Northwestern Journal of International Law & Business

Volume 4
Issue 2 *Fall*

Fall 1982

Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism

Jane A. Zimmerman

Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism

I. INTRODUCTION

The world currently collects, processes, stores, and communicates more data than ever previously possible. Rapid advancements in computer and communications technology since World War II, making possible the current level of data usage, show no signs of slowing down.[1] Recently, remote access computers and computer-satellite links have rendered the transfer of data from one country to another commonplace.[2] The growth of information use and data services has necessitated a redefinition of information which, consequently, has given rise to a new awareness regarding the economic utility of information.[3]

---

[1] William Fishman cites the research and development undertaken in connection with World War II as the cause of enormous advances in computer and communications technology and the corresponding reductions in costs of providing high quality communication links. Fishman, *Introduction to Transborder Data Flows*, 16 STAN. J. INT'L L. 1, 7 (1980). Additionally, progress in the semi-conductor field has produced a tenfold decrease in the cost of computation every five years. One commentator notes that such rapid advancements will soon make even the most fast and efficient machines of today seem "unwieldy." Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 687 (1980).

[2] For example, Control Data Corporation's computer centers, combined with communication links, establish "a worldwide data processing network which allows a user almost anywhere in the free world to have unlimited computer power at their fingertips." *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. 36 (1980) (statement of Philip C. Onstad, Director, Telecommunications Policies, Control Data Corp.) [hereinafter cited as *Hearings*]; *see generally* Fishman, *supra* note 1, at 7-8.

Although the lack of commonly accepted definitions may make the measurement of such data services difficult, these service networks are often classified as the "infrastructure of international business and government operations." Shickich, *Transborder Data Flow*, 11 L. & COMPUTER TECH. 62, 64 (1979). The enormous amount of information crossing borders on a daily basis also attests to the growth and importance of this industry. *See* Emmett, *Strangulation of World Economies*, DATAMATION, Mar. 1978, at 201.

[3] The chairman of Burroughs Corporation recently stated that information has become a true product. In arriving at this conclusion, the chairman noted that the perception, as well as the definition, of information has evolved from a traditional notion of information as the material and supplies that support other activities to a notion of information as the central process itself, around which all else revolves. Speech by W.M. Blumenthal, Transborder Data Flow and the New Protectionism, before the National Computer Conference (May 6, 1981), *reprinted in* VITAL SPEECHES

Along with this new world perspective regarding information's economic value,[4] new legal concerns are developing in the United States and abroad. During the past decade, several European countries have enacted data protection laws[5] designed to protect individuals from the possible abuse of personally identifiable, computerized data.[6] This legislation goes beyond regulating domestic use of computer data to place restrictions on the transfer of personally identifiable data across national borders.[7] The implications of these national laws for international trade and business are prominent topics of international legal debate.[8] Recently, the Council of Europe[9] finalized a convention on transborder flow of personal data.[10] The proposed Council of Europe

---

OF THE DAY, July 1, 1981, at 551. Similarly, two management consultants recently told a group of corporate representatives that corporate data is a resource as important as cash, and should be managed accordingly. Johnson, *Treat Data as Manageable Resource, Firms Told*, COMPUTERWORLD, Mar. 30, 1981, at 35.

[4] *See* Turn, *Privacy Protection and Security in Transnational Data Processing Systems*, 16 STAN. J. INT'L L. 67, 68 (1980); *Hearings*, *supra* note 2, at 174 (statement of John Eger, Attorney).

[5] Austria, Canada, Denmark, France, the Federal Republic of Germany, Luxembourg, Norway, and Sweden now have data protection statutes enacted. *Appendix III Explanatory Report on the Draft Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, EUROPEAN COMMITTEE ON LEGAL COOPERATION MEETING REPORT 20, 22, para. 5 (1980) (a copy of this report is on file at the offices of the *Northwestern Journal of International Law & Business*) [hereinafter cited as *Explanatory Report*]. Belgium, Iceland, The Netherlands, Spain, and Switzerland have legislation under consideration. *Id.* Austria, Portugal, and Spain have incorporated data protection as a fundamental right in their respective constitutions. *Id.*

[6] Data protection laws have been defined as laws enacted for "the protection of the rights, freedoms, and essential interests of persons vis-a-vis the processing of personal information relating to them, particularly when computers aid in the processing procedure." Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87, 89 (1980). The emphasis is placed on regulation of the processing, maintenance, and communication of data rather than on the regulation of the actual content. In that sense, these laws regulate information in an indirect manner. *See generally* Note, *Contracts for Transnational Information Services: Securing Equivalency of Data Protection*, 22 HARV. INT'L L.J. 157 (1981).

[7] For discussion of the major foreign national provisions, see *infra* text accompanying notes 44-69.

[8] Data protection has been recognized as a new branch of law formulated especially for handling the issue of invasion of privacy in regard to computerized data. At the base of the controversy lies the question of whether the law can ever keep pace with a rapidly changing science. *See* Hondius, *Computers: Data Privacy*, IEEE SPECTRUM, Mar. 1980, at 67 [hereinafter cited as Hondius, *Computers: Data Privacy*].

[9] The Council of Europe at its inception in 1948 had 17 member nations; it has now grown to encompass 21 European countries. The Council has been especially concerned with the protection of human rights and the promotion of unity among its members, as well as respect for the Rule of Law. Statute of the Council of Europe, *adopted* May 5, 1949, ch. 1, art. 1(a), 87 U.N.T.S. 103. *See generally* Hondius, *Computers: Data Privacy*, *supra* note 8, at 68.

[10] 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 [hereinafter cited as C.O.E. Convention].

Convention, as well as other efforts at international agreements,[11] attempt to prevent unnecessary restrictions on information movement by harmonizing often conflicting national laws. However, even an international agreement may unduly burden international trade and business, if the practical effect of its terms is overly severe.

This comment will discuss the current status of national data protection laws and their effect on the conflict between the individual interest in retaining personal privacy and the business interest in preserving the free flow of information. Such discussion will highlight the consequences of the proposed Council of Europe Convention's regulation of personal data.[12] A brief look at the history of the information industry, as well as the costs of and justifications for transborder data flow, will serve to establish a framework for the issues and controversies which the Convention addresses. The comment will also focus on specific provisions of the Council of Europe Convention to ascertain its potential burden on international business and potential impact on American trade, suggesting that the present terms of the treaty unnecessarily hamper the conduct of trade. Finally, several improvements will be proposed for future international agreements, emphasizing the role of the United States in developing such agreements.

II. Conflicting Interests

The difficulty in formulating set standards for transborder data flow results from the need to balance two equally important, though competing, interests. The first interest is the economic necessity for free access to information in order to engage in trade or business activities profitably. In opposition to this interest, however, is the fundamental right of individuals to preserve their privacy by limiting the release of any information which personally concerns them. Consequently, an understanding of the two interests' significance and the interplay be-

[11] While several international organizations have considered the issue of transborder data flow, at the present time, the most significant proposal besides the C.O.E. Convention is a set of voluntary guidelines created by an expert group of the Organization for Economic Cooperation and Development. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, *adopted* Sept. 23, 1979; *see also* Guidelines Recommendations of the Council Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80)58 (Oct. 1, 1980).

[12] Personal data is information regarding an individual and may be recorded or stored on paper in a computer's memory bank. *See* Note, *supra* note 6, at 158. For the purposes of this comment, "data" will be limited to automatically processed personal data as in the C.O.E. Convention. Such data have been reduced to numbers and symbols which the computer can manipulate and produce upon command as a computer print-out. *Id.*

tween them is a prerequisite to a proper evaluation of the impact of any data protection law or agreement.

The complexity of international business today places a premium on the speed and accuracy of information flow. No longer can business transactions profitably occur over a number of days. In order to benefit from innumerable business opportunities, transactions must occur in hours, or even minutes.[13] Since a large part of international business decisions today take place in multinational corporations with branches in various parts of the world,[14] computerized communication links are the only means to achieve the necessary transmission speed. Similarly, computerized filing systems that quickly analyze complex bodies of information are essential to efficient and profitable business operations.[15] Information electronically transmitted or stored tends to be less ambiguous because it has been reduced to the computer's binary series of choices.[16] The data's reliability and accuracy is thus increased, generating better informed and more efficient business decisions.[17]

The United States has a special interest in maintaining the free flow of information. Information flow is likely to control almost all trade, either because trade consists directly of information exchanges, or because the conduct of trade is totally dependent on information exchange systems.[18] Since the United States is currently the world leader in information technology and trade,[19] international restrictions on the information industry most likely will affect United States business interests more than those of any other country.[20] There could be a severe reduction in the currently massive amounts of United States rev-

---

13 For example, IBM conducts business in 120 countries and new technology makes possible the rapid exchange of enormous quantities of data over substantial distances, enabling IBM to maintain its world-wide operation. *Hearings*, *supra* note 2, at 3 (statement of John Rankine, Vice-President of IBM). *See also* Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tarriff Trade Barriers?* 10 L. & POL'Y INT'L BUS. 1055, 1060 (1978).

14 It has been predicted that multinationals, the heavy users of international data, will account for up to 20% of the world GNP by 1985. Fishman, *supra* note 1, at 13.

15 Noll, *The Interactions of Computers and Privacy*, 7 HONEYWELL COMPUTER J. 163, 168 (1973).

16 Information is fed into a computer as a series of numbers consisting of ones and zeros; this is the binary number system. Thus, at the risk of over-simplification, the computer is nothing more than a series of devices which have only two states, on or off. Since there is no in-between state, information stored, analyzed, or transmitted by the computer is subject to little, if any, distortion. The resulting reduction in ambiguity increases the reliability of computerized data.

17 *See* R. VERNON, STORM OVER THE MULTINATIONALS: THE REAL ISSUES 2 (1977).

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

19 *Hearings*, *supra* note 2, at 327 (statement of Henry Geller, Assistant Secretary of Commerce). *See also* Shickich, *supra* note 2, at 64.

20 Eger, *supra* note 13, at 1056.

enue from the international information industry[21] if burdensome regulations decrease the utility of information exchange systems.

The incentive to preserve the free flow of information, along with the increased mobility of data, effectively generates a concern for the protection of personal privacy. The concern stems from feared misuse of computerized data. The conflict between the two interests is important because both the right to freedom of information and the right to privacy are fundamental human liberties.[22]

It is important here to distinguish between individual and corporate privacy interests.[23] The corporate privacy interest is a practical business interest in protecting the profitability of the enterprise involved, and does not flow from any notion of human rights.[24] The extension of data protection laws to cover this non-fundamental corporate interest could have disastrous consequences from two perspectives. First, the transmission of information within a company is often essential to the company's operations. For example, a firm's main office may need to consolidate corporate records identifying employees so that it knows what skills and resources are available. Curtailment of such information flow could severely hinder the enterprise.[25] Second, where one company possesses information about

---

21 By 1978, telecommunication and information goods had more than doubled their 1972 export total. This sector, together with agriculture and aviation, currently leads the United States export market. *Hearings*, *supra* note 2, at 325-26 (statement of Henry Geller, Assistant Secretary of Commerce). In 1980, foreign revenues accounted for 42% of total revenues of the top 50 United States companies in the data processing field. *Id.* at 521 (statement of Abraham Katz, Assistant Secretary of Commerce for International Economic Policy). Fifty-six percent of all large data bases for service networks are in the United States, and these account for more than 80% of worldwide transmissions. Speech by W.M. Blumenthal, *supra* note 3, *reprinted in* VITAL SPEECHES OF THE DAY at 552. Further evidence of the information industry as a major revenue producer is its place in the American workforce. A recent study shows that approximately 46% of the American workforce is comprised of "information workers," and it is estimated that in a few years 70% of all labor income will be from "information activity." *Hearings*, *supra* note 2, at 203-04 (statement of John Eger, Attorney).

22 The European Convention for the Protection of Human Rights and Fundamental Freedoms, *signed* Nov. 4, 1950, *entered into force* Sept. 3, 1953, Europ. T.S. No. 5, 213 U.N.T.S. 221. The Human Rights Convention recognizes both the right to freedom of information, *id.* art. 10, and the right to private and family life, *id.* art. 8, as fundamental. Since both are viewed as fundamental human rights, neither interest may be promoted to the exclusion of the other. The necessity of maintaining an equilibrium between these rights renders any solution to the conflict involved in transborder data flow much more difficult.

23 Individual or personal privacy refers to questions applying to natural persons as opposed to corporate privacy which applies the same principles to juristic persons, such as associations, foundations, and corporations. For a general discussion of the distinction between these interests and the foundations of each, see Grossman, *Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations*, 4 NW. J. INT'L L. & BUS. 1, 12-18 (1982).

24 *Id.* at 15-17.

25 *Id.* at 16.

another company, required submission of data bases to a competitor for inspection or correction may render conventional marketing practices ineffective.[26] The release of any data base may provide the competitor with an unfair advantage by allowing the competitor to falsify its own marketing practices as an alleged correction, and simultaneously providing it with access to otherwise unavailable information regarding the first company's product development and marketing strategies.[27] Thus, the privacy interest at issue in transborder data flow legislation should be limited to individual privacy interests.

Prior to the advent of the computer, little information was stored because of the lack of facilities and high storage costs. Thus, there was little opportunity to misuse stored information. Additionally, the entity in possession of the data (the data controller) was often known to the person about whom the data was stored (the data subject), since the two parties were usually within reasonable proximity. Consequently, a degree of deterrence existed, preventing unauthorized disclosures. With the development of computers, it is now possible to store enormous amounts of data in relatively small spaces, at minimum costs, and without the data subject's knowledge.[28] Also, the data controller is now physically distant from the data subject and often cannot be traced.[29] Therefore, it is less likely that the data controller will be deterred from disclosing data without the data subject's authorization. Furthermore, computer advances enable more integration and centralization of information,[30] again increasing the danger of information misuse.

Although computer advances compound the perceived possibility of an invasion of privacy,[31] it would be senseless to argue for a return

---

26 *Id.*

27 The potential impact of requiring juristic persons to license all their data bases on marketing, product development, and competitive pricing is "staggering." McGuire, *supra* note 18, at 6.

28 *See* Fishman, *supra* note 1, at 5.

29 A 1973 United States Department of Health, Education and Welfare report noted three changes that the computer brought to information processing. Computer advances created a new class of record-keepers who performed technical tasks and whose contact with suppliers and users of data was remote. ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 12 (1973).

30 Halls, *Raiding the Databanks: A Developing Problem for Technologists and Lawyers,* 5 J. CONTEMP. L. 245, 246 (1978). Formerly, it was too expensive and time-consuming to centralize information, and the consequent disorganization prevented access. Today, information is concentrated and the technology enables data banks to combine so that a 20 page dossier on every person in the United States could be available in four minutes. *Id.*

31 A Louis Harris Association's survey in the United States for Sentry Insurance Co. found that Americans view the computer as a major threat to personal privacy. Fifty-three percent of

to the old method of information storage and exchange. The computer is here to stay and its benefits are widely recognized.[32] The extensive use of the computer in both the public[33] and private[34] sectors attests to current dependence on the computer. Thus, a transformation in traditional notions of privacy is necessary to accommodate new technological developments. The notion of privacy as a deeply personal interest[35] should not be maintained in a society where impersonal machines quickly gather vast amounts of personal information. The idea of a personal privacy sphere simply is inconsistent with information's special character, because once the information is disclosed, sole control over the information is lost.[36] The recipient cannot be forced to forget the information received. Instead, privacy should be considered more broadly as an interest in "fair record management."[37] Most people will accept the existence of data storage as a consequence of modern life. It is only the potential misuse of this stored data that concerns them.[38] Hence, the data collection itself is seldom the issue; rather, the question is how to ensure the fairness of the subsequent use of the data.[39] Data protection laws should, therefore, impose duties on parties handling the particular information, instead of imposing restricitions on data collection itself.[40]

---

those questioned stated that they thought the present use of computers was a threat. *Public Concern on Privacy is Growing*, DATAPROCESSING, July 1979, at 8.

32 The benefits of information flow fall into four functional categories: (1) sharing scientific or technological information; (2) transferring statistical research data; (3) sharing administrative information such as police files or health records; and (4) facilitating economic activities, such as airline reservations, credit agencies, and management of multinationals. Transborder data flow between the parent and branch offices of multinational corporations, falling into the fourth category, is probably the most prevalent, but this by no means diminishes the importance of transborder data flow in other functional categories. *See* Pipe, *Work Paper on Transborder Information Flows: Requirements for a New International Framework*, 9 L. & COMPUTER TECH. 17, 20 (1976).

33 Organizations such as law enforcement agencies (INTERPOL), military conferences (NATO), as well as weather service bureaus and immigration services, depend on international computer links. For a more complete list, see *id.* at 21.

34 Dependence on computer networks in the private sector covers categories such as credit and banking, travel, corporate management, churches, labor organizations, and more. *Id.*

35 *See* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (right to be left alone); Hondius, *Computers: Data Privacy*, *supra* note 8, at 68 (private sphere into which others should not intrude without consent).

36 Hondius, *supra* note 6, at 96.

37 Fishman, *supra* note 1, at 5.

38 Skelly, *Balancing Privacy and Efficiency in an Electronic World*, 12 L. & COMPUTER TECH. 38, 41 (1979).

39 *See* Hondius, *Computers: Data Privacy*, *supra* note 8, at 68. *See also* Note, *supra* note 6, at 161.

40 Hondius, *supra* note 6, at 96-97. A machine is totally neutral, as is information; therefore, any misuse of the data must originate from the people who are in control of the information. *See*

Even though individual privacy interests may require protection where corporate privacy interests do not,[41] there is no absolute right to personal privacy.[42] Unless a legitimate personal privacy interest is involved, the use of data protection laws to restrict information flow is not justified. The existence of the competing interest in free access to information necessitates extra caution to avoid over-regulation which inhibits the efficient conduct of trade and business. A proper balance is necessary before imposing restrictions on the transborder flow of data.[43]

III. National Data Protection Statutes

Current national legislation serves as an example of the difficulty involved in reaching an equilibrium between the two interests at stake in transborder data flow. The impact of national data protection laws on the international information industry[44] is the same whether the legislation is in response to a perceived threat to privacy or is due solely to the self-interest of the enacting nation.[45] The current difficulty in maintaining a balance between privacy and the free flow of information results from two factors. National laws are contrary to the inherent international character of computerized data and other information transfers.[46] A second and related reason is that there are highly diversi-

C. Tapper, Computer Law 127 (1978) (immorality and incompetence are human vices and not mechanical feelings).

41 *See* Grossman, *supra* note 23, at 12-15.

42 *See generally* Fishman, *supra* note 1, at 20 (discussion of OECD Guidelines recognizes that personal data will move across national borders); Dreyfack, *Europeans Tighten Data Flow*, Electronics, Feb. 10, 1981, at 106.

43 Fishman, *supra* note 1, at 20. One commentator noted that even though personal privacy is a rationale for regulation that many nations readily accept, this rationale is quickly becoming secondary to other more harmful rationales. McGuire, *supra* note 18, at 3.

44 At least three subparts form the information industry: (1) the export of computers and communications equipment; (2) the foreign market for United States data processing services; and (3) the transmission of information necessary for multinational enterprises to operate. *Hearings*, *supra* note 2, at 216 (statement of Matthew Nimetz, Under Secretary, Department of State). Current data protection legislation, with its provisions restricting data entering and leaving the country, will most drastically affect the transmission of information vital to multinationals. However, the legislation may also adversely affect both the export of communications equipment and the international market for data processing. *Id.*

45 *Hearings*, *supra* note 2, at 203 (statement of John Eger); Note, *supra* note 6, at 168.

46 Information travels irrespective of national boundaries, thereby making it inherently international in character. Professor Knut Selmer, the chairman of the Norwegian Research Center for Computers and the Law, recently related an example of the impossibility of regulating transborder flows of information: during World War II, Norwegians used secret radios after the Germans confiscated all radio equipment in an effort to contain and control information flow. Scannell, *Issues of Transborder Data Flow Seen Missed*, Computerworld, Feb. 2, 1981, at 18 (report on Knut Selmer's speech before the First International Symposium on Computer Security

fied perceptions among nations regarding the best method to protect privacy adequately. The national character of laws enables such differences to develop. Thus, even though agreement exists on basic principles underlying data protection, national laws may prevent the application of those principles.

Sweden enacted the first law regulating the transborder flow of information.[47] This statute has since served as a model for most other European data protection laws.[48] The purpose behind its enactment was to assure Swedish citizens that personal information would only be used for purposes consistent with that for which it was collected.[49] The most prominent feature of this act is the provision establishing a Data Inspection Board (DIB) empowered to license all data bases within the country.[50] The DIB's regulatory powers and duties are broad and discretionary. It bases its licensing decisions merely on the kind and quantity of data stored,[51] and other data characteristics subject to discretionary judgment. Almost all European countries have authorized a similar regulatory agency to enforce their privacy protection laws.[52] The DIB also monitors all information transmitted from the country.[53] Often, the DIB may prevent data removal simply because the nation receiving the information is perceived to have inadequate protection for the data.[54]

---

and Privacy). *See also Hearings*, *supra* note 2, at 227 (statement of Matthew Nimetz, Under Secretary, Department of State).

47 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.), *effective* July 1, 1979, *reprinted in* 5 COMPUTER L. SERV. app. 9-5.2a, No. 2 [hereinafter citied as Swedish Data Act].

48 *See* Shickich, *supra* note 2, at 68. *See also* Hondius, *Computers: Data Privacy*, *supra* note 8, at 68.

49 *See* Eger, *supra* note 13, at 1072.

50 Swedish Data Act, *supra* note 47, § 2. Section 2 states: "A personal file may not be set up or kept without permission from the Data Inspection Board. The setting up of a personal file means also collection of data to be included in the file."

51 *Id.* § 3. Section 3, in pertinent part, provides:

> The Data Inspection Board shall grant permission to set up . . . a personal file if there is no reason to assume that . . . undue encroachment upon the privacy of registered persons will occur.
> In judging whether undue encroachment may occur special attention shall be paid to the nature and quantity of the personal data to be recorded in the file, to how and from whom the data are to be collected, and to the attitude to the file. . . assumed to be held by the persons who may be registered.

52 *Hearings*, *supra* note 2, at 336 (statement of Henry Geller, Assistant Secretary of Commerce). The European data protection laws generally establish a privacy protection standard and an administrative enforcement mechanism.

53 Eger, *supra* note 13, at 1070; Shickich, *supra* note 2, at 68. Any data to be transmitted outside of the nation must be submitted to the DIB for inspection prior to transmission.

54 For example, a small Swedish town sought a British firm to produce health identification cards for its residents. The Swedish DIB, however, would not authorize the release of the health

The monitoring function is not confined to disallowing the transfer of data to those countries without adequate safeguards. Regulations also restrict data flow where the laws of two countries partially conflict, even though both laws are designed to generate adequate data protection. For example, the German Data Protection Act incorporates technical security standards to prevent the receiving country from altering the received data.[55] In essence, this regulation may prevent the receiving country from decoding data received to process or store it. Serious legal complications may result if the receiving nation has laws similar to those of the United Kingdom, where the British Post prohibits the receipt of coded data unless it is supplied with the key to the code.[56] Such conflicting provisions may well produce an irresolvable dilemma which will severely curtail or totally block information flow. Although monitoring activities authorized in these older European statutes may unduly hinder the free flow of information, the laws are at least limited to personally identifiable data. Some of the more recent data protection statutes have extended data protection to juristic persons (corporations, foundations, and other associations), and have restricted the transfer of information concerning such entities.[57] The basis of legisla-

---

information to the British firm, despite a contractual provision that no copies of the records would be made, because the United Kingdom lacked "insurance in terms of law or administrative authority against stealing or further use of this population file." Pantages & Pipe, *A New Headache for International DP*, DATAMATION, June 1977, at 115, 118. Similarly, before Germany enacted its data protection statute, a German based corporation wishing to centralize its corporate personnel files was unable to consolidate its records on Swedish employees with its other personnel materials in Munich. *Id.*

In the United States, Michael Blumenthal, chairman of Burroughs Corporation, stated that Burroughs' system to make information available on employee skills was in jeopardy. The West German legal counsel had advised Burroughs that the very existence of the system would require government approval and the establishment of confidentiality guarantees. Even then, there were no assurances that later use of the system would not be obstructed. Speech by W.M. Blumenthal, *supra* note 3, *reprinted in* VITAL SPEECHES OF THE DAY at 553. Blumenthal additionally noted that Burroughs was already having difficulties with its regional computer systems designed to diagnose problems in customer's computers and to transmit information from the central computer to guide on-site repairs. The Canadian government refused to allow the system to be hooked up to a Canadian computer which needed hardware repairs. *Id.*

55 Federal Data Protection Act, 1977 Bundesgesetzblatt I 201 (W. Ger.), *reprinted in* 5 COMPUTER L. SERV. app. 9-5.2a, No. 3. Section 6(1), in pertinent part, states: "Persons processing personal data. . . shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Law, and in particular the requirements set out in the Annex to this Law." Paragraph 9 of the Annex to Section 6(1) states: "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)."

56 Eger, *supra* note 13, at 1074.

57 In 1977 and 1978, Austria, Denmark, and Norway enacted privacy legislation extending to legal entities. The Norwegian Privacy Act, section 1, provides: "The term 'personal information' shall mean information . . . directly or indirectly, traceable to identifiable individuals, associa-

tion concerning commercial privacy is intrinsically weaker and the need for the free flow of information is much more compelling.[58]

The United States approach to privacy legislation differs significantly from the European approach. The most prominent differences lie in the United States refusal to adopt a sweeping, omnibus approach to privacy legislation, choosing instead to adopt a sector by sector legislative policy as specific privacy problems arise.[59] Additionally, the United States relies on judicial enforcement of privacy, rather than on a regulatory agency approach.[60] From the European perspective, these differences render data protection in the United States impermissibly lax. This may result in the blockage of data flow to the United States, since the European laws do not allow the transmission of data to states with inadequate protection. Any such blockage would cause significant harm to United States industries by increasing the cost of obtaining vital operating information.[61] Therefore, even though American and European data protection begin from the same notion of "fair record management,"[62] the United States task is to convince European nations that the American approach to data protection will ensure adequate or equivalent protection for data stored and processed in the United States.[63]

Presently, there may be gaps in American legislation, but these gaps are due less to the inadequacy of existing legislation than to the

---

tions or foundations." Personal Data Registers Act, No. 48 (June 9, 1978) (Nor.), *reprinted in* 5 COMPUTER L. SERV. app. 9-5.2a, No. 5.

Both the Danish Private and Public Register Acts of 1978 provide: "this Act shall apply to registers kept for specified companies, institutions, associations and the like that cannot be classified as part of the public administration. . . . (Public Authorities Registers Act, 1978, sec. 2)." Private Registers Etc. Act, No. 293, 1978 Lovtidende for Kongeriget Danmark [LKDk] A833 (Den.), *reprinted in* 5 COMPUTER L. SERV. app. 9-5.2a, No. 6; Public Authorities' Registers Act, No. 294, 1978 LKDk A 839 (Den.), *reprinted in 5* COMPUTER L. SERV. app. 9-5.2a, No. 7.

The Austrian Federal Act of 18th October, 1978, on the Protection of Personal Data provides, in article 2, part 1, paragraph 2: "Persons affected: natural or legal persons or associations of persons under commercial law, about whom data are collected, processed or disclosed." Data Protection Act, No. 565, 1978 Bundesgesetzblatt für die Rupublik Österreich [BGBlÖ] 3619 (Aus.), *reprinted in* 5 COMPUTER L. SERV. app. 9-5.2a, No. 8.

58 *See supra* notes 23-27 and accompanying text.

59 Hondius, *Computers: Data Privacy*, *supra* note 8, at 70.

60 *Hearings*, *supra* note 2, at 338 (statement of Henry Geller, Assistant Secretary of Commerce); Fishman, *supra* note 1, at 5.

61 *See* Note, *supra* note 6, at 163.

62 *See supra* notes 35-40 and accompanying text.

63 Several commentators think that United States law is at least as adequate as European privacy legislation, and may actually be broader. Turn, *supra* note 4, at 76; *Hearings*, *supra* note 2, at 318 (statement of Henry Geller, Assistant Secretary of Commerce). Therefore, the problem is merely one of convincing European states.

non-existence of legislation for certain types of data.[64] Furthermore, these gaps result more from the differences encountered in a common law as opposed to a civil law system, than from a lack of concern for privacy.[65] In fact, the United States has strongly advocated privacy protection where need has been demonstrated.[66] Although further United States privacy legislation may increase the opportunity for greater data flow from Europe to the United States, American trade and business may benefit most by seeking international agreement to harmonize, and perhaps to equalize, the national legislation of all countries. This will prevent each government from extending its nation's privacy legislation beyond its legitimate perimeter in an effort to further protectionist policies, since there would be an extra-national check on such misuse.[67] Despite the fact that the free flow of information is not an absolute value,[68] the over-extension of data protection laws conflicts with the principles underlying currently existing international fair trade legislation.[69] The only way to avoid this economic protectionism is to seek an international agreement that will limit the amount of permissible regulation.

---

64 The adoption of a sector by sector approach has led to limited protective legislation in areas such as credit information or educational information. *See generally* Hondius, *Computers: Data Privacy*, *supra* note 8, at 70. This, in effect, has left other types of information such as medical and research records without any privacy protection. However, even these areas have been or are under consideration for legislative action. *See* H.R. 5935 and S. 305, 96th Cong., 2d Sess. (1980) (bill concerning confidentiality of medical records); H.R. 3409 and S. 867, 96th Cong., 2d Sess. (1980) (bill concerning confidentiality of records collected during the process of research).

65 The United States common law system has been characterized as only limiting freedoms after a harm has occurred, whereas the European civil law system tends to legislate first to prevent the possible occurrence of any mischief. Turn, *supra* note 4, at 76. Therefore, the non-existence of protection in certain areas of data collection in the United States is due more to the approach taken in regard to the legislative process, than to a policy that legislation is not necessary.

66 The United States legislative record in the area of privacy proves that the United States has a strong concern for civil rights and the protection of personal privacy. For example, the United States Privacy Act of 1974, 5 U.S.C. §552a (1976 & Supp. IV 1980), is a powerful tool to protect government records from abuse at the federal level. In the private sector, again, the Fair Credit Reporting Act, 15 U.S.C. §§ 1681a-1681t (1976 & Supp. IV 1980), and the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (1976 & Supp. IV 1980), both offer substantial privacy protection. *Hearings*, *supra* note 2, at 337 (statement of Henry Geller, Assistant Secretary of Commerce).

67 *Hearings*, *supra* note 2, at 220-21 (statement of Matthew Nimetz, Undersecretary, Department of State).

68 *See generally* Fishman, *supra* note 1, at 20; Dreyfack, *supra* note 42, at 106.

69 *See generally* General Agreement of Tariffs and Trade (GATT), *signed* Oct. 30, 1947, *entered into force* Jan. 1, 1948, 61 Stat. A 3, T.I.A.S. No. 1700, 55 U.N.T.S. 194. While this agreement concerns tariff and non-tariff barriers only in regard to the trade of goods or products, the principal requirement of fair trade on an international level may be applicable to services such as telecommunications.

IV. The Costs of Restricted Information Flow

The costs resulting from regulation of information flow emphasize the need to limit regulation to narrowly-defined exceptional circumstances. The costs of transborder data flow restriction are based on the notion that humans are social creatures with a need to share knowledge in an effort to organize the world more efficiently for the mutual benefit of all.[70] The specific harm resulting from data protection laws depends on the type of information involved. Traditionally, transborder data flow occurs for four reasons. The first three reasons relate to the public sector of information transfer, while the fourth category pertains to the private sector: (1) the transfer of scientific and technological information; (2) the transfer of administrative data, such as police files or disease control data; (3) the transfer of statistical data; and (4) the transfer of economic or commercial data.[71] Governments or international agencies almost exclusively initiate public sector transfers. Data protection laws are less likely to produce harmful effects in this sector since bilateral agreements often resolve questions concerning the use of data.[72] Still, in a world of constantly shifting international relations, the potential for ignoring such agreements exists, depending upon the degree to which current relations with the other nations are amicable and cooperative. In this sense, a multilateral treaty may afford more effective privacy protection. Over time, nations may begin to accept the wide-spread principles contained in a multilateral treaty as international customary norms. Even this protection, however, may not be enough to ensure sufficient free flow of information when one considers that the fullest possible knowledge is vital to proper decisionmaking.[73]

In contrast to public sector regulation, data protection laws have

---

70 John Pierce, of the California Institute of Technology, wrote: "Without external communication we might live, but we would be ignorant, lonely individuals. We would have neither the inspiration of accumulated skill and knowledge nor the support of a society." Pierce, *Communication*, Sci. Am., Sept. 1972, at 31. Similarly, John Eger has stated that information flow benefits groups and nations by reducing the ignorance and misunderstandings that are often the source of conflicts. In this sense, Eger states: "Barriers to free flow can only constitute a rear guard action in the growth of the global community in economic, social, and cultural terms." *Hearings*, *supra* note 2, at 210 (statement of John Eger, Attorney).

71 *See* Pipe, *supra* note 32, at 20.

72 Grossman, *supra* note 23, at 8.

73 In a fall 1980 report to the United Nations Educational Scientific and Cultural Organization, the significance of information was set out: "The flow of technical information within nations and across national boundaries is a major resource for development. Access to such information, which countries need for technical decisionmaking at all levels, is as crucial as access to news sources." McCarter, *Nations Seeking Limits on TDF*, Computerworld, Mar. 3, 1981, at 53. While this report was specifically concerned with technical and scientific information, its implications extend to all data necessary to various types of decisionmaking.

great potential for producing harmful effects in the private sector, where information transfers consist of economic and commercial data and are not subject to prior bilateral agreements. The private sector, accordingly, has always been more susceptible to regulation with respect to transborder flow.[74] Data flow restrictions in the private sector certainly have more potential for an outright financial impact.[75] In addition, the restrictive impact of data protection laws in this sector, while imposing costs on the country seeking the data, is also likely to impose both political and economic costs on the domestic sectors of the nation with the data protection law.[76] Comparatively, the domestic costs may outweigh any benefits to the country enacting this type of privacy legislation.

One potential domestic cost of data protection legislation is that it prevents organizations from seeking data processing service abroad. This results in lost revenue to the country offering the processing services by reducing the market for services that it offers.[77] However, the enterprise seeking services outside its own country is also harmed because it is forced to seek alternatives to what it presumably chose as the best processing service.[78] Costs result when the enterprise must turn to less adequate processing services or pay a higher price for equivalent services.[79] A second cost is that data protection laws often prohibit the import of foreign computer equipment.[80] This again results in lost revenue to the exporting nation since the market for its computer equipment is reduced.[81] It may, however, injure the potential importing

74 Grossman, *supra* note 23, at 9.

75 The potential for large revenue loss exists if foreign data protection laws are enforced with respect to the United States. Foreign revenues accounted for 42% of the total data processing revenues of the top 50 data processing companies in the United States. *Hearings*, *supra* note 2, at 521 (statement of Abraham Katz, Assistant Secretary of Commerce). *See supra* note 21 and accompanying text.

76 Note, *supra* note 6, at 169. The costs to the nation with data protection laws generally result from the discontent within the private sector due to the additional expenses the enterprises must undertake.

77 *See Hearings*, *supra* note 2, at 216 (statement of Matthew Nimetz, Undersecretary, Department of State).

78 It is assumed that every rational enterprise will act in the most cost efficient manner by selecting the best services available for its needs at the lowest price. This also assumes that there is more than one service from which to choose.

79 For a more detailed account of this notion of cost, see Note, *supra* note 6, at 169.

80 Many United States observers believe that data protection is used to ensure Europe's control over new digital communication techniques. Dreyfack, *supra* note 42, at 106. *See also Hearings*, *supra* note 2, at 402 (statement of Russell Pipe, President of Transnational Data Reporting Service, Inc.).

81 *Hearings*, *supra* note 2, at 216 (statement of Matthew Nimetz, Undersecretary, Department of State).

nation as well, if that nation does not have the requisite technology or capabilities to develop equivalent computer systems.[82] Even though data protection legislation is designed to encourage the development of domestic technological capabilities, the domestic enterprises will be harmed if forced to forego needed advanced computer equipment, or to pay a significantly higher price for the domestic production of such equipment.

Within the private sector of information transfer, costs result from a reduced flow of vital information from branches of an enterprise located in countries with data protection laws.[83] In this situation, the multinational is presented with three options. First, the multinational may regionalize its record-keeping, so that each branch in each country maintains its own records. While this option is the most economically beneficial for the host nation,[84] it is likely to be avoided by the multinational since it would be costly and ultimately inefficient.[85] The second option is to remove totally the multinational's operations from any country with restrictive data protection laws. This option would result in lost revenues for both the enterprise and the host nation; thus, this alternative is also unlikely to be adopted. Finally, the enterprise may submit the desired data to the appropriate Data Inspection Board[86] and

---

82 Many of the countries which resist the import of information have no information technology or industry of their own. At present, they cannot hope to compete technologically with advanced nations. Eger, *supra* note 13, at 1065.

83 *Hearings*, *supra* note 2, at 216 (statement of Matthew Nimetz, Undersecretary, Department of State). John Rankine, Vice-President of IBM, stated that information flow is needed to maintain sufficient inventory of employee skills to keep foreign customers up to date on engineering, design, manufacturing information, and technical changes or improvements. *Id.* at 3.

84 Regionalization of record-keeping provides each enterprise branch office with its own data storage unit, thus increasing employment opportunities, tax revenues, and national product within the host nation, and decreasing the need for and costs of data regulation, since there would be little need for transborder data flows. *See* Note, *supra* note 6, at 167-68.

85 Pantages & Pipe, *supra* note 54, at 116. *See also Hearings*, *supra* note 2, at 57 (responses of Control Data Corporation). This cost may become increasingly obvious if governments which license data processing and storage equipment begin to favor domestic data processing companies. Michael Blumenthal, of the Burroughs Corporation, maintains that this cost is likely to occur due to a loophole in the new GATT Multilateral Trade Agreement, which exempts telecommunications from its Government Procurement Code. This Code generally prohibits preferential treatment, but with telecommunications exempted, it could be treated preferentially. Speech by W.M. Blumenthal, *supra* note 3, *reprinted in* VITAL SPEECHES OF THE DAY at 552.

86 The European data protection laws consist basically of the establishment of a privacy protection standard and an administrative mechanism, usually a regulatory type of agency known as a Data Inspection Board (DIB), to ensure that the privacy standard is enforced. *Hearings*, *supra* note 2, at 336 (statement of Henry Geller, Assistant Secretary of Commerce).

The Swedish Data Act, *supra* note 47, which has served as the prototype for most other data protection statutes, requires the DIB to inspect and approve or disapprove all data leaving the country.

hope that the Board will approve the transfer of the most essential and less sensitive corporate data. Costs result for the multinational enterprise since the business assumes the risk of the Board's refusal to transmit certain data. Although not as obviously, this option also will create costs to the host country. The submission of the data to the Inspection Board in essence is a disclosure of data and carries with it the potential for the members of the Board to misuse the information. This may produce high costs to the citizens of a nation supposedly protected from abusive and unnecessary dissemination of personal information.[87] The number and severity of costs involved in the impairment of information flow demonstrate that data protection laws should only apply under narrow circumstances. The resulting encouragement of free flow of information should prove beneficial for both the country seeking data and the nation enacting the data protection law.

V. Justifications for Restricted Information Flow

Data protection laws generally protect individuals from the abuse and dissemination of confidential data; thus, legitimate rationales for such protection exist. Usually, a combination of several rationales constitute the motivating force behind data protection legislation.[88] While each state interest or rationale by itself may be laudable, the combination of several increases the danger of extending the laws beyond their justifiable limits. A review of these interests will underscore the difficulty in reaching the proper equilibrium between the free flow of information and the personal privacy interests so as to avoid the overregulation of international information flow. In turn, recognition of this difficulty mandates the need for extra caution in determining any set of standards for data regulation to prevent disguised protectionism.

The perceived need to regulate transnational data flow begins with the territoriality of domestic laws and the potential loss of jurisdiction and control over the use of data once it leaves the country.[89] While several grounds may support the regulation, the result of each rationale

---

[87] Warren Burton, Vice-President of Tymshare, Inc., a remote access data processor based in California, recently criticized the establishment of data inspection boards: "The concept of a central government authority which knows and controls the information on all citizens and commerce seems to contradict, in practice, the protection of human rights." *Hearings*, *supra* note 2, at 69. *See also* Shickich, *supra* note 2, at 71.

[88] For a detailed discussion of political, economic, and individual interests involved in transborder data flow, see 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, 246-54 (1974).

[89] *Id.* at 249.

is to manifest the government's preference for protecting, controlling, and conserving data within its national borders, rather than importing, exporting, or exchanging the new ideas that information offers.[90] Generally, a nation cites several grounds for its regulation, claiming privacy protection as the primary motivation. However, the primacy of any particular ground will vary with the involvement of different facets of the information industry.[91]

One major ground for data protection legislation is the state's interest in maintaining its sovereign status and in preserving the nation's cultural identity.[92] Governments have often exercised their sovereignty for the welfare of their citizens by regulating the type of information reaching their people.[93] The development of the computer has transformed this interest to regulating data entering and leaving the country.[94] In essence, many foreign governments believe that the transborder data flow out of their country, whether for processing or storage, could result in their country becoming overly dependent on the processing or storage country.[95] Effective and efficient government decision making requires enormous amounts of information. Thus, the degree of accessibilty to information determines the government's ability to make its own decisions. Therefore, one nation's dependence on another for the storage of vital data could result in significant harm to the customer nation if the storage nation limits the return of data to its owners. There are two potential results, depending on the degree to which the data is withheld. First, the storage nation may impose its own value system on the customer nation by selectively releasing information to distort the decision making process.[96] Second, if the storage nation refuses to release any of the data, the customer nation is likely to

---

90 *Id.* at 227.

91 *See supra* note 44.

92 Developing countries, which have long feared cultural inundation by industrialized nations, rely heavily upon the concern for sovereignty. *See* McCarter, *supra* note 73, at 53 (third world seeks redress for the imbalance of data flow by seeking access to world-wide data networks and limiting access to their own domestic data bases). Underlying these restrictive measures are claims of biased news reporting by the foreign press and the refusal of industrialized nations to share information technology on the developing nations' terms. Eger, *supra* note 13, at 1081.

Developed nations are now similarly fearful of cultural inundation resulting from the foreign storage of data. Hugh Falkner, a Canadian Minister of Science and Technology, expressed this fear as "the danger that industrial and social development will be largely governed by the decisions of interest groups residing in another country." *Id.* at 1078-79.

93 For example, obscenity laws and regulation of information for national security reasons have long been considered legitimate functions of governments. Bigelow, *Transborder Data Flow Barriers*, 20 JURIMETRICS J. 8 (1979).

94 *See generally* Fishman, *supra* note 1, at 20.

95 Eger, *supra* note 13, at 1078-79.

96 *Id.*

appear indecisive and thereby lose the respect and confidence of its people.[97]

A second rationale for data protection legislation is administrative in nature. The government of the customer nation needs access to information in order to perform services for its citizens.[98] This rationale again involves the dependence of the customer nation on the storage nation to release vital information without which the customer nation's government cannot perform essential services. The failure to perform such services would discredit the government. Therefore, the customer nation prefers to retain the data to avoid this result.

A third rationale involves the individual and his or her own privacy interest.[99] The government must protect the privacy rights of its citizens. Potential invasions of privacy arise both when transborder flows occur in the course of business between multinationals and within multinational enterprises.

A final interest is economic protection. This rationale usually appears where the import and export of computer machinery and related equipment is involved, but it appears also where there is data processing or storage outside a nation's boundaries. This interest involves many protectionist qualities in that the government is using data protection laws to develop its domestic computer technology and industry.[100] There has been a realization that information is a powerful resource.[101] The result is that the government prohibits the use of foreign equipment or services to keep the revenues within the country, and to encourage, or even to force, local industries to upgrade their own

---

97 *Id.*

98 For example, the administrative need for information includes data for effective crime detection and prevention, fire protection, and public health care. Gotlieb, Dalfen & Katz, *supra* note 87, at 249-50.

99 For discussion of the individual privacy interests, see *supra* notes 28-40 and accompanying text.

100 Several countries are targeting the telecommunications and information industry as vital to national growth in the 1980s. *Hearings*, *supra* note 2, at 324 (statement of Henry Geller, Assistant Secretary of Commerce). Mr. Geller expressed the fear that the new importance of information will cause countries to further the development of their domestic industries through protectionist policies. *Id.*

101 Louis Joinet of France stated at a 1977 Vienna symposium: "Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries." Eger, *supra* note 13, at 1065-66. It is not only governments, however, that have recognized the need for this industry: "Telecommunications and information resources are increasingly seen as essential to national survival. ITT succinctly captured this theme in a recent advertisement: 'By the year 2000, a country's gross national product will largely depend on its ability to deliver information.' " *Hearings*, *supra* note 2, at 402 (statement of Russell Pipe, President of Transnational Data Reporting Service, Inc.).

capabilities.[102]

While each of these interests may be more or less legitimate bases for enacting data protection legislation, that is not the present concern. Rather, the concern is that a combination of the rationales to create the motivating force for legislation will also exert pressure on a government to extend the application of data protection. This may ultimately undermine the free flow of necessary information. Their significance, then, lies in recognizing the need to counteract this additional pressure, rather than in determining which particular rationale is the impetus behind a state's legislation. Provisions to avoid over-regulation are essential for any data protection law or agreement, otherwise vital information flow may be unjustifiably burdened.

VI. The Council of Europe Convention

The Council of Europe Draft Convention (C.O.E. Convention),[103] while admirably taking great steps toward the protection of personal privacy, has not considered at least two essentials for an international agreement: flexibility and maximum standards. Since the ratification of this Draft Convention seems imminent,[104] it is increasingly important to understand the potential impact of this Convention on international trade in general, and on American trade and business in particular.[105] A brief discussion of the essential advantages of international agreements will expose the potential problem areas in the C.O.E. Convention. Subsequently, a review of the Convention itself will elucidate the inadequate consideration that the drafters gave to these areas.

International agreements on transborder data flow are superior to national legislation because automatic data processing is an inherently international discipline. New technology continually facilitates the

---

102 Shickich, *supra* note 2, at 64.

103 C.O.E. Convention, *supra* note 10.

104 As of the time of this writing, nine of 21 governments have signed the C.O.E. Convention, although none have ratified it. The European Communities, however, have urged ratification. Statement of Lucy Humer to the Working Group on Transborder Data Flows of the Advisory Committee on International Investment, Technology and Development, Washington, D.C., Sept. 10, 1981.

105 The impact of the Convention on international trade and business may occur sooner than expected. While most treaties enter into force only upon ratification, as does the C.O.E. Convention, many authorities find that merely signing the treaty obligates the signatory to avoid defeating the object and purpose of the treaty prior to its entry into force. Indeed, some commentators maintain that a kind of contractual obligation begins at the same time negotiations commence. *See generally* Rogoff, *International Legal Obligations of Signatories to an Unratified Treaty*, 32 ME. L. REV. 263 (1980). This obligation originates from article 18 of the Vienna Convention on the Law of Treaties, U.N. Doc. A/Conf. 39/27, *reprinted in* 63 AM. J. INT'L L. 875 (1969).

travel of data across national borders. This characteristic dictates similar legal treatment for data regardless of the countries through which the information travels.[106] Furthermore, the pace at which technology is developing necessitates the sharing of limited national expertise. International cooperation may allow such sharing and avoid unnecessary duplication or divergence of work.[107] Finally, transborder data flow impacts on fundamental human rights, rights which should be protected equally for all humans, without regard to nationality, by harmonizing national laws.[108] Any international agreement on transborder data flow must remain flexible enough to adapt to the fast-paced, rapidly changing technology that characterizes the telecommunications and information industry. Such an agreement cannot bind its signatories to terms which will soon be outdated and burdensome. In addition to setting minimum standards of data protection, an international agreement on transborder data flow must contain maximum standards in order to prevent the over-regulation of data flow which potentially may curtail international trade and business.[109]

The avowed purpose of the C.O.E. Convention is not to prevent data flow; rather, it is to ensure that individual liberties, especially the right to privacy, are respected with regard to automatic data processing.[110] The Council of Europe utilized the Convention to reaffirm its member states' commitment to "freedom of information regardless of frontiers."[111] Still, application of the Convention may actually impede the flow of data because its provisions are too inflexible and it does not sufficiently prevent over-regulation.

The Convention consists of three main parts: (1) "Basic Princi-

106 Kirby, *Developing International Rules to Protect Privacy,* 12 L. & COMPUTER TECH. 53, 55 (1979); Hondius, *Computers: Data Privacy*, *supra* note 8, at 67.

107 Kirby, *supra* note 106, at 55; Hondius, *Computers: Data Privacy*, *supra* note 8, at 67.

108 One United States official noted that "the dynamic nature of [information] technology and industry also argues against taking immediate action which will be difficult to update as appropriate." *Hearings*, *supra* note 2, at 337-38 (statement of Henry Geller, Assistant Secretary of Commerce). Similarly, it is feared that agreements would contain language inhibiting research, development, and applications in the quickly changing technology. *Id.* at 221 (statement of Matthew Nimetz, Undersecretary, Department of State).

109 *See supra* text accompanying notes 70-87.

110 C.O.E. Convention, art. 1, *supra* note 10. Article 1 states: "The purpose of this convention is to secure in the territory of each Party for every individual whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")." Indeed, Frits Hondius, Chairman of the Public Law Division of the Council of Europe, and the driving force behind the adoption of the convention, stated: "We passed the convention in the interest of the free flow of information, because without international legal action, national laws were putting heavy restrictions on transborder data flows." Dreyfack, *supra* note 43, at 106-08.

111 C.O.E. Convention, Preamble, *supra* note 10.

ples," which outline the substantive law provision; (2) "Special Rules" on transborder data flow; and (3) "Mechanisms for Ensuring Mutual Assistance" between the parties.[112] In approaching the problem of privacy, the Council began by setting out, in the first part, certain core principles found in virtually all data protection legislation.[113] These core principles, in effect, are a minimum standard of protection that any contracting party must provide in the automated processing of personal data. Even though the Convention enumerates minimum standards, various Convention articles also authorize one or more of the following deviations from the core principles: the refusal to apply the provisions of the Convention to certain types of data;[114] the extension of the Convention to cover additional types of data;[115] or the application of stricter standards of protection than the Convention requires.[116] The problem with all these authorized changes in the application of certain provisions, or even changes in the provisions themselves, is that there is no specification of maximum protection standards. The second part of the Convention, Special Rules, directly addresses the problem of transborder data flow.[117] This part, consisting of one article, article

---

112 *Explanatory Report*, *supra* note 5, at 22, para. 5.

113 The common core is based on the principles contained in resolutions adopted by the Committee of Ministers of the Council of Europe in 1973. Resolution (73)22 established principles of data protection in the private sector, and Resolution (74)29 provided similar protection in the public sector. COUNCIL OF EUROPE, COLLECTED RESOLUTIONS ADOPTED BY THE COMMITTEE OF MINISTERS IN THE FIELD OF CIVIL, COMMERCIAL, AND INTERNATIONAL LAW (1973).

114 C.O.E. Convention, art. 3, § 2(a), *supra* note 10. Article 3, section 2, in pertinent part, provides:

> 2. Each State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:
> a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited.

115 *Id.* art. 3, §§ 2(b)-(c). Sections (b) and (c) of Article 3 provide:

> b. that it will apply this convention also to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;
> c. that it will apply this convention also to personal data files which are not processed automatically.

116 *Id.* art. 11. Article 11 provides: "None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention."

117 C.O.E. Convention, ch. III, art. 12, *supra* note 10. Article 12 states:

> 1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
> 2. Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party.
> 3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
> a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those

12, attempts to reconcile the Basic Principles of data protection, set out in the first part, with the principle of free flow of information.[118] Nonetheless, this article alone, as well as in combination with provisions allowing changes in the application of protective standards, may prevent the attainment of this objective. The third part of the Convention sets out provisions for the mutual assistance of contracting parties in regard to individual violations,[119] and sets up a consultative committee to facilitate cooperation with regard to the Convention itself.[120] This part essentially leaves the continued vitality of the Convention to the various parties through the implementation of the Basic Principles in their domestic law.[121]

The second part of the treaty, concerning transborder data flow, is of primary concern to this comment. At first glance, article 12 seems to prohibit any restrictions on data flow, at least between contracting parties, except in exceptional circumstances. Upon closer analysis, however, it becomes evident that this may not be the result in actual practice. The article potentially allows a party to prohibit transborder data flow to another party, or to subject the data to special authorization as long as the restriction is not "for the sole purpose of the protection of privacy."[122] Although the "sole purpose" provision was originally intended to prevent the use of the Convention as a hidden trade barrier,[123] this language may not accomplish that purpose. In fact, it could have the opposite effect, since any other ground in addition to the privacy rationale may justify the regulation of data flow.[124]

Reciprocity or equivalency of national laws is the main enforcement mechanism of the Convention. While the Convention allows derogation from the limiting provisions of article 12,[125] these derogations are not allowed where the receiving party provides *equivalent* data protection.[126] Yet, the provisions permitting deviations from the core prin-

---

files, except where the regulations of the other Party provide an equivalent protection;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

118 *Explanatory Report*, *supra* note 5, at 32, para. 61.

119 C.O.E. Convention, ch. IV, arts. 13-17, *supra* note 10.

120 *Id.* ch. V, arts. 18-20.

121 *See Explanatory Report*, *supra* note 5, at 25, para. 20.

122 C.O.E. Convention, art. 12, *supra* note 10.

123 *Explanatory Report*, *supra* note 5, at 33, para. 66.

124 The ambiguity of this provision would allow restriction of data flow regardless of the extent of the privacy interest, as long as there is another legitimate purpose to the restriction.

125 C.O.E. Convention, art. 12, *supra* note 10.

126 *Id.*

ciples without setting maximum standards may frustrate the goal of the treaty because the deviations may create non-equivalent levels of protection. If unequal protection is present, article 12 permits increased restrictions on data flow.

Once a nation enacts stricter protective standards than the Convention requires, the nation may then refuse to transfer data to any country which has less stringent protective standards, even if both nations have complied with the core principles.[127] Thus, the failure to provide maximum privacy standards colors the Convention with the protectionist attitude which it avowedly is trying to avoid.[128] Although requiring free flow of information between any countries complying with the Convention's minimum "core" principles would also solve the problem of uneven standards, it is unlikely that nations would be willing to agree to such a drastic reduction in their control over information. Thus, the proposal of maximum standards defining a range of "equivalency" is a compromise position aimed at formulating some international agreement and avoiding continued reliance on national laws.

The problem with reciprocal or equivalent standards manifests itself again in the area of sanctions and remedies.[129] Since sanctions are left to the contracting parties' discretion, the potential exists for widely divergent sanctions in different countries for similar actions. One nation may maintain that a nation with less severe sanctions offers less protection than its own because its own sanctions provide more deterrence. As a result, the country with stricter laws would be justified in refusing to transfer data outside its national boundaries.

In addition to problems with the Convention's specific provisions, there is the general problem of lack of flexibility. This is a result of inexperience in the area of data protection.[130] The development of

---

[127] For example, one party may have extended the Convention's application to protect data pertaining to juristic persons (article 3, section 2(b) permits an extension to associations, foundations, companies, corporations, and other juristic bodies). If the potential recipient party has not made a similar extension, the first party may legitimately refuse the transfer of data to that country by claiming that the recipient's protection is not equivalent. Under the current language of the Convention, this situation could occur even where the prospective recipient has otherwise complied with the terms of the treaty. Moreover, the first party has almost total discretion, since under article 12, section 3(a) it may refuse to transfer the data merely due to the nature of the data. The other provisions allowing unlimited changes in certain protective standards may undermine the goal of the Convention in similar manners.

[128] *See supra* notes 110-11 and accompanying text.

[129] C.O.E. Convention, art. 10, *supra* note 10. Article 10 states: "The Parties undertake to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

[130] *Hearings*, *supra* note 2, at 324 (statement of Henry Geller, Assistant Secretary of Com-

technological capabilities to conduct the type of activities with which the Convention is concerned has occurred only recently. The newness of the field, combined with continued rapid advancements, indicates that any agreement may quickly become obsolete and unworkable.[131] Perhaps voluntary guidelines that do not impose binding legal sanctions would be more beneficial until there is a better understanding of the precise scope and limits of this new area of telecommunications and transborder information flow.[132] There is no doubt that international agreement can promote the resolution of transborder data flow issues. However, more progress is necessary before a binding treaty is enacted, otherwise many issues may remain unresolved and left to a slow amendment process.[133] Unnecessary and slow procedural processes have no place in today's rapidly developing world of computer technology. The enactment of the Convention in its present form may greatly harm American trade and business. The requirement of equivalent standards of protection may be more difficult to satisfy than the "adequate" protection standard contained in most of the current national legislation.[134] Consequently, the Convention, by not setting maximum standards, may curtail information flow even more than present legislation. An inflexible treaty without provisions for rapid adaptation to technological developments may produce substantial losses. Furthermore, these harms may result whether or not the United States is a party to this treaty, since the United States relies on information flow to and from many countries who would be parties.[135] Thus, it is critical for the United States to take a strong and comprehensive stance on transborder data flow issues to achieve an improved international agreement.

---

merce). Mr. Geller recognized that the relative newness of this body of law could easily lead to the inadvertent use of terminology which would quickly prove to be burdensome.

131 *See generally* Kirby, *supra* note 107, at 55. For example, the notion of "databank" is already outdated under some laws since the manipulation of data may occur without any permanent records. Hondius, *Computers: Data Privacy*, *supra* note 8, at 67.

132 This is one of the advantages to the OECD Guidelines, *see supra* note 11. These guidelines are similar to the C.O.E. Convention, except they are not binding, calling instead for voluntary compliance. For an analysis of these guidelines, see Kirby, *supra* note 107.

133 C.O.E. Convention, art. 21, *supra* note 10. This article sets out the amendment process for the Convention. It involves the convening of several administrative groups, as well as notification of all contracting parties. In addition, each contracting party must approve any amendment. The laboriousness of this process exacerbates the detrimental impact of a binding, inflexible convention. *See* Kirby, *supra* note 107, at 55-56.

134 *See supra* note 54 and accompanying text.

135 The provisions discussed in this comment have been regulations that are permissible between parties to the Convention. The permissible regulation on data transfer to non-parties is even broader. *See* C.O.E. Convention, *supra* note 10.

CONCLUSION

The computer's technological developments that enhance the communications and information industry have also created serious legal problems in the international forum. The central issue involves protecting the privacy interests of individuals, while simultaneously maintaining the free flow of information between countries. Such information flow is the essence of international trade and business, as well as effective government. National attempts at data protection laws have only created more potential conflict. The divergent standards of protection currently existing among nations may easily be used for national, self-interested purposes that eventually will impede international information flow. All nations, their governments, and their citizens will suffer if such a blockage occurs, preventing access to needed information. The time has come for international agreement concerning transborder data flow. However, it still may be too early for a binding treaty, unless that treaty provides sufficient flexibility to respond to rapid technological changes. The information industry is constantly changing, and an inflexible binding treaty may have difficulty adapting to those changes. Additionally, it is essential that any international agreement set maximum and minimum limits on the amount of privacy protection that is permissible or required. Without such limits, even an international agreement may result in conflicting standards of protection, creating the blockage of information transfer.

The Council of Europe has concerned itself with protecting personal privacy with regard to the automatic processing of data; however, its Convention does not sufficiently consider the need for flexibility or the need for maximum limits on protection. Without provisions allowing increased flexibility and providing maximum standards, the present Convention could have a significant adverse impact on international trade in general, and especially on American trade, due to the prominence of the United States in the information industry. The United States, as the world leader in information technology, must take the initiative to formulate new guidelines that will take these essential factors into account. Such an effort may demonstrate that privacy and free flow of information are in fact compatible interests. Hopefully, United States efforts would aid in a new treaty proposal when the communications industry has developed sufficiently to warrant a binding international agreement.

Jane A. Zimmerman