid.
100. Epperson, "Contracts for Information Protection," p. 157.
101. Ibid., p. 174.
102. Fishman, "Introduction to TDF," p. 23.
103. Kirby, "Basic Rules," p. 64.