Northwestern Journal of International Law & Business

Volume 4
Issue 1 *Spring*

Spring 1982

Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations

Garry S. Grossman

Northwestern Journal of International Law & Business

Spring 1982
Volume 4
Number 1

Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations

*Garry S. Grossman**

INTRODUCTION

The merger of computer and communications technologies in the past two decades has revolutionized information processing throughout the world.[1] The most recent telecommunications advances make possible direct international transfers of sensitive personal data via

* Former Information Policy Coordinator, Office of Health Research, Statistics, and Technology, U.S. Department of Health and Human Services; A.B. (Computer and Communications Sciences), 1973, University of Michigan; M.Sc. (Computer Science), 1977, University of Toronto; J.D., 1982, National Law Center, George Washington University; presently associated with Fried, Frank, Harris, Shriver & Kampelman, Washington, D.C.

1 See, for example, *Computers in Communications: A Ratings Survey*, DATAMATION, July 1981, at 100, for evidence of how extensive the merger of the two technologies has become. The interdependence of the technologies has generated new application areas for both. The use of computers has changed communications industries by vastly increasing the possible speed and complexity of transmissions. Without the quantum leap into automated message transmissions that computer technology made possible, the international flow of data would, at best, be limited by the previous technological capabilities.

For the computer industry, as well, the marriage has been a welcome one. Not only have many new markets been created by the automation of communications systems, but computer technology itself has been spurred to new heights of speed and complexity in order to meet the demands of message switching systems.

computer-satellite links.[2] Computerized data bases containing commercial information identifying citizens of one country are now routinely transferred to and stored in another, often without the knowledge of the individuals identified in the data. Numerous European countries have enacted data protection legislation with the avowed intent to protect their citizens from the improper use of personal information that is transferred extranationally.[3] These data pro-

---

2 These advances are well beyond the stages of research and development, and have reached the general public. Examples include proposals for direct satellite to home television transmission, and the phenomenal growth of satellite usage in communications companies such as Comsat and AT&T.

3 One of the salient characteristics of the transborder data flow issue is the rapidity with which it has become a problem of major concern.

At the present time, the following national legislation has been enacted. Austria: Data Protection Act, No. 565, 1978 Bundesgesetzblatt für die Republik Österreich [BGBlÖ] 3619 (Aus.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 8 [hereinafter cited as Austrian Data Protection Act]. Canada: Canadian Human Rights Act, ch. 33, 1976-1977 Can. Stat. 887 (1977). Denmark: Private Registers etc. Act, No. 293, 1978 Lovtidende for Kongeriget Danmark [LKDk] A 833 (Den.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 6 [hereinafter cited as Danish Private Registers Act]; Public Authorities' Registers Act, No. 294, 1978 LKDk A 839 (Den.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 7 [hereinafter cited as Danish Public Registers Act]. France: Act 78-17 of Jan. 6, 1978, Concerning Data Processing, Files, and Liberties, 1978 Journal Officiel de la République Française [J.O.] 227, 1978 Recueil Dalloz-Sirey, *Législation* [D.S.L.] 77 (Fr.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 4 [hereinafter cited as French Data Processing Act]; Act 78-22 of Jan. 10, 1978, Concerning Access by and Protection of Consumers in the Area of Certain Credit Operations, 1978 J.O. 299, 1978 D.S.L. 84 (Fr.). Luxembourg: Law Governing the Use of Name-Linked Data in Data Processing, Document Parlementaire No. 2131 (1979) (Lux.). New Zealand: Wanganui Computer Centre Act 1976, No. 29, 1976 N.Z. Stat. 168, *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 9; Wanganui Computer Centre Amendment Act 1977, No. 83, 1977 N.Z. Stat. 1091, *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 10. Norway: Personal Data Registers Act, No. 48 (June 9, 1978) (Nor.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 5 [hereinafter cited as Norwegian Privacy Act 1978]. Sweden: Data Act, No. 289, 1973 Svensk Författnings Samling [SFS] 518 (Swed.), *as amended by* Act of June 12, 1979, No. 334, 1979 SFS 727 (Swed.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 2 [hereinafter cited as Swedish Data Act]. United States: Freedom of Information Act, 5 U.S.C. § 552 (1976), *as amended by* Government in the Sunshine Act, 5 U.S.C. § 552b (1976); Privacy Act of 1974, 5 U.S.C. § 552a (1976); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, §§ 1100-22, 92 Stat. 3697 (codified in scattered sections of 12, 31 U.S.C.); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-81t (1976); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1976); Tax Reform Act of 1976, § 1202a, 26 U.S.C. § 6103 (1976). West Germany: Federal Data Protection Act, 1977 Bundesgesetzblatt I 201 (W. Ger.), *reprinted in* 5 COMPUTER L. SERV., app. 9-5.2a, No. 3 [hereinafter cited as West German Data Protection Act].

Most of the above statutes have also been reprinted in EXPERT GROUP ON TRANSBORDER DATA BARRIERS AND THE PROTECTION OF PRIVACY, WORKING PARTY ON INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, OECD DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY, COMPILATION OF PRIVACY LEGISLATION IN OECD MEMBER COUNTRIES, No. I.C. 4 (DSTI/ICCP/79.11) (1979). For additional materials, including reports of national commissions and study groups, see Novotny, *Transborder Data Flows: A Bibliography*, 16 STAN. J. INT'L L. 181, 188 (1980).

tection laws prohibit the export of such information under certain specified conditions.

This perspective focuses on one of the more troublesome issues surrounding national restrictions on international data flow: the emergence of corporate privacy laws. In several data protection laws recently enacted in Europe, restrictions have been imposed that limit the transborder transfer not only of data identifying individuals, but of data that identifies corporations as well. These particular statutes also appear to give corporations the right to inspect other corporations' data bases in which they are identified, like similar provisions in most other data protection laws granting individuals the right of access to records identifying them. To some degree, all data protection laws impose a burden on multinational corporations and others who seek to move data transnationally.[4] The laws containing corporate privacy provisions, however, may have a particularly severe long term impact on United States trade.[5] Data protection laws containing only individual privacy provisions do not impose this extra burden. Thus, it is important to examine and compare the burdens imposed by, and the justifications offered for, the enactment of individual and corporate privacy provisions in order to determine if the additional burden on trade is warranted. Such an inquiry requires a delineation of the differences between individual and corporate privacy interests from both a legal and a policy perspective.

An examination of the individual and corporate privacy interests through their differing common law development, statutory treatment, and impact on international trade suggests that the primary rationale underlying corporate privacy has little to do with privacy. Rather, the rationale appears to be one of furthering the national economic development of the country enacting the legislation. Moreover, the trade barriers erected by corporate privacy provisions cannot be justified by the same interests that rationalize individual privacy provisions. Corporate privacy provisions, therefore, should not be included in data protection laws. To avoid the international trade barriers generated by corporate privacy provisions, nations that have enacted or are considering the enactment of data protection laws must be persuaded to es-

---

[4] Although multinationals are not the only parties affected by data protection laws, they are the parties most acutely affected. *See infra* Section II.

[5] The apocalyptic view expressed by Bank of America's Director of Telecommunications Regulatory Policy, B.C. Burgess, that "if we can't move information, we go out of business" may oversimplify the problem, but it serves to highlight the current serious concern of multinational companies. Sanger, *Multinationals Worry As Countries Regulate Data Crossing Borders*, Wall St. J., Aug. 26, 1981, at 1, col. 4.

chew such provisions in their own laws. This important result can be achieved by negotiating aggressively for international agreements that encourage free trade. It may also be achieved by adopting a more accommodating policy in the United States through enacting stronger individual privacy protection than currently exists.

I. THE ECONOMIC STAKES

In order to understand the impact that foreign privacy laws have on the United States, it is necessary to recognize the immense economic stakes involved. As the world leader in information technology, the United States exports more than twelve billion dollars per year in computer and communications equipment alone.[6] Data processing services account for untold billions more in revenue. These exports appear as computer systems and telecommunication services throughout the world, forming the technological network which enables the transborder flow of data in diverse situations. For example, a typical export might involve computer terminals or other "peripheral equipment" needed to link into an existing data base system (such as a credit verification service), in which the central processing unit and principal storage media remain in the United States. The transborder data flows form the link between the remote equipment and central data storage. In addition, exports might include data processing equipment purchases by a foreign subsidiary of a multinational corporation, in order to process and transmit data back to its parent corporation in the United States.

The importance of developing sophisticated information technology resources has been recognized by foreign governments. In Europe and Japan, government-industry cooperation is viewed as a necessary ingredient to eradicate American dominance in international information markets and to alter the balance of economic power.[7]

---

[6] *International Data Flow: Hearings Before the Subcomm. on Gov't Information and Individual Rights of the House Comm. on Gov't Operations*, 96th Cong., 2d Sess. 325 (1980) (statement of Henry Geller, United States Department of Commerce). The computer-communications equipment export market must be distinguished from the export of data processing and communications services, which gives rise to most of the problems addressed in this perspective. While sales of equipment usually involve relocation of the equipment to the user's site, sales of data processing and communications services, in contrast, usually involve the transmission of data from its origin (or initial user) to some remote location. The advantages possessed by particular providers of data processing services may stem from economies of scale, the complexities of the processing involved, or other factors. *See also* HOUSE COMM. ON GOV'T OPERATIONS, 96TH CONG., 2D SESS., INTERNATIONAL INFORMATION FLOW: FORGING A NEW FRAMEWORK, THIRTY-SECOND REPORT, H.R. REP. NO. 1535 (1980).

[7] For more details of actions taken by the Japanese and European governments to promote

It is within this economic framework that transborder privacy issues must be addressed, for it has become apparent that legislation avowedly intended to protect personal privacy can be extremely effective in interfering with international commerce. These non-tariff trade barriers can prohibitively increase the cost of doing business, inhibit technological development, or even exclude foreign competition entirely.[8] Although European data protection laws were passed with legitimate concern for privacy protection, it must be recognized that there are significant nationalistic motives behind much of the privacy legislation as well.[9] In response to these measures, the United States must counter its vulnerability to non-tariff trade barriers[10] by seeking an international agreement that, *inter alia*, distinguishes the privacy interests of individuals from those of corporations.

The elimination of existing (and impending) corporate privacy provisions in data protection laws would enhance free trade by eliminating trade barriers that make protected domestic markets inaccessible to United States and other external competition. Such elimination would not damage the privacy interests of individual citizens—the true intended beneficiaries of such laws. In some circumstances, the removal of corporate privacy provisions would benefit trade by reducing private sector costs of complying with government regulation of data practices. More important, in many instances the detrimental effects

---

their data processing industries, see Solomon & Grossman, *Tax and Non-tax Policies to Promote Capital Formation: Stimulating High Technology in the 1980's*, 1 AM. J. TAX POL'Y 63 (1982); SUBCOMM. ON TRADE, HOUSE COMM. ON WAYS AND MEANS, 96TH CONG., 2D SESS., HIGH TECHNOLOGY AND JAPANESE INDUSTRIAL POLICY: A STRATEGY FOR U.S. POLICYMAKERS (Comm. Print 1980); SEMICONDUCTOR INDUSTRY ASSOCIATION, THE MICROELECTRONIC CHALLENGE 11-15 (1981); Durniak, *U.S. Beachhead for Japanese Computers is only the Start*, ELECTRONICS, Mar. 27, 1980, at 113; Gregory, *Success in Innovation is the Main Problem Ahead*, 106 FAR EASTERN ECON. REV., Dec. 14, 1979, at 50; *The Japanese Challenge*, DUN'S REV., Aug. 1980, at 80.

8 Government-industry cooperation is by no means limited to the various protectionist policies described in this paper. In Japan, the United States fiercest competitor, government assistance to the semiconductor industry has been committed and extensive. The Japanese government has altered the industry's debt-equity ratio by making extensive funds available at favorable interest rates. The impetus to capital formation has been a major factor in the rapid growth of the Japanese share of the world computer market. *See* SEMICONDUCTOR INDUSTRY ASSOCIATION, U.S. AND JAPANESE SEMICONDUCTOR INDUSTRIES: A FINANCIAL COMPARISON (1980).

9 *See infra* notes 58-80 and accompanying text.

10 Access to information is often taken for granted in the United States. Senator George McGovern recognized this vulnerability in 1977 when he remarked that an information-dependent country such as the United States could be attacked by "cutting off contact between the headquarters and the overseas branches of a multinational firm [by] taxing telecommunications crossing borders [or by] building information walls" between nations. *See* McGovern, *The Information Age*, N.Y. Times, June 9, 1977, § A, at 21, col. 2.

of corporate privacy statutes may totally exclude United States firms from certain markets. The elimination of these legal impediments would reopen markets, and introduce the quality and cost advantages that accompany increased competition.

The United States should advocate a position that both supports appropriate individual privacy protection and minimizes the burden on international trade. Such a position must meet two likely criticisms from the nation's principal trading partners. First, some Europeans are concerned that individual privacy is inadequately protected in the United States. As discussed *infra*, in Section V, United States privacy legislation, unlike its typical European counterpart, reflects a sector by sector approach that leaves privacy protection to contractual resolution by the parties involved. Where United States privacy protection laws fail to cover part of the field—as is the case with individually identifiable medical records—the enactment of appropriate legislation would respond to a pressing domestic need. Such laws could also encourage continued international data flow by providing legal protection for foreign individuals identified in medical records data bases located in the United States.[11] Thus, one might envision a statute that addressed itself to all domestically stored medical records, not solely those involving United States citizens. Such a statute would provide any individual with both the rights of access to and modification of records identifying him or herself, and the necessary standing to seek a judicial remedy if records were disclosed without consent. Although another remedy might provide more effective protection for foreign citizens, the provision of standing to sue in United States courts for private judicial enforcement is consistent with existing privacy legislation that seeks both to minimize direct government regulation and to encourage uniform data handling practices throughout the United States with respect to medical records. This approach would perhaps serve to assuage some European concerns.

Second, United States policymakers must take a stand in the current international controversy over the legitimacy of corporate, as opposed to individual, privacy protection. The corporate privacy interest is conceptually different from and inherently weaker than the individual privacy interest. As is discussed *infra* in Section III, the individual privacy interest has a lengthy history, with firm roots in the United States Constitution's orientation toward the protection of individual rights. The enforcement of corporate privacy rights has no similar justifications. It is, as envisioned by its advocates, a vehicle for govern-

[11] *See infra* note 89 and accompanying text.

ment regulation of business. Corporate informational privacy ultimately is an issue of commercial policy and should be addressed as such.[12] Evidence of the individual-corporate distinction also may be seen in the grossly disparate consequences of enforcing the two types of provisions. Enforcement of individual privacy rights has a substantial impact on how a company does business by preventing its use of specified information outside the country. The corporate privacy right, however, with its attendant spectre of providing competing corporations (or the government) with access to data bases that identify competitors, presents problems of a much greater magnitude. Free trade itself is threatened by the statutory creation of a corporate privacy right.

A notable, if small, step toward international accord has been taken with respect to individual privacy through a recent agreement reached by members of the Organization for Economic Cooperation and Development on guidelines for individual privacy.[13] Ultimately, however, the regulation of international data flow is an issue of economic and commercial policy. Within that context, the clarification of what are legitimate privacy interests, and what are not, will help clarify the larger debate over what is essentially a question of world commerce.

II. Types of Transborder Data Flows

An examination of individual and corporate privacy interests must commence with the observation that restrictions on data transfers in the private sector differ significantly from restrictions on transfers involving government records. Public sector data flows are qualitatively different from private sector data flows because, in the public

12 Confusion often arises over conflicting uses of the terms "privacy," "confidentiality," and "security." The working definitions used here have been adopted by the Association of Data Processing Service Organizations. Privacy is defined as a social issue involving questions of what data should be collected and stored, and to whom they should be released. Individual privacy and personal privacy are used synonymously to refer to these questions as they apply to natural persons, as opposed to corporate privacy, which refers to juristic persons, including associations, institutions, and corporations. Confidentiality, on the other hand, is a subset of the privacy issues concerning the protection of information from unauthorized disclosure, modification, or destruction. Data security describes procedural measures taken to assure confidentiality. *See* Association of Data Processing Service Organizations, Inc. (ADAPSO), [U.S.] Guidelines on Security, *quoted in* Marks, *A Perspective on Information Policy, Privacy and Transborder Dataflow Restrictions*, 5 Computer L. Serv. § 7-5, art. 2, at 11 (1979). Questions of privacy and security can apply to manual as well as automated systems. *See* Noll, *The Interactions of Computers and Privacy*, 7 Honeywell Computer J. 163, 165 (1973).

13 For a more detailed discussion of the OECD Guidelines, see *infra* notes 104-114 and accompanying text.

sector, the government itself possesses the identifying data. A government is presumably capable of negotiating adequate protection for its citizens before it makes any data transfers to an entity outside of its jurisdiction. Thus, differences between the sectors call for separate legislative approaches.

In the public sector, transborder data flow may be initiated by either national governments or international agencies. When governments or agencies exchange data under bilateral agreements or multilateral treaties, the purpose of the transfer is usually to obtain information unavailable domestically for its own administrative and regulatory purposes. For example, the United States Food and Drug Administration and the Centers for Disease Control exchange with their foreign counterparts health data identifying manufacturers and institutions.[14] International data transfers for purposes of law enforcement, social welfare, and commercial regulation are also commonplace.[15] Although no two national data systems have yet been linked for direct automated transmissions, the reasons for this are political rather than technical.[16] Before such automated transfers can be initiated, the governments involved must resolve questions of disclosure and unauthorized use of the transferred data. Thus, regulatory difficulties are less likely to occur in the public sector than in the private sector. The parties controlling the data are national governments, which can presumably protect the interests of their own citizens in such transactions.[17]

---

14 Ironically, the United States Congress may have made exchanges of this type potentially injurious to information confidentiality. Under the Freedom of Information Act, information exchanges between the United States and foreign governments which do not involve national security matters are subject to public release upon request.

15 Pipe, *Work Paper on Transborder Information Flows: Requirements for a New International Framework*, 9 LAW & COMPUTER TECH. 17, 21 (1976).

16 The technical problems have been solved for the most part as witnessed by already extant corporate and governmental systems. *See infra* text accompanying notes 18 and 21.

17 It is in the realm of intergovernmental exchanges of data that a contractual approach would provide the most feasible way to protect citizens' interests. To the extent that the "consideration" in such exchanges—personally identifiable data—would be mutual, sufficient disincentives to breaching the agreement would exist on both sides. *See* Note, *Contracts for Transnational Information Services: Securing Equivalency of Data Protection*, 22 HARV. INT'L L.J. 157, 162 (1981).

One obstacle that must be overcome, however, is the problem that might occur if one of the countries has domestic legislation that is inconsistent with the receipt of foreign data. For example, the Freedom of Information Act may require the release of foreign data received by a United States government agency from a foreign government, even if a promise of nondisclosure was made by the agency, except where the data falls under one of the Act's exemptions. 5 U.S.C. § 552(a)(1976). In this instance, additional legislation would probably be necessary to eliminate the problem.

Most intergovernmental data sharing occurs under the auspices of United Nations affiliated agencies. These agencies collect personally and institutionally identifiable data under agreements with various participating nations. Interpol, for example, collects, processes, and discloses to its members extensive data that identify individuals suspected of criminal activity.[18] The World Health Organization also gathers data in confidence from member countries identifying the manufacturers of drugs and medical devices. When conflicts of law arise from inconsistent national data protection laws, they tend to have little impact on international agencies because the agencies are not subject to the domestic laws of their host countries.[19] Generally, therefore, public sector transborder data flows are removed from the arena of trade policy questions. Such is not the case with respect to private sector transborder data flows.

Private sector transborder data flows present extensive and problematic privacy questions. Multinational corporations in the communications, banking, credit, insurance, tourism, entertainment, and employment services industries are extensively involved in international trade, and such trade requires these corporations to transfer information from country to country.[20] Additionally, domestic corporations transacting business with foreign concerns regularly transmit sales information back to their home countries. In either case, the rewards of commercial efficiency, and, ultimately, commercial viability itself, depend upon centralization in one country of all business-related data, including data identifying foreign individuals and corporations.

Commercial data transferred across national borders can be classified into two categories. The first category consists of information identifying individual persons. It is typified by a commercial transaction in which a client has business dealings with a foreign enterprise or subsidiary domiciled in his or her own country. Swissair, for example,

---

18 F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE 260 (1975).

19 The unique legal position of international agencies necessitates rather unique operational restrictions. Typically, any limits that are to be imposed on their data processing activities must be written into the agency charter. Presumably, data processing contractors with an international agency would be subject to the domestic data protection laws in their host country.

20 Of course, international trade itself is hardly a recent phenomenon. However, the modern-day multinational corporation has required, as an essential part of its infrastructure, access to information about its business operations in many countries. Automated management information systems can help to process the immense amount of data needed to operate any large business. Whether the data are stored in one central location at corporate headquarters or elsewhere as part of a network system, they will cross national borders at some time. *See* Pipe, *supra* note 15, at 21.

like many other corporations, maintains its headquarters and central computer facility in one city (Zurich), but has on-line terminals in many major cities throughout the world which are linked to its headquarters.[21] Commercial transaction data transmitted to a central computer invariably includes information identifying individual persons. Transborder data flows will also occur when the internal records of a multinational corporation are collected and processed at a central location outside the country in which the data were collected. Intracorporate information stored internationally usually includes employee records (such as medical and payroll files), client records (such as mailing lists), and other information identifying individuals. Although employees usually are granted access to their own records, they have neither the legal right of access nor the right to prevent release by their employer once the data have been removed to another country.[22]

The second category of commercial data consists of intracorporate records containing information identifying other corporations. This information may include details of competitors' products or sales, whether collected for business planning purposes or for potential litigation. Individuals are not identified but the competing corporations are named. It is this category that is covered by the corporate privacy provisions of data transfer laws. Although confidential commercial information identifying competitors, including clients, sales, and other economic indicators, is unquestionably valuable to its owner, it is fundamentally different from sensitive employee medical records because its impact is purely business related. Naturally, if the intracorporate records do not identify individuals or corporations, privacy questions do not arise.[23] However, technical problems[24] such as data security

---

21 F. HONDIUS, *supra* note 18, at 246.

An "on-line" system is one that provides processing while a user waits for the response. For example, an airline reservation system that can generate information regarding current seat availability on a flight is on-line, while a biweekly payroll run is not.

The significance of on-line systems is that the transborder data flow must occur instantaneously as part of the transaction involved. Any inspection of the data leaving a country must be automated, if it is not totally to destroy the utility of the on-line system.

22 The situation could be complicated even further if access to the employee records were sought legitimately by the employer's government. In United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3rd Cir. 1980), United States government access to employee medical records was permitted by the court for epidemiological research. While a corporation might attempt foreign storage of the medical records in order to prevent access by the employee's government, the corporation would be unable to prevent access by the government of the foreign country where the records are being stored, conceivably producing a politically untenable solution.

23 In practice, any attempt to distinguish comprehensively between corporate and individually identifiable data being transmitted out of a country creates insurmountable administrative problems. One approach that might be taken would be to create an overseeing agency. The administrative agency could delegate responsibility for compliance respecting all data transfers

will remain a primary concern where the information constitutes intellectual property,[25] even if individuals or competitor corporations are not identified therein.[26]

Private sector transborder data flows may also include information intended for non-commercial use. International labor, professional, and religious associations have networks for intraorganizational data transfers, which may create problems similar to those of commercial data transfers. Examples include release of mailing lists without the consent of members or membership lists which themselves denote religious or political affiliation. Individual privacy concerns regarding non-commercial data are similar to those for commercial data. The only significant distinction is that individual affiliation is usually completely voluntary, thus affording the individ-

---

made. If data inspection were performed manually, the agency could at best expect to examine templates identifying the types of data involved or else sample a very small portion of the data being transmitted. From a technical perspective, a single portal for all data entering and leaving the country might afford the power totally to terminate the data exchanges of a company; however, as compared to more traditional means of enforcement, such as an injunction, such a measure would be exorbitant in cost, and onerous to the parties affected.

24 Technical considerations revolve basically around three areas: data security, data quality, and auditing/compliance. In the area of data security, significant advances have been made. Technology now exists for, *inter alia*, backup storage of data, alternate communications links, secure software, user identification, and data encryption.

The maintenance of data quality has also advanced as the state of the art in data base system design has become more sophisticated. Measures to protect data quality include controls over who may alter data, restrictions on the types of data retained, and requirements that data be timely.

With respect to auditing and compliance, as noted *supra* in note 23, automated solutions may prove to be technically infeasible. The use of formal software verification computer programs as a means of ensuring compliance is still in its infancy and is not yet capable of proving the correctness of any but very small systems. In addition, "shadow systems" that are designed to mislead auditors and circumvent legal requirements are, at present, very difficult to unearth.

For further information on technical problems, see Turn, *Privacy Protection and Security in Transnational Data Processing Systems*, 16 STAN. INT'L L. J. 67, 80 (1980); Turn, *Technical Aspects of Privacy Protection*, Proc., 78 COMPSAC 229 (1978).

25 Issues arising out of the automated text processing capabilities will create problems undreamed of a decade ago with respect to intellectual property stored in computers. De Sola Pool & Solomon have argued, correctly, that current legal concepts of copyright will create more problems than they will solve when applied to computer communications. De Sola Pool & Solomon, *Intellectual Property and Transborder Data Flows*, 16 STAN. INT'L L.J. 113 (1980).

The above authors also suggest that copyright law and regulation do not present a practical solution to transborder data flow conflicts. In arguing that traditional legal approaches could be better adapted than copyright law to cope with these problems, de Sola Pool & Solomon suggest that solutions based on practice in the 1970s will be irrelevant in the 1980s. *Id.*

26 Where the intellectual property is a patent or copyright that has been validly issued by numerous countries (as is common practice today), a security breach may cause no subsequent damage. However, if trade secrets (which may include commercial lists or even computer software) are obtained through a breach of security, the ensuing competitive damage may be irreparable.

ual an option to terminate his affiliation with the organization involved. Commercial credit and employment relationships, however, do not offer the individual similar leverage.

III. Foundations of Individual and Corporate Privacy Interests

In the debate over the enactment of data protection legislation, advocates of protectionist non-tariff trade barriers have overlooked the differences between corporate and individual privacy interests.[27] This oversight has placed an unmerited veil of legitimacy around attempts in some nations to add corporate privacy provisions to existing individual-oriented data protection laws in an effort to foreclose competition from United States multinational corporations by blocking information flow.

The privacy interest of individuals should be seen as fundamental, deriving its importance from the societal norms we call human rights. In contrast, the establishment of a corporate privacy interest arises out of decisions about economic policy. No true "privacy" interests are at issue here. Thus, the rationale for protecting corporate privacy is distinctly different from the rationale for protecting the privacy rights of individuals. In light of the significant burden on international commerce that accompanies corporate privacy legislation, these differing rationales must be closely examined to determine if the burden is justified.

To discern the difference between the corporate privacy interest and the individual privacy interest, the following three assertions must be examined. First, historically, the two interests have been treated differently in both the common law and statutory law. Second, the rationale for corporate privacy rests upon a wholly separate foundation from that of individual privacy. Third, an inspection of the two respective classes (individuals and corporations) reveals that corpora-

27 One example of this confusion occurred in 1971, when the International Association of Lawyers submitted several draft resolutions on privacy in transborder data flows to the Council of Europe, each proposing substantially equivalent privacy protection for individuals and for businesses (Draft Articles for an International Convention for the Protection of Personal and Industrial Privacy; International Agreement for the Protection of the Personal and Industrial Spheres). The failure of the proposals to identify the unique characteristics of corporate privacy generated misunderstanding regarding the two interests. The proposals' attempt to remold the traditional subjective right of privacy into an objective privacy area failed because it oversimplified the issues. However, the "objectivized privacy area" concept took root, and evolved into the present day concept of data protection, that is, the regulation of data handling practices in order to protect ultimately the privacy of individuals. *See* F. Hondius, *supra* note 18, at 96-97.

tions have an entirely different reason for seeking access to data bases that identify them than do individuals.

The common law foundations of individual privacy in the United States are fairly recent. For both social and technological reasons, individual privacy was of little significance in early America. Before the advent of mass media and telecommunications, personally identifiable information was rarely available from sources other than those close to the individual. In small towns and rural areas, a person invariably knew who possessed personal information about him or her. The source of the data, therefore, was usually immediately known, or if not, then easily traceable.[28]

In 1890, Samuel Warren and Louis Brandeis proposed the recognition of a common law tort action for invasion of privacy.[29] In time, the common law came to recognize privacy interests against appropriation of personal data, intrusion on personal affairs, public disclosure of private information, and defamation.[30] The common law, however, never provided sufficient protection against the abuse (as opposed to the appropriation) of personal data, allowing damages only where economic loss could be proven.[31]

In comparison, the United States Constitution delineates the privacy interests of individuals only indirectly. Most relevant to data processing are the right to associational privacy,[32] the right to possess beliefs free from governmental intrusion,[33] and the right to be free from unreasonable searches and seizures.[34] Although the protection of these interests does not provide adequate personal protection against data abuse, it does impose general limits on government use of data.[35]

---

28 For further discussion, see A. MILLER, THE ASSAULT ON PRIVACY, ch. 5 (1971).

29 Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

30 The common law right to privacy is described in detail in A. MILLER, *supra* note 28, ch. 5.

31 That damages would be limited to economic loss from misuse of data is not surprising. Prior to the advent of automated data processing, the manual processing of data was so cumbersome that it was difficult to even conceive of a data processing service industry, much less the possibility of extensive data theft.

32 U.S. CONST. amend. I, *construed in* NAACP v. Alabama, 357 U.S. 449 (1958) (recognition of right to be protected against state compulsion to disclose affiliation with the NAACP).

33 U.S. CONST. amend. I, *construed in* Schneider v. Smith, 390 U.S. 17 (1968) (a screening program for American merchant vessels was held unconstitutional where questions were asked that impinged upon first amendment freedoms but were concerned with appellant's beliefs, not his conduct).

34 U.S. CONST. amend. IV, *construed in* Katz v. United States, 380 U.S. 347 (1967) (tapping telephone conversation while petitioner used telephone booth was an illegal search and seizure violating petitioner's right to privacy).

35 The Supreme Court at least recognized the threat of possible abuse from automated data processing in Whalen v. Roe, 429 U.S. 589, 605 (1977), where a state planned to create a data base containing information identifying all users of prescription drugs. The dictum in the case

An expansion of statutory privacy protection from the original common law and constitutional bases has occurred in recognition of the fact that, as the Privacy Protection Study Commission noted, "in America today, records mediate relationships between individuals and organizations."[36] Unlike nineteenth century America, current disclosures of confidential information cannot be easily traced back to those few people in the community (banker, doctor, lawyer, etc.) that hold such information. Today, a data processing manager who indiscriminately releases personal data will not be held legally accountable to the victim of the abuse absent a statutory remedy. Even the existence of such a remedy, however, if limited to domestic abuses, would be of little avail when the data are already stored in a foreign jurisdiction.[37]

The rationale for individual privacy protection rests upon the societal values of dignity and uniqueness of the individual—i.e., human rights. As computer technology has diffused, it has become cost-efficient to create massive registries containing information about individuals. Thus, individuals seeking to prevent abuses of computerized information identifying them must first locate the data bases where they are personally identified. This concern was articulated in the 1973 report of the United States Department of Health, Education, and Welfare Advisory Committee on Automated Personal Data Systems.[38] The HEW report outlined five basic components of the right of individual data privacy:

1. No secret systems should exist.
2. An individual should be guaranteed access to examine records identifying him or her.
3. Personally identifiable data should be used only for the purposes for which they were collected.
4. An individual should be ensured the right to correct inaccurate personal data.
5. Organizations should take measures to ensure the accuracy and security of personal data controlled by them.[39]

---

suggests that without any safeguards on disclosure, the constitutional right to privacy might have been violated.

36 PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 3 (1977).

37 Once the data have been removed from the country, the foreign jurisdiction may afford no legal remedy to a foreign citizen seeking relief. Furthermore, additional duplication of the data may have already occurred in the interim with removal to other jurisdictions.

38 ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION, & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 4 (1973).

39 *Id.* These principles later became a cornerstone of the Privacy Act of 1974. The annual report of Privacy Act systems of records makes this information publicly available. *See infra* note 82.

Although the individual privacy interest rests upon human rights, the human rights rationale also requires that privacy protection not be overbroad.[40] Overbroad data protection laws encroach upon freedom of expression.[41] Data protection laws that restrict removal of individually identifiable data from a country are especially vulnerable to this criticism. For example, data export restrictions on the transfer of nonsensitive portions of intracorporate employee records and the transfer of personal data with the express consent of the data subject would be an unjustifiable protection of individual privacy.[42]

Furthermore, data protection laws that limit data flow may block access to scientific and technical expertise. In developing countries, for example, data transfer restrictions erected to stimulate the domestic computer-communications industry by preventing data from leaving the country may backfire by denying domestic businesses access to state-of-the-art techniques. In this complex situation, many developing countries may feel that they must make a Hobson's choice between blocked technological progress and continued economic dependence. This dilemma presents an excellent opportunity for the United States to improve relations with these nations by cooperating in the search for compatibility between individual privacy protection and competitive free trade.

A final rationale supporting the existence of the individual privacy interest becomes apparent from an enumeration of the harms that individual privacy provisions are designed to eliminate. Absent such provisions, individuals may suffer personal indignities, unwarranted deprivation of the rights and privileges of citizenship, unfair denials of credit, or even incarceration because they are unable to assess and to correct inaccurate data identifying them. Moreover, an individual needs the protections provided by privacy statutes because of the individual's relative lack of bargaining power against the large institutions controlling the data that identify him or her.

Unlike the individual privacy interest that has evolved historically through common law and constitutional interpretations, the corporate privacy interest has little precedent to support it. Until the recent

---

40 The opposing conclusion was reached regarding human rights issues in Gotlieb, Dalfen & Katz, *The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles*, 68 AM. J. INT'L L. 227, 257 (1974), *reprinted in* 5 COMPUTER L. SERV. § 9-7.5, art. 1, at 32.

41 For a more detailed discussion of the balance between freedom of expression and the right to privacy, see A. MILLER, *supra* note 28, at 205-06.

42 One illustration of nonsensitive portions of an employee record might include work locations, managers' names, and technical skills available to the corporation.

emergence of several European statutes with corporate privacy provisions, such an interest had not been recognized.

It should be noted that narrowly construed constitutional grounds do exist to support an extremely limited corporate privacy interest. In the United States, first amendment rights of expression have been upheld for corporations, although the scope of the protection is narrower than that for individual freedom of speech.[43] Constitutional and legal traditions in Germany and Austria also encompass juristic persons; nevertheless, the constitutional bases there for corporate privacy are much narrower than for the individual privacy interest. It has been suggested that a broad constitutional basis for corporate privacy should exist as a means for protecting individual privacy.[44] However, individual privacy—as evidenced by the vast majority of extant laws—is best protected by statutes sensitive to the adverse impact directly felt by the individuals affected. In any case, such an argument does not address the treatment of data that identify competing institutions, rather than individuals.

The extension of privacy rights in the data protection arena to include juristic persons ostensibly protects a corporation by preventing competing corporations from abusing information in their data base that identifies it. Yet, an examination of the impact of this protection on most corporations and other institutions reveals that corporate privacy laws hardly would be desirable. To extend principles of individual privacy to the corporate sphere by enforcing a right of access among corporations holding commercial information about each other could damage competition. One commentator, noting the recent passage of such a provision in Norway,[45] observed that:

> [Corporations] will be required to register and/or license all data bases they maintain regarding each other, to allow other entities, even competitors, to inspect, challenge, and demand corrections or deletions of data; and to grant other companies the right to limit dissemination and/or use of data regarding them unless notification has been given. Furthermore, the transborder data flow of information relating to entities themselves will be subject to the same potential restrictions that can be applied to personal data on individuals. The potential impact on marketing, product development, and pricing, and on competition in general is

43 *See* First Nat'l Bank v. Bellotti, 435 U.S. 765 (1978) (expression of corporation's views were constitutionally protected even where it could not be proved that the issues materially affected the corporation's business).

44 F. HONDIUS, *supra* note 18, at 100.

45 Norwegian Privacy Act 1978, *supra* note 3, § 1. For relevant text, see *infra* note 79.

staggering.[46]

As stated above, an individual benefits from access rights to inspect and correct data bases containing personally identifiable information about him or her. If, however, the information identifies a corporation instead of an individual, it will not benefit that corporation to grant it access rights similar to those granted to an individual. With respect to corporate privacy, the protection of human rights is not at issue. Rather, the interests and the consequences are purely economic. Reciprocal rights of access would be highly anti-competitive since whatever competitive advantage a corporation gained from obtaining access to its competitors' records regarding itself would be more than offset by forced disclosures from its own records.

In contrast, corporate privacy protection from indiscriminate access and public disclosure by the government may be desirable. For example, American hospitals that request assistance from the Centers for Disease Control do not want their identity disclosed.[47] Many voluntary disclosures to governments may be made available only when an institution is promised confidentiality in return. The National Center for Health Statistics, for example, has legislative authority to promise that the names of institutions obtained in its surveys will not be released without the consent of the identified institution.[48] More generally, the Trade Secrets Act provides that no federal employee may disclose any confidential commercial information that has been collected by the federal government unless specifically authorized by law.[49]

However, a policy that protects data which have been confidentially disclosed to further a government purpose needs less justification than a policy that restricts intra-corporate transmission of data that

---

46 McGuire, *The Information Age: An Introduction to Transborder Data Flow*, 20 JURIMETRICS J. 1, 5-6 (1979).

47 An analogous, but unrelated situation has arisen under the rubric of inverse Freedom of Information suits. In such cases, a corporation may challenge the intended release of data by the government as a result of some third party's Freedom of Information Act request. *See* Chrysler Corp. v. Brown, 441 U.S. 281 (1979); Department of Air Force v. Rose, 425 U.S. 352 (1976); National Parks & Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974).

48 Public Health Service Act, 42 U.S.C. § 242m(d) (1976); see *infra* note 65 for text of statute.

49 18 U.S.C. § 1905 (1976). Section 1905, in pertinent part, provides:

> Whoever, being an officer or employee of the United States or of any department or agency thereof, publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment . . . which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; . . . shall be fined not more than $1,000, or imprisoned not more than one year, or both; and shall be removed from office or employment.

have been privately generated for competitive business purposes. The recent corporate privacy provisions adopted in Norway not only authorize government licensing and inspection of data, but seemingly impose the same export restrictions that are imposed on data identifying individuals. The true beneficiaries of such a statute would be the domestic industries and national governments seeking to impede the business of multinationals in their countries. Essentially, then, corporate privacy in the data protection arena is no more and no less than a vehicle for erecting protectionist commercial policies.

IV. Justifications Offered for Non-Tariff Trade Barriers

Governments that impose privacy laws which act as non-tariff trade barriers offer a variety of justifications for their policies. Developing countries often cite American cultural dominance and a lack of independence from the United States economy as reasons for attempting to limit the influx of American products and services. In developed countries, an additional factor is present. These countries realize that their economic success in the next half century depends upon wresting the markets for data processing and services away from the grip of American businesses. These rationales do not justify the protection of privacy *per se* for either individuals or corporations. Rather, they are commercial reasons for fostering national economic development, which is the primary motivation behind corporate privacy laws. Protectionist justifications have also been offered to buttress human rights rationale for individual privacy protection.

Nations yet to enact individual privacy legislation,[50] in particular the developing countries, may desire to retain control over domestic data and data processing. The importation of data processing services and consequent exportation of data may be seen by these countries as an intrusive United States presence, capable of imposing alien standards on them. Developing nations are concerned that persons making administrative business decisions from the United States based on foreign-source data may not be aware that they are imposing a cultural bias on the countries affected by their decisions. For example, the criteria used for granting and revoking credit may differ widely between a developing country and the developed country where the credit decisions are made. But since the decision is made at the corporate headquarters in the developed country where the data base is maintained,

[50] A complete list of all nations that *have* enacted privacy or data protection legislation is included *supra* in note 3. Others are presumed not to have acted although discussions are currently ongoing in many nations.

its standards form the basis for credit decisions in the developing country.

Even when the two countries have much in common, as do Canada and the United States, information technology has a cultural impact.[51] Many standardized aptitude tests, for example, are developed and graded in the United States. When the tests are administered in Canada, they impose a bias against Canadian students by assuming detailed knowledge of United States history and culture.[52] Between the United States and a Third World country the contrast is even sharper.

The problems faced by a country which is information poor country relative to the United States are not unlike those faced by a "one-crop" nation. As long as remote data processing services cost less than the same services procured domestically, the developing country remains technologically underdeveloped, waiting for its domestic market in data processing products and services to evolve. Meanwhile, its own data processing industry fails to develop because there is little demand for domestic data processing products. The technological disparity is so complete that data processing users in developing countries often find it less expensive to contract for data processing services that use satellite technology to communicate thousands of miles back to the United States than to procure, implement, and maintain their own systems.[53] The continual export of raw data for processing elsewhere may ultimately, stunt other domestic industries that owe their growth to data processing. Demand for data processing personnel may subsequently stall and the ancillary growth in support industries experienced in the developed countries may only materialize slowly.[54]

Many developed nations, albeit for different reasons, also are defensive of United States dominance in data processing and services. In western Europe and Japan, it has become axiomatic that information

---

51 Science and technology may undermine religious teachings and social mores. An interesting portrayal of these effects is described in Bowler, *Will Science and Technology Bring Conflict Within Third World Countries?*, 57 SCIENCE FORUM 12 (1977).

52 Gotlieb & Katz, *Work Paper on Issues Associated with the Transborder Flow of Personal Information*, 9 LAW & COMPUTER TECH. 3, 12 (1976).

53 Privacy legislation that restricts data flow out of the country can assist the domestic data processing industry as effectively as import tariffs do. Tariffs operate by altering the relative prices of domestic and foreign products and services in favor of domestic industry. Data export legislation is less subtle: domestic goods and services are favored because dealing with foreign companies is, in essence, declared *malum prohibitum*.

54 For more information on the rapid growth of the industry and a general introduction, see McGuire, *supra* note 46.

control is the key to political and economic security.[55] Regardless of how information-rich a country may be, its sovereignty is endangered to the extent that its information resources are controlled extra-jurisdictionally. For example, the data processing service used by the Fire Department of Malmo, Sweden, stores architectural firefighting information in a data base located in Cleveland, Ohio.[56] Consider the potential hazard should technical problems or even a hostile act in the host country lead to a communications failure. The difficulties are sufficient to give pause even when personally identifiable data are not involved.

This is not to suggest that isolationism is preferable to interdependence. Rather, it is simply to note that interdependence has a cost which is more keenly felt by the other developed nations than by the United States. The cost is minimal, however, when compared with the economic gains possible through unrestricted international trade. Corporate privacy laws that restrict trade are strategems in pursuit of isolationist national economic growth and not in defense of a justifiable interest in privacy.

V. Recent National and International Developments

The recent evolution of privacy protection laws in Europe and the United States reflects markedly different philosophies between nations. In the United States, legislation has generally focused on provisions for self-enforcement through the American judiciary.[57] In contrast, most European countries have imposed direct statutory limits on data handling by regulating private sector practices. The different approaches not only reflect varying views of the appropriate role of government, but have also made uniformity of privacy protection more difficult to achieve.

European data protection laws typically create a governmental commission with specified executive and judicial powers to regulate domestic data practices. The Swedish Data Bank Statute[58] was the

55 *See, e.g.*, McGovern, *supra* note 10.

56 Burnham, *United States is Worried by World Efforts to Curtail Flow of Information*, N.Y. Times, Feb. 26, 1978, § A, at 1, col. 3. The example demonstrates the extent of international interdependence, and just how essential foreign stored data bases may be to domestic stability, whether or not they contain data identifying individuals.

57 *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1976).

58 Swedish Data Act, *supra* note 3. Many of the statutes cited in this paper have also been reprinted in Office of Telecommunications, U.S. Dep't of Commerce, Selected Foreign National Data Protection Laws and Bills (1978). Portions of the Swedish act reprinted in the following footnotes are representative of the language used in most of the European laws. As noted in the text, the provisions of the laws are very similar.

first of these laws to regulate automated transborder data transfers. Its avowed legislative intent was to assure Swedish citizens that computerized data would be used only for the purposes for which they were collected. The act created the Swedish Data Inspection Board, a government agency with strong regulatory powers. The Swedish act requires the Data Inspection Board to discriminate among different types of data. The Board can deny permission to create any system of personal records by refusing to grant the necessary license.[59] The decision whether or not a license issues is based upon the kind and quantity of information to be collected.[60] For example, only under extraordinary circumstances will the Board grant a license to a private party seeking to collect or disclose data relating to health, religion, or other associational affiliations.[61] Furthermore, the statute gives individuals the right to locate, examine, and correct any records containing information concerning them.[62]

---

59 Swedish Data Act, *supra* note 3, § 2. Section 2 states:

A personal register may not be started or kept without permission by the Data Inspection Board.

The first paragraph of this section does not apply to personal registers established according to a decision by King or Parliament. Before such a decision is taken the Data Inspection Board shall be heard.

60 *Id.* § 3. Section 3 states:

The Data Inspection Board shall grant permission to start and keep a personal register, if there is no reason to assume that, with due observance of the regulations laid down pursuant to sections 5 and 6, undue encroachment on the privacy of individuals will arise.

At the appraisal whether undue encroachment may arise special attention should be given to the kind and quantity of personal information meant to be included in the register and to the attitude towards the register shown or expected from the individuals meant to be registered.

61 *Id.* § 4. Section 4 states, in pertinent part:

Permission to start and keep a personal register containing information that anyone is suspected of or convicted for a crime or has been subjected to coercive action . . . may not be granted . . . unless there are extraordinary reasons for this.

Permission to start and keep a personal register otherwise containing information about anybody's illness or state of health or information that anybody has received social assistance, treatment for alcoholism or the like, or has been the subject of proceedings under the Child Welfare Act or the Foreigners Act, may not be granted to a person other than an authority which is by law or statute responsible for keeping a record of such information, unless there are special reasons for this.

Permission to start and keep a personal register containing information about anybody's political or religious views may be granted only where there are special reasons. This shall not, however, apply to a personal register that an association wants to keep of its own members.

62 *Id.* §§ 8, 10, 22. Section 8 states, in pertinent part:

If there is reason to suspect that personal information in a personal register is incorrect, the responsible keeper of the register shall, without delay, take the necessary steps to ascertain the correctness of the information and, if needed, to correct it or exclude it from the register.

If a piece of information, that is corrected or excluded, has been handed over to a person other than the individual registered, the responsible keeper of the register shall, at the request of the individual registered, notify the receiver concerning the correction or the exclusion . . . .

Section 10 states, in pertinent part:

The German Data Act,[63] passed in 1977, is similar to its Swedish counterpart. It, too, creates a central authority with licensing power over all private and public data bases. Personal data from secondary (i.e., indirect) sources are subject to the same strict requirements that encompass primary data. The remedies prescribed by the Swedish, German, and most other European data protection laws involve both administrative and judicial enforcement through data inspection boards. Fines and imprisonment may be imposed to enforce rights of access and correction. The boards then act in a judicial capacity when hearing administrative appeals. Anyone illegally procuring access to, changing, or deleting records is subject to prosecution for "data trespass."[64] In addition to statutory criminal enforcement provisions, Sweden has created a private cause of action to protect data from abuse.[65] This private cause of action differs from common law privacy actions in the United States because the scope of data encompassed under the Swedish law is much greater. Furthermore, in Sweden the private cause of action is an alternative to enforcement by the Data Inspection Board. In the United States, however, the private cause of action is the sole avenue for relief.

More important from the standpoint of international trade, these European data protection laws exert control over information flowing out of the country. The controls may apply to data identifying individuals or may limit removal of data identifying any juristic person, that is, corporations and institutions as well. The legislation of three European countries regarding only individuals will illustrate.

At the request of an individual registered the responsible keeper of the register shall as soon as possible inform him of the personal information concerning him in the register. When an individual registered has been thus informed, new information need not be given to him until twelve months later.

Information according to the first paragraph of this section shall be given free of charge to the individual . . . .

Section 12 states:

Should a responsible keeper of a register cease to keep a personal register the Data Inspection Board must be notified. The Data Inspection Board shall prescribe how the register should be dealt with.

63 West German Data Protection Act, *supra* note 3.

64 Swedish Data Act, *supra* note 3, § 21. Section 21 of the Swedish act provides that:

Any person who, without authorization, effects access to recordings for ADP or unduly alters or obliterates such information or includes it in a register will be sentenced for data trespass to pay a fine or to a term of imprisonment not exceeding two years, if the perpetration is not punishable by the Penal Code . . . .

Section 1 of the German act states that the purpose of the statute is to "ensure against the misuse of personal data during storage, communication, modification, and erasure (data processing) and thereby to prevent harm to any personal interests that warrant protection." West German Data Protection Act, *supra* note 3, § 1.

65 Swedish Data Act, *supra* note 3, § 21. For relevant text, see *supra* note 64.

Sweden is a typical example. The Swedish Data Inspection Board is authorized to forbid any removal of data from the country if it concludes that the recipient nation's privacy safeguards are inadequate.[66] In one incident prior to passage of a similar privacy act in Germany, the Swedish Data Inspection Board denied permission to Siemens, a German based corporation, to consolidate its Swedish employee records with the remainder of its employee files in Germany.[67] In another instance, a Swedish county government was denied permission to transfer a list of its county residents to a British firm for data processing because the Swedish Data Inspection Board perceived gaps in British privacy protection.[68] Since its enactment, application of the Swedish law suggests that information control itself is as important a by-product of the Swedish Data Act as is the protection of privacy.[69]

In both instances above, only individually identifiable data were being transferred. Thus, the corporation and government entity involved were adversely affected because of restrictions on individually identifiable data, and not because of restrictions on data identifying other corporations. The Swedish statute does not include a corporate privacy provision. The burdens on trade created by restrictions on individual data present problems whose resolution is not specifically addressed in this discussion.[70] It is clear, however, that the burdens will be unnecessarily compounded if transborder transfers of data identifying other corporations are treated analogously to individually identifiable data.

The German Act goes even further by legislating mandatory technical security requirements during data transmissions. Reasoning that

---

66 *Id.* § 11. Section 11 provides, in pertinent part:

> If there is reason to believe that personal information will be used for ADP abroad the information may be issued only after permission by the Data Inspection Board. Such permission may be given only if there is ground to believe that the issuance will not cause undue encroachment on privacy . . . .

67 Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-tariff Trade Barriers?*, 10 LAW & POL'Y INT'L BUS. 1056, 1072 (1978).

68 *Id.* at 1072 n.88.

69 For several examples attesting to the importance of control over information flows, see *id.* at 1072-73.

70 One interim solution that has been suggested is to provide data protection that is "functionally equivalent" to the standards mandated by a given European country through contractually established obligations on the part of a multinational corporation wishing to remove data from the country. *See* Note, *supra* note 17, at 175. This proposal represents little more than a "legal" method of complying with burdensome restrictions, while sidestepping much more important questions of law. The United States government should frame its data protection policy with an intent to reduce such burdensome international trade practices.

the data are still within German jurisdiction[71] during the moment they are being transferred out of Germany, the act requires the transmitting party to guarantee that access to or alteration of the data by a third party will be impossible during transmission. The requirement may well lead to end-to-end encryption of all data transfers.[72] If the recipient country has imposed different standards, even more significant problems may be created. For example, the British Post Office (BPO) forbids encrypted data transmissions from entering Britain if the BPO is not supplied with the encryption key.[73] However, by providing the encryption key, the transmitting party violates the German security requirement. Thus, data transfers that satisfy the German standard violate the British standard, and vice versa.

---

71 Unauthorized access during transmission is a problem that is distinct from questions of right to privacy. The distinction has been delineated in Gotlieb & Katz, *supra* note 52, at 7.

72 West German Data Protection Act, *supra* note 3, § 6(1) and Annex to § 6(1). Section 6(1) states:

> Persons processing personal data and referred to in Section 1(2) or acting on behalf of the persons or establishments referred to therein shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, and in particular the requirements set out in the Annex to this Act. Measures shall be required only if the cost involved is reasonable in relation to the desired level of protection.

The Annex to Section 6(1) includes more specific provisions:

> Where personal data are processed automatically, appropriate measures suited to the type of personal data to be protected shall be taken to ensure observance of the provisions of this Act:
> 1) Unauthorized persons shall be refused admission to data processing facilities which process personal data (admission control);
> 2) Persons employed in the processing of personal data shall be prevented from removing storage media without authorization (leakage control);
> 3) Unauthorized input into the memory and the unauthorized examination, modification or erasure of stored personal data shall be prevented (memory control);
> 4) The use by unauthorized persons of data processing systems from which or into which personal data are transmitted by means of automatic equipment shall be prevented (user control);
> 5) It shall be ensured that persons entitled to use a data processing system have access by means of automatic equipment only to the personal data to which they have a right of access (access control);
> 6) It shall be ensured that it is possible to check and to establish to which establishments personal data can be communicated by means of automatic equipment (communication control);
> 7) It shall be ensured that it is possible to check and establish what personal data have been input into data processing systems, by whom and at what time (input control);
> 8) It shall be ensured that personal data which are processed on behalf of third parties are processed strictly in accordance with the instructions of the principal (control of processing on behalf of third parties);
> 9) It shall be ensured that data cannot be read, modified or erased without authorization during their communication or during the transport of relevant storage media (transport control);
> 10) It shall be ensured that the internal organization of authorities or enterprises is suited to the particular requirements of data protection (organization control).

73 *See generally* Gotlieb & Katz, *supra* note 52, at 7 (domiciliary law mandating no secondary use of data without prior consent would be breached if foreign country allows unfettered access, even if no actual infringement of privacy occurred).

The French Data Act of 1978,[74] taking another tack, attempts to address behavioral issues that are seemingly unrelated to privacy. Although the French act shares many regulatory characteristics with the Swedish and German acts, it additionally prohibits any evaluation of human conduct based solely on information retrieved from an automated data base.[75] For criminal penalties to take effect, personal freedoms need not even be infringed, as long as some decision was based solely upon data utilizing automated technology. At least in France, it seems, this "beginning of legislation on social profiles" represents more an attack on automation *per se* than it does an enhancement of personal privacy protection.[76]

Although early European data protection legislation, including the three acts above described, focused exclusively on data that identified individuals, the most recent statutes have adopted corporate privacy provisions which include juristic persons (corporations, nonprofit institutions, etc.) as well. In Austria,[77] Denmark,[78] and Norway,[79] the recently passed data protection statutes, if read literally, require corporations to obtain licenses for all data bases that they maintain about each other, and to allow competitors the right to inspect them. The laws seemingly extend the inspection rights to include even corporate administrative files containing confidential commercial information.[80] This represents a significant departure from the already controversial

---

74 French Data Processing Act, *supra* note 3.

75 *Id.* art. 2. The statute states that:

> No court decision resulting in a judgment on human behavior may use as its basis automatically processed data which outline the profile or the personality of the person concerned.
>
> No administrative or private decision resulting in a judgment on human behavior may use as its basis automatically processed data which outline the profile or the personality of the person concerned.

76 Statement of Louis Joinet, French Ministry of Justice, in *Focus on France*, TRANSNAT'L DATA REP., Mar. 1978, at 3.

77 Austrian Data Protection Act, *supra* note 3, art. 2, part. 1, § 3(2).

Part 1, section 3(2) of Article 2 provides: "Persons affected: natural or legal persons or associations of persons under commercial law, about whom data are collected, processed or disclosed."

78 Danish Private Registers Act and Danish Public Registers Act, *supra* note 3, part. 1. Part 1, section 1.-(1) of the Private Registers Act provides:

> Registration comprising personal data where electronic data processing is used and systematic registration comprising private or financial data on any individual, institution, association or business enterprise or other data on any personal matter that may reasonably be demanded to be withheld from members of the general public, shall be permitted only subject to the provisions of Parts 1 and 2 of the Act.

79 Norwegian Privacy Act 1978, *supra* note 3, § 1. Section 1, in pertinent part, provides:

> The Act is applicable to personal data registers and to other facilities whereby personal information is utilized in certain types of activities.
>
> The term "personal information" shall mean information and assessments which are, directly or indirectly, traceable to identifiable individuals, associations or foundations.

80 *See* McGuire, *supra* note 46, at 4-6.

role of the data inspection board with respect to individual data. Any semblance of an attempt to protect individual privacy vanishes and is replaced by a governmental mandate to forage among private corporate data bases under the rubric of protecting other corporations' privacy. However, this is not privacy protection, but rather a heavy-handed form of commercial regulation.

In contrast, legislation in the United States has distinguished between individual and corporate privacy and has been limited to the former. The United States legislation covers specific sectors where individual rights are perceived to need protection rather than including the entire information processing industry. United States privacy statutes rely heavily on the judicially self-enforcing mechanism of private actions. Unlike the European laws, emphasis is given to the protection of individual rights rather than to the regulation of data and data practices as such. Thus, the European laws frequently distinguish between automated and non-automated data bases, while United States law typically applies to all systems of records. Due to the narrow sectorized approach to privacy legislation in the United States, anticompetitive corporate privacy provisions have not been enacted.

The most extensive United States privacy protection statute covers public sector data. The Privacy Act of 1974[81] limits disclosures from government data bases to previously published routine uses, and to the individuals identified.[82] Rights of access and correction are enforced through administrative appeals to the federal agency controlling the data and through the federal judiciary. A similar limitation in Canada extends privacy protection only when federal data systems are involved.[83]

In the United States, disclosures of specific classes of government records are expressly restricted by law. Of these, census and health

---

81 Privacy Act of 1974, 5 U.S.C. § 552a (1976).

82 In addition, the Federal Register annually publishes notices of all systems of records maintained by United States government agencies. *See, e.g.*, 45 Fed. Reg. 84,401 (Dec. 22, 1980), for part of the 1980 annual publication of Privacy Act systems of records within the Department of Health and Human Services. The notices include the following information: system name; security classification; system location; individuals covered by the system; categories of records stored; authority for maintenance of the system; purpose; routine users of the records; policies and practices for storing, retrieving, accessing, retaining, and disposing of records; safeguards of the system; system manager's name and address; notification procedures; record access procedures; contesting record procedures; record source categories; and exemptions from certain provisions of the Privacy Act.

83 Canadian Human Rights Act, ch. 33, Pt. IV, 1976-77 Can. Stat. 913, 914 (1976). Application 50 of Part IV states: "This Part applies to all federal information banks." "Federal information bank" is defined as "a store of records within the control of a government institution where any of the records comprised therein are used for administrative purposes." *Id.*

data are most stringently controlled.[84] At the National Center for Health Statistics, for example, any disclosure of personally identifiable data is specifically limited to the purpose for which they were collected, and may not be released under any circumstances without the identified individual's consent.[85]

However, in the private sector, United States legislation against abuse and disclosure of personal data is far narrower than in the European statutes. The principal legislation regulating these data practices is the Fair Credit Reporting Act.[86] This act grew out of abuse of credit records in the 1960s. It mandates accurate reporting of credit data, the right of access to credit records, and correction of inaccurate information. Remedies are provided through a private cause of action rather than a central enforcement agency.

There is little argument that one problem with the American approach is that it leaves gaps in the breadth of protection afforded. The shortcomings are not, however, due as much to difficulties in targeting legislation at a given sector (which, for example, was quite successfully accomplished with the Fair Credit Reporting Act), as they are to the complete absence of legislation in other sectors, such as medical records.[87] Thus, the overall scope of United States statutory protection is too narrow, although existing legislation may cover specific areas comprehensively. The United States has recognized the corporate/individual dichotomy, but by failing adequately to protect domestic indi-

---

84 13 U.S.C. §§ 8, 9 (1976). Section 8, in pertinent part, provides:

> (a) The Secretary may, upon a written request, and in his discretion, furnish to Governors of States and Territories, courts of record, and individuals, data for genealogical and other proper purposes, from the population, agriculture, and housing schedules prepared under the authority of subchapter II of chapter 5 . . . .

Section 9, in pertinent part, provides:

> (a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, may, except as provided in section 8 of this title—
>
> (1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or
>
> (2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or
>
> (3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports.

85 42 U.S.C. § 1306 (1976); 42 U.S.C. § 242m(d) (1976). Section 242m(d) (section 308(d) of the Public Health Service Act) provides, in pertinent part:

> No information obtained . . . [under the authorities of the National Center for Health Statistics] may be used for any purpose other than the purpose for which it was supplied unless authorized under Regulations of the Secretary . . . . [S]uch information may not be published or released in other form if the particular establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented . . . to its publication or release in other form . . . .

86 Fair Credit Reporting Act, 15 U.S.C. §§ 1681a *et seq.* (1976).

87 *See infra* note 89 and accompanying text.

vidual interests, has made itself vulnerable to protective foreign laws that unnecessarily burden commerce.

Soon after the passage of the Privacy Act, the Privacy Protection Study Commission was created to study the data privacy situation in the private sector and to make suggestions for legislation. The Commission recommended legislation in numerous areas where protection of individual privacy was nonexistent.[88] Despite recent congressional interest, these proposals have yet to be enacted into law.[89] Congressional inaction has international ramifications beyond the immediate domestic need for statutory protection. If other nations perceive a lack of United States commitment to further legislation, they may well respond by expanding further their own domestic restrictions on data flows to achieve the protection they desire.[90] Although it is still unclear which ultimate direction the 97th Congress will choose, United States economic interests abroad will be better served if Congress, following the philosophy of the existing United States privacy laws, enacts additional individual privacy protection, rather than if it continues to follow a path of inaction. Such legislation, if enacted, would maintain the dichotomy between individual and corporate privacy. No provisions for enforcing a corporate privacy right would be included, and a private cause of action would be created only in specific sectors. The proposal to protect the confidentiality of medical records, discussed above, is a good example of one sector where legislative action is appropriate. Although the American and European methodologies would continue to diverge, the United States would move closer to the European level of substantive individual protection. The current absence of a United States statute implementing a corporate right of privacy reflects a widespread concern with imposing an unjustifiable economic burden on commerce in the name of privacy protection.[91] This burden can be further minimized by fully protecting

88 Privacy Protection Study Commission, *supra* note 36.

89 H.R. 5935 & S. 503, 96th Cong., 1st Sess., 125 CONG. REC. H 11012, S1934 (1979) (medical records); H.R. 3409 & S.867, 96th Cong., 1st Sess., 125 CONG. REC. H1929, S3874 (1979) (research records). These bills addressed problems of confidentiality in medical records and in records gathered in the process of research. Provisions of the bills included rights to access and limitations on disclosure.

90 For details, see *supra* notes 3, 66-70, and accompanying text.

91 Congress opted to postpone more extensive regulation of individual privacy rights in the private sector until the impact of such legislation could be analyzed. S. REP. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 U.S. CODE CONG. & AD. NEWS 6916, 6934-36. It thus seems highly unlikely that a proposal for a corporate privacy right would be entertained by Congress in the foreseeable future.

individual privacy interests in the United States in an effort to allay European concerns.

The United States interest in protecting personal privacy and expanding international trade in information markets conflicts sharply with existing European data protection laws. The lead position of United States exporters of information technology is already threatened. It will erode further if the various federal agencies involved in international telecommunications and trade policy are not coordinated by a lead agency. United States participation in current international discussions on international data flow is of limited value if it is not actively supported by the present administration at home, as well as abroad. As an example of the extent to which the international situation could deteriorate, consider for a moment several options that have been suggested over the past decade in Canada, the United States closest trade partner.[92] The proposals materialized from concerns over the inadequacy of individual privacy protection in the United States. They share the intellectual seed from which the European corporate privacy concept has sprouted.

First, it was proposed that all organizations storing data on Canadian citizens in data banks outside the country be required to register with the Canadian government.[93] This approach, however, would erect no barriers to the actual flow of data, and thus do nothing to lessen the risk of abuses perpetrated in private, foreign data banks. Moreover, the proposal would increase the risk of governmental abuse of personal data since it would provide centralized access to the storehouses of such information.[94]

A second, more radical proposal, was to prohibit all foreign storage of personal data identifying Canadian citizens.[95] Such an outright ban would not only impose intolerable restraints on the freedom of expression, but also would present unsolvable enforcement problems. A third suggested solution was to create a domestic "library" consisting of duplicates of all personal data files transported out of Canada.[96] This would be prohibitively expensive, and, in any case, would fail to

92 Many of the approaches have been directly addressed in Canada over the past decade. *See* COMPUTER/COMMUNICATIONS POLICY: A POSITION STATEMENT BY THE GOVERNMENT OF CANADA 17 (1973); Gotlieb, Dalfen & Katz, *supra* note 40.

93 Gotlieb, Dalfen & Katz, *supra* note 40, at 24.

94 Gotlieb, Dalfen, and Katz argue that the national register raises serious public policy questions regarding the limits to be imposed on the intrusive powers of government, whether or not exercised in the name of protecting its citizens. The personal register would be yet another data bank that would require protective measures to prevent its abuse. *Id.*

95 *Id.* at 25.

96 *Id.*

achieve the presumed objective of regulating the type of information transferred.

In addition, it has been suggested that Canada might require foreign corporations to restructure their Canadian branches into independent Canadian subsidiaries, thus forcing all personal data bases to be under the control of the "domesticated" company.[97] Even disregarding the myriad business-related difficulties such a law would create, independent subsidiaries would probably still find ways to circumvent the restriction.

Several of these proposals—notably the "library" approach and corporate restructuring—suggest the potential for an emergent corporate privacy statute in Canada. At the very least, these two proposals, by failing specifically to address the difficulties arising from individually identifiable data, evidence a continuing confusion of individual and corporate privacy which might have been avoided by more extensive United States privacy laws. Although several of the suggested approaches would not even accomplish their purpose of retaining control over information exported from Canada, it is clear that any one of them could severely disrupt Canadian-American trade.[98]

For the United States, the importance of directing international attention to the transborder data flow problem is motivated by, *inter alia*, the commercial need for consistency in national laws. It is evident that international trade in data and data processing services may be severely handicapped if subjected to a panoply of national laws that are overly restrictive of data transfers. Minimizing overbroad privacy laws that can act as non-tariff trade barriers, thus, must be a high priority in United States participation in trade negotiations.[99] Data protection laws, whether corporate- or individual-oriented, create non-tariff trade barriers. Arguably the burden that accompanies corporate provisions differs only as a matter of degree from that accompanying individual provisions. The key distinction between the two interests, however, does not lie in the extent of the burdens generated. Corporate data laws are not aimed at protecting individual privacy interests,

---

97 *Id.*

98 Determining in advance exactly what the impact would be is not feasible due to the extensive interdependence of various sectors of the Canadian and American economies. Most importantly, the flow of information is usually tied to the flow of goods and services, and it is inevitable that restrictions on one would adversely affect the other.

99 Kirby, *Developing International Rules to Protect Privacy*, 12 LAW & COMPUTER TECH. 53, 56 (1979). International agreements may also delay the current trend toward taxing data transfers by the number of "bits" of data transmitted rather than the number of telephone lines leased. *Id.* at 57. A "bit" is technical terminology for a binary digit, i.e., the numbers zero or one in base two. This is the almost universal numbering system of automated data processing systems.

and therefore cannot be justified on that basis. Instead, corporate privacy laws serve as a means of regulating commerce between corporations and governments. Once this difference between corporate and individual provisions is recognized, the additional burden that accompanies corporate provisions becomes unjustifiable. Eliminating corporate provisions will be a major step toward minimizing the trade barriers generated by data protection laws.

For the countries that have enacted data protection legislation protecting individuals, an international solution is both necessary and appropriate.[100] The limited power of domestic privacy laws over extra-jurisdictionally stored data has caused some countries to turn to international law to try to impress stronger privacy protection on other nations.[101] An even greater impetus is the apprehension that in some jurisdictions no privacy laws at all will be enacted, creating "data havens" where personal information is stored to circumvent more stringent national laws elsewhere.[102]

International agreement holds the greatest promise of all potential methods for the eventual resolution of the data protection problems.[103] In negotiating such an agreement, corporate privacy provisions should be treated as a purely economic issue, that is, they should be treated as being only as justifiable as an opposing tariff. With respect to individual-oriented data protection laws, uniformity of data handling practices must ultimately be achieved for unrestricted trade in data and data processing services.

Strong United States initiatives are responsible, in part, for the focus of the Organization for Economic Cooperation and Development (OECD) Guidelines on Individual Privacy. The agreement, signed by sixteen of twenty-four OECD members in September,

---

100 *See supra* notes 71-73 and accompanying text.

101 *See* Gotlieb & Katz, *supra* note 52, at 2.

102 *Id.* at 3. The argument has more recently been leveled at the United States for advocating less protectionist privacy laws than certain European countries. *See* Emmett, *New TDF Concerns Surface*, DATAMATION, Feb. 1981, at 48. The suggestion that, from a human rights perspective, the policies of United States "data haven" are morally bankrupt for not protecting the privacy of its residents has more propaganda than substantive value when viewed in light of existing United States privacy legislation.

103 An examination of existing private international remedies suggests that they are an inadequate international solution. Traditionally, the primary barrier against bringing an international action in tort has been the absence of common law privacy protection. Even in countries such as the United States where constitutional law provides limited common law privacy protection, actions brought in extra-jurisdictional breaches would be defeated if brought outside of the United States. Gotlieb & Katz, *supra* note 52, at 13 n.16. Although the private international remedy may receive more favorable judicial treatment in the future, the inconsistency of domestic laws has made it evident that a broader approach is needed.

1980,[104] suggests voluntary guidelines for national legislation rather than a binding international convention.[105] Due both to the rapidly developing technology and to the fact that many nations have yet to enact any privacy legislation, a binding convention would probably have been premature. Voluntary guidelines identify privacy as a priority area where agreement is desirable, if not yet imminent. It is to be expected that those nations most enthusiastically supporting data flow restrictions will respond with much more zealous enforcement than the United States. Such is the flexibility—and inherent limitation—of nonbinding agreements that focus on precepts rather than implementation.

The cardinal principle of the guidelines is the individual's right to have access to any stored information that identifies him or her. As Justice M.D. Kirby,[106] coordinator of the OECD effort, stated during the negotiations, "If nothing else is achieved in domestic privacy protection and in international efforts to protect privacy in transborder data flows, then agreement about this right of access will be a most significant legal development."[107]

As agreed upon, the OECD Guidelines contain eight basic principles that may be summarized as follows. First, data collection should be limited to necessary information that is obtained by lawful and fair means. Where appropriate, the consent of the data subject should be obtained. Second, personal data should be accurate, complete, current, and relevant to the purposes for which they are to be used. Third, the intended uses of the data are to be specified at the time they are collected. Fourth, any disclosures of the data must either be compatible with the purposes for which they were collected or be authorized by law. Fifth, reasonable security safeguards should be taken against loss or unauthorized access, destruction, use, modification or disclosure of data. Six, no secret data should exist. A general policy of openness should be encouraged regarding the existence and the nature of all personal data held by data controllers. Seventh, data subjects should have the right to obtain data about themselves within a reason-

104 Emmett, *supra* note 102, at 48. Recommendation of the Organization of Economic Cooperation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80) 58 (Oct. 1, 1980). At the September 23, 1980, meeting where the recommendations were adopted, Australia, Canada, Ireland, Turkey, and the United Kingdom abstained. *See* Emmett, *supra* note 102, at 48.

105 A detailed analysis of the guidelines may be found at 22 HARV. INT'L L. J. 241 (1981).

106 Chairman, OECD Expert Group on Transborder Data Barriers and the Protection of Privacy.

107 Kirby, *supra* note 99, at 59.

able time and in intelligible form, and to challenge the accuracy and the relevance thereof. They should have the right to have inaccurate or irrelevant data erased, completed or modified, as is appropriate. Finally, for every data collection, a data controller should be accountable for compliance with the above principles.[108]

The guidelines recommend that each country act to limit the amount and method of data collected, and to assure data integrity.[109] Furthermore, when primary data are collected, respondents should be informed of the purpose for which the data will be used. Under the guidelines, disclosure for other purposes is only allowed if either the identified individual assents or judicial authorization is obtained. Finally, the guidelines provide that all data systems have one person designated accountable for ensuring that individual rights are protected.[110]

The OECD Guidelines on Individual Privacy are laudable for the progress, however modest, that they have made in establishing at least a modicum of international accord on this highly politicized issue. Never before have this many countries agreed, even as to general principles, about data protection.[111] One positive by-product of the agreement is that its structure helps to focus attention on the differences between individual and corporate privacy interests. Moreover, the guidelines, by addressing only individual privacy issues, avoid the pitfall of consolidating questions of individual versus corporate privacy into one document.

Unfortunately, the guidelines may be more notable for what they do not accomplish. For the subscribing OECD countries, it is doubtful that concerns regarding inadequate United States privacy protection will be assuaged by guidelines that include no specific procedures for compliance and implementation by each national government. From the United States perspective, concern exists that some European countries will utilize the guidelines to justify stengthening already stringent data protection laws.[112] Future progress will depend to a great degree upon the positions taken by the countries that are still considering legislation. A primary difficulty is that the guidelines will do little more than create a superficial appearance of similarity. Ulti-

---

108 Emmett, *supra* note 102, at 48.

109 Data integrity as an issue is distinguished from the right to examine and correct data because it places a duty on the data processor to ensure that he is storing accurate data in the first place. For further delineation of these issues, see *supra* note 12.

110 Kirby, *supra* note 99, at 60.

111 *See, e.g.*, The Council of Europe's experience in 1971, discussed *supra* in note 27.

112 Emmett, *supra* note 102, at 48.

mately, in five to ten years, a more specific document, perhaps a binding convention, is inevitable.[113] This document should resolve questions of inconsistent implementation strategies by different countries, limit data restrictions to the spheres of data where privacy abuse presents the greatest risk, and achieve reciprocal recognition of individual remedies when data is inappropriately disclosed. It is too early now to ascertain to what extent the OECD Guidelines will pave the way for a future agreement on individual privacy.

However, in the wake of ratification of the OECD Guidelines, reports are reaching the press of a move toward creating a parallel agreement recognizing a corporate privacy interest.[114] Any international agreement legitimizing corporate privacy legislation would be nothing less than a resounding setback for international free trade. But as the growing amount of national legislation indicates, the issue will not simply disappear if the United States fails to address it. The individual/corporate dichotomy must be brought to the attention of European countries considering enactment of corporate privacy statutes. Effective negotiations by the United States now may limit the repetition for corporate interests of the controversial and growing number of individual-oriented data protection laws and the non-tariff trade barriers they impose. If there was ever a critical time for a unified United States position on transborder data flow issues, it is now.

VI. Conclusion

In sum, the corporate privacy interest cannot be justified as a protection of individual or of corporate interests. It is a form of regulating commerce that imposes a heavy burden on free trade. The United States has recognized the distinction between corporate and individual privacy interests, but has failed adequately to protect individual interests. Foreign countries have perceived a threat to the privacy interests of their nationals in the transmission of identifiable data to countries where they have concluded that the confidentiality of data is inadequately safeguarded. They have responded by enacting data protection laws that restrict trade as well. The individual privacy interest is

113 See the currently proposed Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, Europ. T.S. No. 108, which has been adopted by the Committee of Ministers of the Council of Europe, but not yet ratified by all of its members. *See also* Council of Europe, Information Bulletin on Legal Activities, No. 4, at 15 (July 1979); Evans, *Computers and Privacy: The New Council of Europe Convention*, Eur. Prac. (1981).

114 *Id.*

more justifiable than the corporate interest, but it, too, involves significant commercial issues.

Although the full impact of the European data protection laws—both individual and corporate—has not yet been felt by the United States,[115] their initial repercussions are noticeable.[116] It is imperative that a coherent American information policy address the various problems in international data flow, particularly corporate privacy. Although concern for these issues exists, for example, within the National Telecommunications and Information Administration and the Department of Justice,[117] the continued failure both to agree upon objectives[118] and to unify the voices of the various federal agencies[119] will only allow the unfettered expansion of restrictive corporate privacy statutes, and the further eclipse of American economic interests.

Although the OECD Guidelines on Individual Privacy are a beginning in this regard, the United States should continue to support OECD efforts aimed at harmonizing conflicting laws. The prevention of international corporate privacy guidelines must be high on the national agenda of the United States. At the least, short term goals should include aggressive government support of United States business in negotiating bilateral solutions with those countries that have already enacted data protection laws.

The United States can be particularly influential in the developing countries. These countries must be shown that a workable balance can exist among the competing interests of individual privacy protection, the free flow of information endangered by corporate privacy statutes, and their own continued domestic economic and technological development.[120] The American position on transborder data flows and privacy must be an outgrowth of a well-defined domestic information policy. It is hoped that the failure of several recent privacy bills in the Congress[121] does not presage future congressional inaction in this area,

---

115 *See, e.g.*, W. Michael Blumenthal, Remarks to the National Computer Conference (May 6, 1981) *reprinted in* 47 VITAL SPEECHES OF THE DAY 550, 552 (1981).

116 Emmett, *supra* note 102, at 48.

117 *See, e.g.*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEP'T OF COMMERCE, THE FOUNDATIONS OF UNITED STATES INFORMATION POLICY 17 (1980).

118 *See, e.g.*, Eger, *supra* note 67.

119 Such unifying legislation has been introduced in the House of Representatives. H.R. 1957, 97th Cong., 1st Sess. (1981), would establish an interagency Council on International Communications and Information.

120 A good outline of issues relevant to national development can be found in Committee on Computers and Public Policy, Association for Computing Machinery, *A Problem-List of Issues Concerning Computers and Public Policy*, 17 COMMUNICATIONS OF THE ACM 495, 502 (1974).

121 *See supra* note 89.

and that executive leadership will unify the numerous internal voices into a single chorus. Only at that time will United States efforts to prevent further proliferation of laws restricting transborder transfers of corporate data have any significant prospect of success.