Cornell International Law Journal

Volume 14
Issue 2 *Summer 1981*

Article 1

# The Glabal Phenomenon of Teleinformantics: An Introduction

John M. Eger

# THE GLOBAL PHENOMENON OF TELEINFORMATICS: AN INTRODUCTION

*John M. Eger*†

## INTRODUCTION

We live in a period of enormous political, economic, and social change as the United States, together with other industrialized nations, rushes headlong into a postindustrial, interdependent, information-based age.[1] These changes are driven largely by applications of computer and telecommunications technology that have permitted more communications at greater speeds and over longer distances, virtually shrinking the globe. Indeed, the merging of data-processing and communications technologies has allowed, enhanced, and accelerated global interdependence on both a geopolitical and macroeconomic level. This marriage has also created another kind of technology, information technology, whose value is greater than the aggregate value of its constituent parts and around which a new industry is burgeoning.

The meaning of the word information is broadening. The word information no longer refers only to conventional bodies of statistics, facts, academic knowledge, scientific data, and daily news. Its meaning now comprehends the electronic sensing and computer analysis of the human heartbeat, the electronic impulses that measure physical phenomena in outer space or beneath the sea, and the numeric

---

† B.A., Virginia Military Institute; J.D., John Marshall University; Legal Counsel to the Chairman of the Federal Communications Commission, 1971-1974; Director, White House Office of Telecommunications Policy, 1974-1976. The author expresses his gratitude to Joanna Horsfall for her able research and helpful suggestions.

1. The International Business Machines Corporation, one of the world's largest information providers, described the new age in a recent advertisement:

> Information: there's growing agreement that its the name of the age we live in.
>
> . . . .
>
> . . . [W]e have entered a new era, a post-industrial stage of development in which the ability to put information to use has become critical, not only to the essential production of goods, but to efforts to provide a better life for the individual, as well.

FORTUNE, July 1977, at 42-43. The American Telephone and Telegraph Company and the Xerox Corporation, among others, have employed similar advertising strategies. *See, e.g., id.,* Feb. 25, 1980, at 154; *id.,* Oct. 22, 1979, at 101.

digits that record airplane reservations or transfer funds to and from bank accounts. No matter how they are recorded and stored, whether on film, paper, or magnetic tapes, whether in books, magazines, instruction manuals, movies, videotape, or electronic computer memories, all data are part of this growing information industry.

We depend increasingly on these various forms of information for the growth and health of the economy, the smooth functioning of institutions, and the quality of our individual lives. Information has become a marketable, transferable, exportable commodity—a commodity whose production, sale, and consumption engage more and more of us every day.[2] This is not strictly a domestic phenomenon. West Germany, Japan, France, and other industrialized countries are experiencing and analyzing the same trends. By ascertaining the probable impact of new information technologies and assessing the need for increased governmental intervention, the governments and industries of these countries are attempting to accomodate and foster the orderly introduction of this technology. Nonetheless, the inevitability and the velocity of the change resulting from the introduction of new information technologies have created serious insecurity for the developed and the developing nations alike.

This article uses a relatively new word, teleinformatics, to refer to the confluence of telecommunications and computer technologies and its pervasive economic, social, and political implications. Teleinformatics is still conceptually nascent and, considering its significance, governed by surprising contradiction and ambiguity.[3] Rapid technological development has not only outstripped the existing legal framework. It has also widened the gulf between society's recognition of the occurrence of change and its ability to understand the impact of change. The results are a vast wasteland of misconception and misunderstanding and a growing legal vacuum.[4]

2. By some estimates, the production, processing, and distribution of information goods and services are responsible for nearly one half of the United States gross national product and for an equal share of the nation's wages. N.Y. Times, July 8, 1977, at A1, col. 1; *id.* at 10, col. 1.

3. Even the vocabulary created to describe the phenomenon is cumbersome. The terms informatics, informatique, telematique, communications, and others have been devised, but no two of these terms convey the same meaning.

4. Information technology's tendency to outstrip the law is not an entirely new quality. Decisional law often trails a half step behind change, because it tends to rely on prevailing custom for guiding principles and because of the limitations of *stare decisis*. H. HART & A. SACKS, THE LEGAL PROCESS: BASIC PROBLEMS IN THE MAKING AND APPLICATION OF LAW 138-39, 427-69, 565-620 (tent. ed. 1958). International customary law has similar and severer limitations. *See* I. BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 4-12 (3d ed. 1979).

Although teleinformatics issues demand speedy resolution, developments in information technology have been too sweeping and too rapid to give rise to generally accepted

Data protection laws, telecommunications tariffs and protocols, and informatics plans have arisen around the world. In an effort to accomodate the real and potential impact of an unrestrained global market for information goods and services, individual nations and their subdivisions have adopted these measures without adequate international and even domestic consultation and coordination. There is clearly a movement worldwide toward significantly expanded regulation of commercial and personal information, accompanied by controls on the export and import of all kinds of information and by constraints on the use of technology for the collection, storage, use, and dissemination of data. Nonetheless, on the international level at least, the lack of coordination begs confusion and even chaos.

Information has become a valuable resource with political, social, and cultural implications. Many governments recognize this and are considering policies to protect or promote their national interests. Some have drawn analogies between the information and industrial revolutions that invariably conclude that only the effective and prompt exploitation of information resources and technology will assure a nation a place in the so-called new international economic order and preserve national autonomy.[5]

The Intergovernmental Bureau for Informatics (IBI)[6] defines informatics as "the rational and systematic application of information to economic, social and political development."[7] In practice, this means a carefully crafted national plan governing computer and telecommunications developments to serve the needs and further the aspirations of the individual nation-state. Brazil, for instance, uses the term informatics to describe information policies designed in

principles. Some countries have responded with comprehensive statutes. *See* notes 29-75 *infra* and accompanying text. But this approach is also faulty. Its anticipatory and prophylactic regulatory machinery can stifle the creative and beneficial aspects of information technology.

5. *See, e.g.,* note 111 *infra*.

6. The IBI was created under the auspices of the United Nations, E.S.C. Res. 394 (XIII), 13 U.N. ESCOR, Supp. (No. 1) 50, U.N. Doc. E/518 (1951); E.S.C. Res. 318 (XI), 11 U.N. ESCOR, Supp. (No. 1) 50, U.N. Doc. E/411 (1950); E.S.C. Res. 160 (VII), 7 U.N. ESCOR, Resolutions July 19-Aug. 29, 1948, U.N. Doc. E/966; E.S.C. Res. 22 (III), 3 U.N. ESCOR, Resolutions Sept. 11-Dec. 10, 1946, U.N. Doc. E/233 (1946), and the United Nations Educational, Scientific, and Cultural Organization (UNESCO), UNESCO Res. 2.24, UNESCO 6C/Resolutions 22 (1951).

The organization provides assistance to developing countries in the application of information technology and serves increasingly as a forum for the discussion of informatics policies. HOUSE COMM. ON GOV'T OPERATIONS, INTERNATIONAL INFORMATION FLOWS: FORGING A NEW FRAMEWORK, H.R. REP. No. 1535, 96th Cong., 2d Sess. 28-29 (1980) [hereinafter cited as 1980 House Report]. In 1980, the IBI sponsored the Conference on Transborder Data Flow Policies with participants from sixty-two countries and fifteen international organizations. 3 TRANSNAT'L DATA REP. No. 3/4, at 17 (1980).

7. Informatics: Its Political Impact, IBI Doc. DG 1-04, at 2 (1980).

large part to achieve specific economic goals.[8] Under one such policy, Brazil encourages the expansion of its domestic computer and telecommunications capabilities in part by restricting access to facilities abroad.[9]

As early as 1977, Louis Joinet, then a magistrate of the French Ministry of Justice, framed the debate succinctly: "Information is power," he said, "and economic information is economic power"[10]—a phrase that has been repeated ad continuum, perhaps ad nauseum, ever since. According to Joinet, information has economic value, and the ability to store and process certain types of data may well give one country political and technological advantages over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows.[11] In response to these challenges, the French rendition of an informatics strategy, coined the *télématique* plan,[12] outlines broad areas of authority for the National Government, with a special emphasis on the telecommunications aspect of the new information technologies.[13] The various organs of the

8. *See* Address by Joubert de Oliviera Brizida, Executive Secretary of the Brazilian Special Secretariat of Informatics, 1980 Intergovernmental Bureau for Informatics Conference on Transborder Data Flow Policies in Rome, Italy (June 23, 1980), *printed in* 3 TRANSNAT'L DATA REP. No. 3/4, at 32 (1980).

9. *Id., printed in* 3 TRANSNAT'L DATA REP. No. 3/4, at 32, 33 (1980).

10. Statement by Louis Joinet, Organisation for Economic Co-Operation and Development (OECD) Symposium on Transborder Data Flows and the Protection of Privacy in Vienna, Austria (Sept. 20-23, 1977). *See also* Joinet, *Les Aspects Juridiques, Economiques et Sociaux des Flux Transfrontières de Donées Personnelles,* 1 INFORMATION, COMPUTER AND COMMUNICATIONS POLICY 208, 211 (1979).

11. Joinet, *supra* note 10, at 211. More recently, Alain Madec, a French economist and Chairman of the French Commission on Transborder Data Flows, argued that transborder data flows, unless controlled, threaten the decay of the nation-state by making it subordinate to multinational organizations and enterprises. Madec, *Economic and Legal Aspects of Transborder Data Flows,* in OECD Doc. DST I/ICCP/80.26, at 33, 37 (1980) [hereinafter cited as Madec paper].

12. The French term *informatique* generally refers to data processing. Simon Nora and Alain Minc coined the word *télématique* to describe the convergence of telecommunications and data-processing technologies. Stratte-McClure, *French Telecommunications: Digital Technology and the Telematique Program,* SUPP. TO ELECTRONIC NEWS & SCIENTIFIC AMERICAN 13 (1980). *See* S. NORA & A. MINC, L'INFORMATIZATION DE LA SOCIÉTÉ 17 (1978) [hereinafter cited as Nora-Minc report]. With the development of the *télématique* plan, the latter term has come to refer to information policy as well.

In 1976, the President of France commissioned the Inspector General of Finances, Simon Nora, to investigate the computerization of French society and to make suitable proposals concerning this matter to the Government. Nora-Minc report, *supra,* at 3-4. The resulting report to the French President, the Nora-Minc report, was the catalyst and the blueprint for the developing *télématique* plan. The report was essentially the first of its kind in the world. Because it examines both the technology and its effects on matters of national importance, the report serves as a model for other nations. Moreover, the report's sometimes startling findings did much to make informatics prominent among public issues. The report forecasts, for instance, a thirty percent reduction, possibly within one decade, in the number of jobs provided by France's insurance and banking industries. *Id.* at 36.

13. *See, e.g.,* BUS. WEEK, Oct. 1, 1979, at 86.

French postal and telecommunications agency (PTT)[14] are expected to implement many of the programs.[15] The Government has also established a cabinet level position with responsibility for the full development of the *télématique* concept.

The new office coordinates the activities of governmental organs whose areas of responsibility overlap and promotes various applications with its generous budget.[16] As compared with the informatics plans of other nations, the French program has plentiful resources, a highly developed focus, and a special urgency. The *télématique* plan concentrates on two levels, social and industrial. By promoting the general computerization of society, the plan will develop the domestic market. Selective trade and telecommunications tariffs and regulations, including the taxation of business information, will allow France to gain important economic advantages over the United States in the information market.[17]

In teleinformatics policies, economic issues often obscure human rights issues. The quantification and taxation of information transiting international borders are of particular concern. Municipal and international law have long recognized the importance of protecting the expression of ideas. Article nineteen of the Universal Declaration of Human Rights proclaims that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[18] Although the Declaration is not a legal instrument,[19] it is part of the fabric of international law[20] and is widely understood

14. The European PTTs are state agencies. They generally own the facilities and regulate the activities of the post and telecommunications.

15. *See* note 13 *supra*. *See generally* Stratte-McClure, note 12 *supra*.

16. *See* Straffe-McClure, *supra* note 12, at 5.

17. *See generally id.*

18. Universal Declaration of Human Rights, G.A. Res. 217 (III) U.N. Doc. A/810, at 71, art. 19 (1948).

19. *E.g.*, H. LAUTERPACHT, INTERNATIONAL LAW AND HUMAN RIGHTS 397-408 (2d ed. 1968).

20. *E.g.*, I. BROWNLIE, *supra* note 4, at 569-71. Brownlie states that the Declaration has indirect legal effect in two ways. First, some of the Declaration's provisions constitute general principles of law. Second, the Declaration serves as an authoritative guide to the interpretation of the United Nations Charter. *Id.* at 571. Article 55 of the Charter states that "the United Nations shall promote: . . . (c) universal respect for, and observance of, human rights and fundamental freedoms for all . . . ." U.N. CHARTER art. 55. Article 56 provides that "[a]ll Members pledge themselves to take joint and separate action in cooperation with the Organization for the achievement of the purposes set forth in Article 55." *Id.* art. 56. For a view contrary to that of Brownlie, see H. LAUTERPACHT, *supra* note 19, at 408-14. Lauterpacht also rejects the argument that the Declaration is binding on the organs of the United Nations. *Id.* at 414-17. Lauterpacht ascribes to the Declaration neither direct nor indirect legal authority, but rather a limited moral authority. *Id.* at 417-25.

to be the foundation for the principle of a free flow of information among nations.[21]

Nonetheless, information has also become a commodity, both as an intermediate good and as a good of final consumption. The economic importance of information in this expanding trade in intangibles forces us to decide which information should be taxable and subject to traditional trade restrictions and which information should be allowed free and open transit to protect the movement of ideas across national borders.

The IBI has created three international working parties to analyze the economic and commercial impact of transborder data flows, data protection and international law, and the international environment for transborder data flows.[22] The discussion in the working parties' final reports may range from clarification of the protection to be afforded certain interests affected by transborder data flows to suggestions for the regulatory means to achieve this protection.[23] Perhaps most important, the working parties will consider whether a "universal data protection instrument"[24] should be prepared in order to bring into international uniformity the rights and responsibilities entailed in transborder data flows.[25]

---

21. *See, e.g.,* Address by F.A. Bernasconi, Director General of the Intergovernmental Bureau for Informatics, 1980 Intergovernmental Bureau for Informatics Conference on Transborder Data Flow Policies in Rome, Italy (June 23, 1980), *printed in* 3 TRANSNAT'L DATA REP. No. 3/4, at 3, 3 (1980); Address by Joubert de Oliviera Brizida, *supra* note 8, *printed in* 3 TRANSNAT'L DATA REP. No. 3/4, at 32, 34 (1980).

The Group of Experts that drafted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data for the OECD cites the International Covenant on Civil and Political Rights, G.A. Res. 2200 (XXI), 21 U.N. GAOR, Supp. (No. 16) 49, U.N. Doc. 6316 (1966), as supporting the principle of a free flow of information. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C (80) 58 (Final), app. para. 11 (Oct. 1, 1980), *reprinted in* OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 18 (1981) [hereinafter cited as OECD Guidelines].

22. International Working Parties on Transborder Data Flow, IBI Doc. TDF 100 (1980). The findings and proposals of the working parties are likely to be controversial. The IBI wants the working groups to examine growing points of friction between the countries of the southern hemisphere and those of the northern hemisphere. In particular, the IBI has asked the working parties to investigate whether the developing countries are subject to any inequity by having to export unprocessed data in return for little compensation while paying high prices in scarce hard currency for imported processed data. *Id.* at 1. The IBI has also requested the working parties to examine the use of information collected by earth-sensing satellites and the institution of regulations requiring administrative consent before information may be transmitted abroad. *Id.* at 2-3.

23. *Id.* at 2.

24. *Id.*

25. The IBI suggests that the "problem of balance in information flow" may require the creation of an international mechanism to regulate transnational information networks. *Id.* at 3.

Alain Madec, Chairman of the French Commission of Transborder Data Flows, published an assessment of the economic and legal aspects of international data flows.[26] Madec presents a system of information classification that could serve as the basis for, among other things, the imposition of customs duties and value-added taxes on transborder data flows.[27] The United States has also examined the characteristics of data flows.[28] Unlike the French study, the United States initiative fulfills an educational function and does not discuss the possible uses for a system of information classification.

Teleinformatics raises not only commercial issues, but broader questions of interest to society generally. By undercutting the significance of physical distances, for example, global satellite telecommunications may have exacerbated rather than reduced cultural differences. Charges of electronic colonialism and cultural imperialism are not necessarily masks for economic protectionism. International cultural relations are as old as the flow of people and ideas across frontiers. Interaction between diverse peoples and cultures, however, has accelerated dramatically in recent years. Moreover, the general population's greater participation in world affairs presents unprecedented opportunities to bring about more cooperation. Nonetheless, it is now evident that neither expanded cross cultural communication nor increased trade necessarily leads to harmony. Thus, all of these issues present a challenge to policymakers, international business, and the international legal community.

What follows is an attempt to survey the rapidly emerging first wave of potential barriers to international information flows and the threat posed to a world already highly dependent on the free flow of information and the unrestricted use of information technology. These potential barriers can be divided into five areas: privacy and data protection laws; telecommunications tariffs, standards, and protocols; informatics strategies; national responses to computer vulnerability; and new links between national sovereignty and information. Finally, this article examines a recent proposal for the development of a national information policy in the United States.

---

26. Madec paper, note 11 *supra*. Madec's assessment and proposals are not an expression of official French policy. *Id.* at 33 n.1.

27. *Id.* at 39-43.

28. U.S. NAT'L TELECOMMUNICATIONS & INFORMATION ADMINISTRATION, WORKING PAPER, AN APPROACH TO IDENTIFYING THE LEGAL AND ECONOMIC ISSUES OF TRANSBORDER DATA FLOW (1980).

# I

## PRIVACY AND DATA PROTECTION

Privacy, or fair information practice as it is known in the United States,[29] has emerged from a position of total obscurity in just fifteen years.[30] The collection, use, and storage of large volumes of intimate

29. The Secretary of the U.S. Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems first coined the term fair information practice. SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS xx (1973). The Secretary's Advisory Committee recommended the enactment of a code of fair information practice that would give legal effect to five basic principles for the protection of privacy in relation to automated personal data systems: (1) the existence of no personal data record-keeping system should remain secret; (2) the individual should have some means of discovering what information about him is in a record and how it is used; (3) the individual should have some means of preventing information about him that was obtained for one purpose from being used or made available for other purposes without his consent; (4) the individual should have some means of correcting or amending a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. *Id.* at xx-xxi.

The Privacy Act of 1974, 5 U.S.C. § 552a (Supp. III 1979), expanded these five principles into eight: (1) the existence of no personal data record-keeping system shall remain secret, and there shall be a policy of openness about an organization's personal data record-keeping policies, practices, and systems; (2) an individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information; (3) an individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information; (4) there shall be limits on the types of information an organization may collect about an individual as well as certain requirements with respect to the manner in which it collects that information; (5) there shall be limits on the internal uses of information about an individual within a record-keeping organization; (6) there shall be limits on the external disclosures of information about an individual a record-keeping organization may make; (7) a record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices that assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and that the information itself is current and accurate; and (8) a record-keeping organization shall be accountable for its personal data record-keeping policies, practices, and systems. U.S. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 497-536 (1977).

30. The Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (current version at 5 U.S.C. § 552 (Supp. III 1979)) was perhaps the first congressional act relating to privacy protection with respect to the collection and use of personal data. By opening the records of Federal Government agencies to public inspection, the Freedom of Information Act establishes a rule in part contrary to the interests of privacy protection. Thus, some have categorized the Act among those public policy interests that compete with privacy protection. *E.g.,* U.S. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 29, at 24-26 (1977). On the other hand, by providing the individual with access to information in governmental records, the Freedom of Information Act, especially after the enactment of the Privacy Act of 1974, 5 U.S.C. § 552a (Supp. III 1979), complements privacy protection. *E.g., id.* at 25, 508-12. *See also* note 29 *supra.*

The Group of Experts that drafted the OECD Guidelines suggests 1973 as the year after which OECD member nations generally began to enact privacy and data protection statutes. OECD Guidelines, *supra* note 21, at 17.

information raise fears that technology will be exploited to misuse personal data. Moreover, on a human rights level, the individual must be able to discover, correct, and update information about him, if he is to have some measure of control over information[31] used by third parties in making decisions about him. This need is as pressing in the United States as it is abroad. The United States has not, however, pursued privacy protection as avidly and comprehensively as have other nations (primarily Western European nations).

Several studies completed in the United States,[32] both private and public, have helped to bring about legislative measures securing to the individual a right to fair information practice.[33] Altogether, twenty-two nations either have adopted or are in the process of

---

The 1970 Data Protection Act of the West German State of Hesse was one of the first laws to address directly the hazards to privacy created by computer technology. Datenschutzgesetz vom 7. Oktober 1970, Gesetz- and Verordnungsblatt I S. 625-627 i.d.F. des Hess. Gesetzes zur Anpassung des Landesrechts an das Einführungsgesetz zum Strafgesetzbuch vom 4. September 1974 (GVBl. I S. 361) Gesetz- und Verordnungsblatt II 300-10, *as cited in* DATA PROTECTION LEGISLATION 113-20 (U. Dammann, O. Mallmann & S. Simitis eds. 1977). The Hessian statute and an earlier, but defeated British bill, the 1969 Data Surveillance Bill H.C. 1968-1969, vol. I, 627 (1969), became the focus for the consideration of privacy and data protection in the early 1970's.

31. *E.g.,* note 29 *supra*. The Secretary's Advisory Committee suggested, however, that privacy be viewed in a contractual framework. The individual, according to the Committee, will have to trade some control over information about him in exchange for the services that a record-keeping organization provides, but both parties to the exchange should participate in setting the terms of the exchange. SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, *supra* note 29, at xx. The Privacy Protection Study Commission, for its part, recommended against extending the Privacy Act of 1974, 5 U.S.C. § 552a (Supp. III 1979), to organizations outside the Federal Government. U.S. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 29, at 497.

32. *E.g.,* L. HARRIS & ASSOCIATES INC. & A. WESTIN, THE DIMENSIONS OF PRIVACY (1979); D. PARKER, S. NYCUM & S. OURA, COMPUTER ABUSE (1973); SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, note 29 *supra*; U.S. NAT'L COMMISSION ON ELECTRONIC FUND TRANSFERS, EFT AND THE PUBLIC INTEREST (1977).

33. On the Federal level, these statutes include the Freedom of Information Act, 5 U.S.C. § 552 (Supp. III 1979); the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (Supp. III 1979); the Equal Credit Opportunity Act, 15 U.S.C. §§ 1691, 1691b-1691f (1976); the Fair Credit Billing Act, 15 U.S.C.A. §§ 1601-1602, 1610, 1631, 1632, 1637, 1666-1666j (West Supp. 1981); the Fair Debt Collection Practices Act, 15 U.S.C. §§ 1601 note, 1692-1692o (Supp. II 1978); the Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681-1681t (West Supp. 1981); and the so-called Buckley Amendment, 20 U.S.C.A. § 1232g (West Supp. 1981). For a list of state statutes relating to privacy protection, see R. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 1978-79 (1978).

The ninety-fifth Congress introduced approximately 100 bills addressing privacy protection. During the ninety-sixth Congress, the Carter administration supported comprehensive privacy protection legislation covering medical, research, financial, and insurance records as well as a measure protecting information held by newsmen. OFFICE OF MANAGEMENT & BUDGET, FIFTH ANNUAL REPORT OF THE PRESIDENT ON THE IMPLEMENTATION OF THE PRIVACY ACT OF 1974, at 15-19 (1979). Congress approved the latter measure on October 13, 1980. Privacy Protection Act of 1980, 42 U.S.C.A. §§ 2000aa, 2000aa-5 to -7, 2000aa-11 to -12 (West Supp. 1981).

adopting privacy and data protection laws.[34]

Although each nation's legislation has its own peculiarities, some striking similarities exist among the data protection laws of Western Europe.[35] Generally, these laws require the registration or licensing[36] of both private[37] and public[38] data banks. Some statutes include manually processed files, but most concentrate on automatically processed files.[39] Limitations are often imposed on the length of time data can be retained,[40] and the secondary use, sharing, and dissemination of data are regulated.[41] Rights of access[42] and notice[43] as well as a right to correct incorrect information[44] is created. These laws generally impose a responsibility for the security and confidentiality of records kept.[45] Many Western European laws establish as a regulatory possibility the requirement of prior authorization for transmitting data abroad.[46] There are sanctions,[47] including imprisonment,[48] for violations. Finally, many Western European countries have created new national, central authorities responsible for the administration of their data protection schemes.[49]

The global ground swell of support for individual rights of privacy is highly credible. Nevertheless, privacy laws, particularly those taking a comprehensive data protection approach to record

34. Australia, Austria, Belgium, Canada, Denmark, Finland, France, West Germany, Iceland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and Yugoslavia. 3 TRANSNAT'L DATA REP. No. 2, at 15 (1980).

35. For a more thorough examination of the data protection laws of Western Europe, see Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers?,* 10 L. & POL'Y INT'L BUS. 1055, 1065-78 (1978). *See generally* F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE (1975).

36. *E.g.,* the West German Federal Data Protection Act, Bundesdatenschutzgesetz (BDSG), 1980 BGBl S. 1469, § 19(4). DATA PROTECTION LEGISLATION, *supra* note 30, at 70-107, contains an unofficial translation of the West German statute's predecessor, 1977 BGBl S. 201.

37. *E.g.,* Bundesdatenschutzgesetz (BDSG), 1980 BGBl S. 1469, §§ 1(2)2-3, 22, 31.

38. *E.g., id.* §§ 1, 7.

39. The West German statute, for instance, applies to nonautomated files only to a limited extent. *Id.* § 1.

40. *Cf. id.* § 14(2) (after the accomplishment of the purpose, data may be retained, but only for scientific purposes and other overriding interests).

41. *E.g., id.* §§ 10, 11, 14(2), 24, 27(2), 32, 35(2), 36 and Annex to § 6(1), at 6.

42. *E.g., id.* §§ 4(1), 13, 26(2), 34(2). Some of these provisions establish rights, others impose duties.

43. *E.g., id.* §§ 12, 26(1), 34(1). Some of these provisions establish rights, others impose duties.

44. *E.g., id.* §§ 4(2)-(4), 14, 27, 35. Some of these provisions establish rights, others impose duties.

45. *E.g., id.* §§ 5, 6, 8.

46. *E.g., id.* §§ 11, 32(3).

47. *E.g., id.* §§ 41-42.

48. *E.g., id.* § 41(1)2, (2).

49. *E.g., id.* §§ 15-21.

management, will pose serious threats to international commerce if fully implemented and enforced.[50]

Despite a shared point of departure, at least on the manifest level of human rights, crucial differences exist between the United States and Western European approaches to privacy protection. In the United States, privacy legislation is pursued on an incremental, "as needed" basis.[51] Other nations have adopted an omnibus approach.[52] Similarly, United States privacy laws afford protection only to individuals or natural persons. In contrast to the United States, Western Europe continues to press for the coverage of legal persons,[53] including corporations, associations, and trade unions,[54] even though the inclusion of legal persons raises little-understood problems in terms of competition, trade secrets, and reduced efficiency.[55] Moreover, comprehensive data protection presents Western European governments with administrative problems far removed from any concern for individual privacy. Because of the emerging informatics strategies, a permanent shift away from the protection of individual privacy alone and toward data protection and the inclusion of a wide range of economic, political, and personal information seems clear and inevitable.

The Organisation for Economic Development and Co-Opera-

50. Western European data protection laws lay down the same rules for all uses and disclosures of personal information. Thus, these statutes tend to protect the information contained in data collections. In contrast to the Western European approach, United States privacy law tends to protect the individual. For instance, the Privacy Act of 1974, 5 U.S.C. § 552a (Supp. III 1979), allows case-by-case determination whether or not personal data is private. For a comparison of the two approaches, see 1980 House Report, *supra* note 6, at 38-40.

51. 1980 House Report, *supra* note 6, at 38-39.

52. The West German Federal Data Protection Act, for instance, establishes relatively identical standards for all data bases, both those in the private sector and those in the public sector. *See* notes 37-38 *supra*.

53. In its strict sense, the word privacy does not apply to legal or nonnatural persons. U.S. DEP'T OF COMMERCE, NAT'L BUREAU OF STANDARDS, CONTROLLED ACCESSIBILITY BIBLIOGRAPHY 2 (1973). The preferred term is confidentiality, and even this word is used in reference to data, not nonnatural persons. *Id.*

54. The data protection laws of Austria, Denmark, Luxembourg, and Norway protect information about legal persons as well as information about natural persons. 3 TRANSNAT'L DATA REP. No. 2, at 16 (1980).

55. One spokesman for the United States financial industry, the Chairman of the Board of Directors of Citibank, argues, however, that protection of the privacy of legal persons deserves at least as much attention as protection of the privacy of natural persons. He suggests that efforts to protect the privacy of natural persons, at least insofar as banking records threaten individual privacy, will be ineffectual, unless banks have the right to protect the confidentiality of their records. Finally, he implies that measures protecting the privacy of legal persons would not substantially add to the costs of protecting the privacy of natural persons, because information about legal and natural persons is frequently inseparable. Letter from Walter B. Wriston to U.S. Representative Richardson Preyer (May 23, 1980) (on file at *Cornell International Law Journal*).

tion (OECD),[56] the Council of Europe,[57] and the European Community (EC),[58] have all considered policy on privacy and data protection. The United States has participated in the formulation of only the nonbinding[59] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[60]

The United States is now actively promoting the OECD Guidelines as minimum standards for corporate conduct.[61] Despite the nonbinding nature of the Guidelines, it is anticipated that their

56. OECD Guidelines, note 21 *supra*.

57. Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108 [hereinafter cited as Council of Europe Convention].

58. The European Parliament's resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing, 22 O.J. EUR. COMM. (No. C 140) 34 (1979); and the so-called Bayerl Report, on which the resolution is based, [1979-1980] EUR. PARL. DOC. (No. 100) (1979).

59. The OECD Council "recommends" the OECD Guidelines to the OECD member nations. OECD Guidelines, *supra* note 21, at 7. Moreover, the document states that its principles "should" be observed. *E.g., id.* at 10. *See id.* at 27.

60. OECD Guidelines, note 21 *supra*. Australia, Canada, Ireland, Turkey, and the United Kingdom have abstained from the OECD Guidelines at present. *Id.* at 5 n.1.

61. There are several reasons why United States companies should comply with the OECD Guidelines. Voluntary adherence to the OECD Guidelines may satisfy those nations that become signatories to the Council of Europe Convention. If voluntary adherence proves illusory, these signatory nations may urge the United States to accede to the Council of Europe Convention. *See* Council of Europe Convention, *supra* note 57, art. 23. The OECD Guidelines do not protect the privacy of legal persons, but the Council of Europe Convention permits parties to the Convention to extend the Convention's scope to include groups, whether they be legal or not. OECD Guidelines, *supra* note 21, at 9, 10, 24, 26, 28; Council of Europe Convention, *supra* note 57, art. 3.2.*b*. A party that has not made the article 3.2.*b* extension may not claim the application of the Convention to groups by a party that has made this extension. *Id.* art. 3.5. By negative implication, an extending party may require all other parties—whether or not they have themselves made the article 3.2.*b* extension—to apply the Convention to transborder data flows concerning groups when these flows originate from the territory of the extending party. Indeed, an extending party might base this claim simply on the Convention's authorization of "extensions." *Id.* art. 3.2.*b*, .5. The Convention does provide that a party shall not subject transborder data flows going to other parties to special authorization for the sole purpose of protecting privacy. *Id.* art. 12.2. Nonetheless, the Convention allows parties to derogate from the principle of article 12.2, unless the receiving party provides protection equivalent to that of the transmitting party. *Id.* art. 12.3.*a*. Thus, the Convention more or less explicitly permits a party to deny the export of data under certain circumstances. Finally, the OECD Guidelines recommend that OECD member nations merely "establish legal, administrative or other procedures or institutions" that will, among other things, "provide for reasonable means for individuals to exercise their rights . . . ." OECD Guidelines, *supra* note 21, at 12. OECD member nations should also "establish procedures to facilitate . . . mutual assistance in the procedural and investigative matters involved." *Id.* In contrast, the Council of Europe Convention requires parties to designate one or more authorities responsible for mutual assistance. Council of Europe Convention, *supra* note 57, art. 13. Moreover, "any person resident abroad" must have the option of submitting a request concerning information about him to the designated authority of the territory in which he resides. *Id.* art. 14.1-.2. Thus, the Convention stops short of requiring parties to establish central authorities with responsibility for privacy and data protection. Nonetheless, the designated authorities may resemble and may in fact become central authorities with broad powers.

adoption in spirit will do much to ameliorate or eliminate many of the concerns other nations express about the security of personal data that transit United States borders or are processed within the United States.

When it negotiated the Guidelines, the United States fully recognized the Western European bias toward anticipatory, prophylactic, and omnibus legislation and the desire of many OECD member nations to produce a binding treaty. While the OECD was drafting the Guidelines, the Council of Europe was busy negotiating the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data.[62] The Convention, unlike the OECD Guidelines, is binding and will assume treaty status following ratification by five acceding countries.[63] The Convention is potentially far more restrictive than the OECD Guidelines[64] and, furthermore, requires acceding countries to pass implementing legislation.[65]

Only widespread adherence to the OECD Guidelines in the United States, by her private corporations, and in other non-European countries can demonstrate the necessary commitment to the principles of privacy protection. The absence of such an affirmation of sincerity will render the Guidelines' voluntary approach a useless exercise, and United States multinational corporations may find restrictive, mandatory codes of conduct, such as the Council of Europe Convention, their only alternative.

The Council of Europe Convention places restrictions on the treatment of personal data that are similar to those in the OECD Guidelines:

> Personal data undergoing automatic processing shall be:
>
> *a*. obtained and processed fairly and lawfully;
>
> *b*. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
>
> *c*. adequate, relevant and not excessive in relation to the purposes for which they are stored;
>
> *d*. accurate and, where necessary, kept up to date;
>
> *e*. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[66]

---

62. Council of Europe Convention, note 57 *supra*.

63. *Id.* art. 22.2.

64. *See* note 61 *supra*.

65. Council of Europe Convention, *supra* note 57, art. 4.1.

66. *Id.* art. 5. The "Collection Limitation Principle" in the OECD Guidelines is comparable to article 5.*a* in the Convention. OECD Guidelines, *supra* note 21, at 10. The "Purpose Specification Principle" in the OECD Guidelines is comparable to article 5.*b* in the Convention. *Id.* Because it explicitly requires initial specification no later than the time of data collection and subsequent specification whenever the purpose changes, the Guidelines' provision is arguably more demanding than the Convention's provision. The Guidelines' "Data Quality Principle" is comparable to art. 5*c-d* in the Convention.

Both the OECD Guidelines and the Council of Europe Convention apply to the public and private sectors,[67] but the Convention covers only automatically processed personal data.[68] At the time of signature, however, parties to the Convention may modify the Convention's coverage to include legal persons (and other organizations such as partnerships) and manually processed files.[69] In the same way, parties may exempt certain classes of files from coverage.[70] Additions and exemptions become reciprocal; thus, a party that exempts certain records from coverage may not expect the other parties to honor similar records with the provisions of the Convention.[71] With this flexibility, the Council of Europe Convention may in time closely resemble the OECD Guidelines. More skeptical observers, however, might perceive this same flexibility as presenting an opportunity to impose more restrictive and costly regulations.

It is not yet clear whether privacy and data protection laws and international codes of conduct will become instruments of the new protectionism. Clearly, some countries may easily design or manipulate their privacy and data protection laws in order to achieve political, cultural, and economic ends unrelated to the protection of individual privacy.

The EC, which has also considered policy on privacy, has from the beginning approached transborder flows of all kinds of information with economic considerations in mind. Unlike the Council of Europe and the OECD, whose real intentions may often be veiled in the negotiating process, the EC has taken direct aim at the capture of a large share of the global teleinformatics market[72] while noticing privacy as only a secondary concern. The so-called Bayerl Report[73]

---

*Id.* The data quality principle does not explicitly require data to be not excessive in relation to the specified purposes, but this might be read into the Guidelines' requirements of relevance.

The Guidelines' purpose specification principle requires the use of data to be limited to specified purposes, *id.*, but there is no provision covering the form in which data is stored after the accomplishment of these purposes. *But cf. id.* at 30 (the explanatory memorandum notes that, '..hen data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form."). Finally, both the OECD Guidelines and the Council of Europe Convention require data controllers to take security measures for the protection of personal data. *Id.* at 10; Council of Europe Convention, *supra* note 57, art. 7.

67. OECD Guidelines, *supra* note 21, at 9, 27. Council of Europe Convention, *supra* note 57, art. 3.1.

68. Council of Europe Convention, *supra* note 57, art. 3.1. The OECD Guidelines do not limit their application to automatically processed data. OECD Guidelines, *supra* note 21, at 9, 24-27.

69. Council of Europe Convention, *supra* note 57, art. 3.2.*b-c*.

70. *Id.* art. 3.2.*a*.

71. *Id.* art. 3.4. *See* note 61 *supra*.

72. WORLD BUS. WEEKLY, Oct. 29, 1979, at 28.

73. [1979-1980] EUR. PARL. DOC. (No. 100) (1979). *See also* note 58 *supra*.

articulates the EC's privacy policy. The report stresses the importance of harmonizing data protection standards internationally to avoid placing unnecessary impediments in the way of international commerce. Of course, the report recognizes the legitimacy of a concern for the protection of individual privacy, but the EC has postponed any action until it has considered whether or not it should supplement[74] or accede[75] to the Council of Europe Convention.

The impact of increased privacy regulations and legislation on teleinformatics issues will be far reaching. It is still unclear in some cases when the protection of human rights ends and the protection of national industries begins. The undue inhibition of international transfers of information will interrupt or obstruct international commerce. The line of demarcation between personal privacy and commercial issues became clearer over the past eighteen months, however, as nations, with France in the lead, began to announce their national plans for economic prosperity in commercial rather than human rights terms.

## II

## TELECOMMUNICATIONS TARIFFS, STANDARDS, AND PROTOCOLS

In contrast to privacy and data protection laws, the implementation of tariffs, higher standards, differing protocols, and policies limiting the import and use of foreign equipment raises barriers blatantly economic in nature. These barriers can more directly affect the cost, management, control, and effectiveness of the information systems of a multinational corporation.

Louis Pouzin, one of Western Europe's leading systems designers, argues that telecommunications tariffs and regulations have proved to be the most effective means for preventing the exchange of information.[76] An example is the cost of leased telephone lines in Western Europe where the price per mile of international lines is three to five times that of domestic lines.[77] According to Pouzin, the Western European PTTs persistently discourage international com-

74. Letter from Etienne Davignon to the President of the European Parliament (Jan. 16, 1979), *reprinted in* [1979-1980] EUR. PARL. DOC. (No. 100) Annex III (1979).

75. Resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing, *supra* note 58, at 36, para. 15.

76. Address of Louis Pouzin in Las Vegas, Nevada (Mar. 6, 1978).

77. Telecommunications regulations may pose barriers to national communications as well. The sharply divergent long distance telephone rates among Canadian provinces are an example. CONSULTATIVE COMMITTEE ON THE IMPLICATIONS OF TELECOMMUNICATIONS FOR CANADIAN SOVEREIGNTY, CANADIAN DEP'T OF COMMUNICATIONS, TELECOMMUNICATIONS AND CANADA 27-28 (1979) [hereinafter cited as Clyne Committee Report].

munications.[78] The PTTs want more than control; they want revenues from the burgeoning growth in data communications. Thus, although the user may once have found the PTTs willing to offer dedicated facilities for lease, so-called private, leased lines, he now finds these facilities unavailable or available at an ever-increasing cost.

The leasing of private lines may never have been popular with the PTTs, but it was a technological necessity, because users' needs were too sophisticated for the public networks to accomodate. Similarly, charging for private, leased lines on a flat fee basis was not a matter of choice, rather it arose largely from the need to charge in a costwise manner. The technical capability to discern what volumes of data were transiting the lines would have been expensive, leaving aside the questionable ethical character of the eavesdropping such monitoring would have required. Nevertheless, even though the demand for private, leased lines continues to increase, the PTTs' greater technical sophistication permits them to question what they have in the past tolerated as a necessary evil.

The PTTs argue that multinational corporations, with their private, leased lines, erode actual and potential revenues for the PTTs by developing their own international, electronic message systems, computer-to-computer networks, and other information systems. These private systems compete directly or indirectly with the existing telex services offered by the PTTs and with the electronic mail services they are rapidly developing.[79]

A first step in the elimination of private, leased lines occurred within the International Telegraph and Telephone Consultative Committee (CCITT).[80] The CCITT is the administrative arm of the International Telecommunication Union (ITU)[81] charged with responsibility for international telecommunications regulation. At a

78. Address of Louis Pouzin, note 76 *supra*. Pouzin suggested that the PTTs indirectly promote the installation of domestic data-processing facilities by setting high international tariffs. *Id.*

79. For a description of the competition among the PTTs themselves concerning their new videotex system, see Clyne Committee report, *supra* note 77, at 61-62.

80. In reaching its decisions, the CCITT permits each country one vote. The CCITT's recommendations specify technical and operational confines for international telecommunications. Because the provision of international telecommunications services requires international cooperation, service providers generally observe the CCITT's recommendations, even though they are not legally binding. *See generally* Jacobson, *The International Telecommunication Union: ITU's Structure and Functions,* in JOHN & MARY R. MARKLE FOUNDATION, GLOBAL COMMUNICATIONS IN THE SPACE AGE app. C (1972); Voge, *The International Telecommunication Union: Its Functions and Structure,* in *id.* app. E.

81. The ITU has 154 member nations and makes its headquarters in Geneva, Switzerland. O'Neill, *The International Telecommunication Union,* TELECOMMUNICATION, Feb. 1981, at 25. The organization seeks

1977 meeting of CCITT Study Group III, the Italian delegation urged the Group to discourage the introduction of new private, leased lines.[82] The proposal also suggested that the Group study the possibility of transferring traffic transiting the private, leased lines to the public networks for tariffing on a volume sensitive basis.[83] Perhaps more important, the Western European PTTs already subject the private, leased lines of the Society for Worldwide Interbank Financial Telecommunications (SWIFT)[84] to a tariff computed in part on the basis of volume.[85]

Actions in the United States have further enlarged the controversy over private, leased lines. The Federal Communications Commission (FCC) has initiated a proceeding intended to eliminate any tariff restriction on the resale and shared use of international telecommunications facilities.[86] By allowing greater competition in the provision of telecommunications services, the permissive resale and

---

a) to maintain and extend international cooperation for the improvement and rational use of telecommunications of all kinds; b) to promote the development of technical facilities and their most efficient operation with a view to improving the efficiency of telecommunications services, increasing their usefulness and making them, so far as possible, generally available to the public; c) to harmonize the actions of nations in the attainment of those ends.

*Id.* at 26. The ITU began in 1865 as the International Telegraph Union. *Id.* at 25. Today, it has two main administrative arms, the International Radio Consultative Committee and the International Telegraph and Telephone Consultative Committee. Jacobson, note 80 *supra*. The ITU pursues its goals by sponsoring international conferences and meetings, publications, exhibitions, and technical cooperation. For a history of the ITU's conferences, see M. FELDMAN, THE ROLE OF THE UNITED STATES IN THE INTERNATIONAL TELECOMMUNICATION UNION AND PRE-ITU CONFERENCES (1976).

82. CCITT Study Group III, Rates for Private Leased Circuits, Doc. COM III-No. 6-E (Feb. 1977) (Italian Administration). One purpose of the Italian proposal was the preservation of PTT revenues. *Id.*

83. *Id.* A working group of CCITT Study Group III ultimately rejected that part of the Italian proposal concerning the provision of new private, leased lines. CCITT Study Group III, Report on the Meeting Held in Geneva from 1 to 3 May 1978, Doc. COM III-No. 51-E, at 4 (July 1978) (Working Party III/1). The Working Party is still studying the proper tariff structure for private, leased lines. *Id.* at 10.

84. In 1973, a group of financial institutions organized SWIFT as a nonprofit, cooperative society headquartered in Belgium. Nacamuli, *SWIFT: Objectives, Standardization, Availability, Auditability, Security, Privacy and Liability,* 3 TRANSNAT'L DATA REP. No. 6, at 7, 7 (1980). SWIFT develops and operates an international communications network to serve the international banking community. *Id.* SWIFT began operating in 1977 and now has nearly 750 members in twenty-seven countries. *Id.*

85. Minutes of the Meeting of Conference of European Postal and Telecommunications Administrations (CEPT) Study Group "General Principles and Tariffs" (Florence, Italy Oct. 7, 1975), *reprinted in* CENTER FOR COMMUNICATIONS MANAGEMENT, INC., NEW TRENDS IN INTERNATIONAL TELECOMMUNICATIONS app. B.

86. Regulatory Policies Concerning Resale & Shared Use of Common Carrier Int'l Communications Servs., 77 F.C.C.2d 831, 832 (1980).

The FCC defines resale as "an activity wherein one entity subscribes to the communications services and facilities of another entity and then reoffers the communications service and facilities to the public (with or without 'adding value') for profit." Regulatory Policies Concerning Resale & Shared Use of Common Carrier Servs. & Facilities, 60 F.C.C.2d 261, 271 (1976), *amended on recon.,* 62 F.C.C.2d 588 (1977), *aff'd sub nom.*

shared use of international facilities would wrest control of international communications from the PTTs. In their responses to the FCC proceeding,[87] foreign telecommunications administrations have made clear their opposition. They may eliminate, or increase sharply the cost of, the private, leased line, if the United States removes, for its part, the restrictions that prevent the resale and shared use of facilities communicating traffic internationally.[88]

From the United States perspective, the FCC initiative is nothing more than an attempt to foster the provision of more varied and economical international data communications services and to bring the regulations governing these services in line with those governing domestic telecommunications.[89] This attempt to impose a domestic initiative onto the international market has drawn mixed reactions. Foreign PTTs and large United States corporate users of telecommunications facilities oppose lifting the restrictions on resale and shared use. The PTTs want to preserve control. The large corporate users fear a Western European reaction eliminating the private, leased lines, on which they depend. Only potential market entrants support the proceeding.

Despite corporate dependence on private, leased lines, the trend is clearly toward reducing, though not eliminating, the availability of this service both domestically and internationally. Because it would eventually achieve the same end with less confrontation, the adoption of volume sensitive pricing for private, leased lines may emerge as a compromise in place of increased restrictions on availability.

A related and equally important dispute concerns access. The

---

American Tel. & Tel. Co. v. FCC, 572 F.2d 17 (2d Cir.), *cert. denied,* 439 U.S. 875 (1978). The FCC defines sharing as

> a non-profit arrangement in which several users . . . collectively use communications services and facilities obtained from an underlying carrier or a resale carrier, with each user paying the communications-related costs associated with subscription to and collective use of the communications services and facilities according to its pro rata usage of such communications services and facilities.

*Id.* at 274. The FCC will apparently apply these two definitions to the international as well as the domestic context. Regulatory Policies Concerning Resale & Shared Use of Common Carrier Int'l Communications Servs., 77 F.C.C.2d at 840 n.18.

87. Comments of Western Union Int'l, Inc., F.C.C. Docket No. 80-176, app. C (filed Aug. 15, 1980).

88. *Id.* at 18-21.

89. *See* Regulatory Policies Concerning Resale & Shared Use of Common Carrier Int'l Communications Servs., 77 F.C.C.2d 831, 834-39 (1980); Separate Statement of Charles D. Ferris, Chairman of the FCC, *id.* at 843-44. For FCC actions regarding the removal of domestic tariffs restricting resale and shared use, see Regulatory Policies Concerning Resale & Shared Use of Common Carrier Domestic Public Switched Network Servs., 77 F.C.C.2d 274 (1980); Regulatory Policies Concerning Resale & Shared Use of Common Carrier Servs. & Facilities, 60 F.C.C.2d 261 (1976), *amended on recon.,* 62 F.C.C.2d 588 (1977), *aff'd sub nom.* American Tel. & Tel. Co. v. FCC, 572 F.2d 17 (2d Cir.), *cert. denied,* 439 U.S. 875 (1978).

West German *Bundespost*[90] has recently issued new regulations,[91] effective January 1, 1982,[92] that will significantly restrict the extent to which private leased lines may have access to international lines. These regulations will present the private user with a choice between, on the one hand, placing computers in West Germany to perform significant processing locally before international transmission and, on the other hand, connection to the new volume sensitive services offered by the West German PTT.[93] "Both alternatives are expensive and should create havoc for remote computing service companies that have spent a fortune establishing efficient data transmission methods and large centers . . . [with] huge volumes of processing 24 hours a day for customers in different time zones around the world."[94] there are indications that other foreign countries intend to follow the West German policy.[95]

Protocol and standards present yet another area for concern. Without compatible protocols and standards, international communication as well as the introduction and marketing of new computer- and communications-based products and services such as home information systems become impossible. The CCITT is the appropriate forum for standards determination and will doubtless provide the arena for major debates on international teletext, videotext,[96] and home information systems.

The United States and Western European standards may vary for different services, which is a crucial factor in the international market potential for the United States viewdata industry. Television standards are an example of this variance. The Western European

90. The *Bundespost* is the PTT of West Germany.

91. Telegram from American Embassy, Bonn, West Germany, to U.S. Secretary of State (Apr. 15, 1980) (on file at *Cornell International Law Journal*).

92. *Id.*

93. *See* Markoski, *Telecommunications Regulations as Barriers to the Transborder Flow of Information,* 14 CORNELL INT'L L.J. 287, 317-19 (1981).

94. DATAMATION, Oct. 1979, at 78.

95. *Id.* Two United States data-processing service organizations, the Control Data Corporation and Tymshare, Inc., have experienced restrictions in Japan similar to those in the West German regulations. *See International Data Flow: Hearings Before the Subcomm. on Government Information and Individual Rights of the House Comm. on Government Operations,* 96th Cong., 2d Sess. 34, 47-52, 61, 62-64, 73-76 (1980) (statements of Philip C. Onstad & Warren E. Burton).

96. The nomenclature for these new and innovative systems is often confused and contradictory. In most fora, videotex is the generic term for cable or broadcasting systems that transmit information from data banks for display on television screens in the home or the office. *See, e.g.,* Clyne Committee report, *supra* note 77, at 61. Within the general category, teletext is a broadcasting system to which an integrated circuit decoder can provide access. For examples of the new services these systems permit, see N.Y. Times, May 4, 1981, at D4, col. 1. These new systems have also spurred a debate over the limits to which their use should be subject. *E.g., Yellow Pages and a Fearful Press, id.* at A22, col. 1.

systems employ a standard with more scanning lines than the United States usage. This discrepancy could make compatibility extremely difficult in a future environment of international videotex. The CCITT has taken up the work of determining international standards, and the United States has been represented, albeit with minimal governmental and popular support. The importance of the United States representation stems from the inevitable interrelationships between videotex and computer manufacturers and software providers. The global development of home information systems using standards incompatible with the United States standards would undoubtedly affect the United States data industry.

## III

## INFORMATICS PLANS

The transborder data flow restrictions and the arbitrary telecommunications tariffs and regulations of the last few years appear stopgap and short term when viewed against the more visionary development of national informatics plans. Broadly stated, informatics plans harness the essential elements of information resources in much the same way a nation might approach its coal or oil. In the name of national interest, informatics plans or strategies generally encourage the development and robust use of computer and telecommunications technology. With their nationalism and inward focus, however, the present informatics plans neglect an elemental factor in the teleinformatics environment: increasing global interdependence, which in turn, necessitates more harmony and coordination in the regulation of information and an expanded exchange of information. Of particular interest to the United States, France's Nora-Minc report[97] raises the issue of potential corporate (primarily IBM) dominance in national affairs and the need to check this development.[98] More recently, the French economist Madec also stressed the need diligently to diminish the threat of corporate influence in the area of teleinformatics in order to maintain national control over national affairs.[99]

The Nora-Minc report has provided the French Government with a solid framework within which to develop its *télématique* plan. These are some of the report's recommendations: cooperation between the PTT and other high technology agencies;[100] concentration on component technology to the same extent as that accorded

97. Nora-Minc report, note 12 *supra*.
98. *Id.* at 62-72.
99. Madec paper, *supra* note 11, at 37.
100. Nora-Minc report, *supra* note 12, at 12-16.

nuclear technology, with a recognition of its essential role in maintaining national independence;[101] the enlargement of the European supply of basic data in order to diminish dependence upon United States data banks;[102] and the construction of a more suitable and flexible model for the economic analysis of teleinformatics.[103] The implications of this last recommendation merit special attention from the United States and its teleinformatics industries. Alain Madec has set the stage for the development of such a system—a scheme for quantifying, classifying, and logically taxing certain kinds of data flows.[104]

Madec recommends an interrelated classification scheme[105] comprising four parts: a legal classification distinguishing between public and confidential data; a commercial classification distinguishing saleable information from that which is not, thereby permitting better regulation of property rights; a functional classification clarifying the information carriers' diversified roles as a distributor, a conduit for two-way communication, or a central nervous system; and an economic classification defining information in terms of its contribution to the process of creating a final product.[106]

For the United States and others concerned with the right to trade freely, new economic approaches raise a compelling question: To what extent can information be detached from its surrounding circumstances, whether from an author, a place, or an entity whose

---

101. *Id.* at 62-70.

102. *Id.* at 28.

103. *Id.* at 111-25.

104. According to Madec, just as international trade in goods is not analyzed by examining solely the packaging or the means of transportation used, neither should economists limit their analyses of trade in information to the signal or the nature of the transmitting medium employed. Madec paper, *supra* note 11, at 39. He recommends, instead, that economists examine the content of data flows and that economic classifications of data flows take into account the underlying reason for a particular data flow, its usefulness, and its value. *Id.* Madec notes that it is increasingly difficult to detect the content of a data flow during its transmission. *Id.* Thus, he argues that the determination of the usefulness of data will require an examination of the data at the terminal ends of the communication circuit:

> [I]t is impossible to study data flows without investigating the "stocks" at either end. Extending our map of data flows to include the geography of stocks is all the more necessary in that data stocks are at the very origin of new information, which is rarely acquired directly from the environment, but usually results from the further processing of existing information. Thus, the stock is closely associated with the value added by the computer.

*Id.*

105. *Id.* at 39-42.

106. Madec's economic classification established three types of flows: (1) transmissions of straightforward information, *e.g.*, messages, books, and television programs, are final consumption flows; (2) transmissions of data requiring further refinement are flows of intermediate or semifinished goods; and (3) exchanges of organizational systems, *e.g.*, computer software, are flows of capital goods. *Id.* at 40.

interests are implicated.[107] Already, many countries advocate for a right to exercise control over any and all information gathered within national borders.[108] The trends shows no signs of diminishing, and these countries are likely to persist as sovereignty and information issues become more closely linked.[109]

The Clyne Committee report[110] is Canada's answer to the Nora-Minc report. The Canadian report stresses the threat to national sovereignty posed by potential national dependence on foreign nations with advanced telecommunications technology.[111] When privacy concerns still dominated the discussion of international communications policies and problems, Hugh Falkner, then Canadian Minister of Science and Technology, anticipated the present debates by arguing that the chief problems with transborder data flow lay elsewhere:

> the potential of growing dependence rather than interdependence, the loss of employment opportunities, in addition to the balance of payments problems, the danger of loss of legitimate access to vital information and the danger that industrial and social development will be largely governed by the decisions of interest groups residing in another country.[112]

The Clyne Committee report addresses each of Falkner's fears. The report details a slate of recommendations[113] across a broad spec-

---

107. *Id.* at 42.

108. *See* note 22 *supra*.

109. *See* notes 166-83 *infra* and accompanying text.

110. Clyne Committee report, note 77 *supra*.

111. *Id.* at 1-5, 30-31, 37, 41-42, 52, 54, 57, 60, 63-65, 75-76, 79, 84. The Clyne Committee report adopted the following definition of sovereignty: " 'the ability of Canadians . . . to exercise control over the direction of economic, social, cultural, and political change.' " *Id.* at 1. This broad definition causes Canadian informatics strategies to overlap with other distinguishable concerns, *e.g.*, computer vulnerability. *See id.* at 60. *See generally* notes 119-54 *infra* and accompanying text. Thus, in Canada, it is difficult to discern where sovereignty ends and informatics begins. The Clyne Committee report, however, makes the direct link: "*[I]nformatics* is a word that is coming into general international use to describe computer-communications of all kinds. Of all the technologies that are developing so rapidly today, that of informatics poses possibly the most dangerous threat to Canadian sovereignty. . . ." *Id.* at 57 (emphasis in original). Nonetheless, the report's discussion makes it clear that the Clyne Committee was equally concerned with the straightforwardly economic implications of computer and communications technology:

> [T]he rich countries in the world today are those that exploited the industrial revolution in the 19th century; the rich countries of the future will be those that exploit the information revolution to their own best advantage in the 20th and 21st centuries. The industrial revolution was exploited in Canada at first by foreign interests, a fact that has produced our "branch-plant economy"; there is an opportunity today, which will not last long, for Canada to exploit the informatics revolution to its own best advantage, and we believe that policies and actions must begin at once to ensure that the facilities for and content of informatics in Canada not be allowed to develop on a "branch-plant" basis.

*Id.* at 58.

112. *Quoted in* COMPUTING EUROPE, Feb. 2, 1978, at 26.

113. Clyne Committee report, *supra* note 77, at 77-86.

trum of economic and social activities. The report recommends that the Government require data-processing activities related to Canadian business operations to take place in Canada.[114] Local data processing will, it is hoped, preserve both employment opportunities and control over Canadian information.[115]

The EC, as noted, has from the outset been primarily concerned with the development of a strong data-processing industry. The EC Commission has launched a program to capture one third of the world teleinformatics market by 1990,[116] and this, too, properly falls into the category of an informatics plan. The EC strategy includes provisions for the following: (1) the standardization of components used in computing; (2) the removal of nontariff trade barriers between EC member countries; (3) allowing all companies in the EC to compete for each member state's governmental contracts; (4) more money for the research and development of computer and chip technology as well as better coordination of national research programs; (5) the establishment of an integrated digital network for telecommunications so that video systems, computers, and more conventional telecommunications can be linked by the same network throughout the EC; (6) the reduction of tariffs on components not manufactured in the EC and a possible increase in tariffs on components that are; and (7) studies to set up a teleinformatic network for the EC institutions.[117]

In a global economy in which exports are critical to national economic survival, these direct initiatives for the capture of the global teleinformatics market bode ill for any nation's less aggressive enterprises. And the EC is not alone. Japan's commercial strategy is infamous, and France recently announced its goal of exporting fully thirty percent of French-manufactured telecommunications equipment by 1982.[118]

---

114. Recommendation 24(b), *id.* at 65, 84. The Clyne Committee also recommended that the Government stimulate the creation of Canadian-owned data banks, support education for programmers and systems analysts, and generally promote the development of Canada's electronics-manufacturing industry. Recommendations 23, 24(e), 25, *id.* at 63, 65, 73, 84-86. For a description of Canada's success in these endeavors, see N.Y. Times, May 11, 1981, at D1, col. 4.

115. Clyne Committee report, *supra* note 77, at 62-64.

116. *E.g.,* Commission of the European Communities, European Society Faced With the Challenge of New Information Technologies: A Community Response, Doc. COM (79) 650 final at foreword 1 (1979).

117. ECONOMIST, Oct. 13, 1979, at 52. *See* Ramsey, *Europe Responds to the Challenge of the New Information Technologies: A Teleinformatics Strategy for the 1980's,* 14 CORNELL INT'L L.J. 237 (1981).

118. *See* note 13 *supra*. The United States market is France's primary target. *Id. See generally* Stratte-McClure, note 12 *supra*.

Data protection laws and informatics plans are not necessarily contrary to international harmony. There is, however, a troubling intellectual enchantment with the concept of a postindustrial, information-based economy and society. This preoccupation may lead to the adoption of unnecessarily restrictive, even counterproductive information laws, taxes, tariffs, regulations, and policies. Once adopted, these measures will be difficult to remove or amend and will ultimately serve to inhibit the more orderly development of the international communications law and policy so badly needed.

## IV

## COMPUTER VULNERABILITY

The concern over national computer vulnerability mirrors the concern over the need for greater privacy protection for the individual. National governments, like individuals, depend increasingly upon computers and telecommunications to store and process information relating to national agriculture, commerce, vital services, and most notably, national defense. Moreover, multinational banks and others routinely transfer around the globe large volumes of data essential for governmental use.[119] The negative impact a country would sustain in the event of a temporary or sustained denial of access to such data reveals the extent of its computer vulnerability.

In the United States, the Department of Defense, other agencies concerned with national security, and numerous defense- and intelligence-oriented think tanks have examined the vulnerability of United States information systems, but there has been little public discussion. Elsewhere in the world, only Sweden has published any substantive work. In 1977, the Swedish Ministry of Defense formed a committee, the *Sårbarhetskommitté* (SÅRK), to investigate the computer vulnerability of the Swedish society and to propose measures to reduce this weakness.[120]

One particular event did much to prompt the Swedish study. In an experimental data communications project, information on the fire hazards of buildings in Malmö, Sweden, including descriptions of their physical plants, locations, and the nearest fire hydrants, was recorded in a computer and communicated to the Malmö fire depart-

119. *See, e.g.,* note 121 *infra* and accompanying text.

120. SÅRBARHETSKOMMITTÉN, FÖRSVARPDEPARTEMENTE, ADB OCH SAMHÄLLETS SÅRBARHET 1 (1978) [hereinafter cited as SÅRK report] (on file at *Cornell International Law Journal*). For a summary in English of the SÅRK report and a description of the SÅRK's subsequent activities, see COMMITTEE ON THE VULNERABILITY OF COMPUTER SYSTEMS, SWEDISH MINISTRY OF DEFENSE, THE VULNERABILITY OF THE COMPUTERIZED SOCIETY (1980) [hereinafter cited as Summary report] (on file at *Cornell International Law Journal*).

ment at the sound of an alarm.[121] The information was stored in a General Electric computer in Cleveland, Ohio, which led Swedish politicians and others to speculate about the consequences that would have ensued, if access to the data base had been impeded.

Despite its sponsorship, the SÅRK report does not confine its findings to matters concerning military security. Instead, the report also categorizes and assesses the risks and pressures implicit in the general use of computers. Although many of the SÅRK's perceptions are novel, the data protection acts of other nations (primarily Western European) reflect similar assessments.[122]

The report divides vulnerability factors into two main categories, internal and external factors. Internal factors[123] are those inherent in the use of computers and include the concentration of computer operations and dependence on assistance from abroad, *e.g.,* for spare parts. External factors[124] include war, both political and economic, terrorism, and crimes against property—which the SÅRK suggests may gain an entirely new dimension in an environment where payment transactions are highly computerized.[125] The report assumes that politically motivated acts of terrorism will continue to increase and that terrorism will become an important consideration in national planning.[126] The report also argues that Sweden's dependence on international data transmission circuits makes Sweden vulnerable to the political instability of each country through which these circuits pass.[127]

The SÅRK report uses worst case analyses, including military attack;[128] the enemy capture of citizen information registers;[129] the destruction or damage of computers and communications systems by the electromagnetic pulse effect of nuclear explosions;[130] and natural catastrophes affecting domestic and foreign data bases on which the country depends.[131] The study considers, among others, registers containing information on banking,[132] inventory,[133] and production processes.[134] In Sweden, government functions as a great storehouse

121. SÅRK report, *supra* note 120, at 246-47.
122. Summary report, *supra* note 120, at 14.
123. SÅRK, report, *supra* note 120, at 12-17, 163-249.
124. *Id.* at 7-17, 120-62.
125. *Id.* at 8.
126. *Id.* at 7-8, 32-33, 125-29.
127. *Id.* at 8-9, 133-42.
128. *Id.* at 143-56.
129. *Id.* at 163-71.
130. *Id.* at 19, 154-56, 257.
131. *Id.* at 157-62.
132. *Id.* at 86-90.
133. *Id.* at 84-86.
134. *Id.* at 80-83.

of personal and commercial information, including information of a confidential and strategic nature such as descriptions of the internal operations of private enterprises and population registers that list places of residence. The SÅRK report contends that all this information could be used to exert undesirable pressure were it to fall into the wrong hands.[135] It comes as no surprise, then, that the SÅRK recommends that Sweden include the Data Inspection Board among the authorities with responsibility for the vulnerability question.[136] The Committee would award to the Board the primary responsibility for licensing, supervising, and examining all data bases.[137]

Other aspects of vulnerability include the functional concentration of some computer systems[138] and the awesome synthesizing capabilities of data-processing technology.[139] Both characteristics would greatly facilitate the assimilation for harmful purposes of disparate and otherwise banal information. The SÅRK report cites even dependence on a small group of key data-processing personnel as an instance of vulnerability.[140] The Committee notes that such a group might become an enemy target[141] and that a work stoppage by it alone could lend powerful leverage in a much larger labor dispute.[142]

The multifariousness and the severity of the national computer vulnerability described by the Committee add force to its call for effective emergency preparedness.[143] The Committee links computer vulnerability to informatics and economics when it implicitly recommends the development of a national computer industry to reduce the vulnerability created by dependence on assistance from abroad.[144] The increased use of better encryption methods is one of the more important recommendations, to be implemented first at the data link, but eventually at the data register itself.[145]

Because it may be of influence outside Sweden,[146] the SÅRK's

135. *Id.* at 163-87.
136. Summary report, *supra* note 120, at 19.
137. *Id.*
138. SÅRK report, *supra* note 120, at 14, 188-93.
139. *Id.* at 15, 203-06.
140. *Id.* at 16-17, 219-26.
141. *Id.* at 17, 223-24.
142. *Id.* at 17, 224-25.
143. *Id.* at 19-20, 231-35, 256-58.
144. Summary report, *supra* note 120, at 13. *See also* SÅRK report, *supra* note 120, at 18, 236-49, 252.
145. Summary report, *supra* note 123, at 13. *See also* SÅRK report, *supra* note 120, at 117.
146. *See, e.g.,* Clyne Committee report, *supra* note 77, at 60.
Computer vulnerability is clearly not a problem peculiar to countries dependent on foreign data bases and other assistance from abroad. Terrorist sabotage, for instance,

recommendation of pervasive licensing[147] should cause some concern in the United States private sector. The proposed licensing scheme would require the disclosure of register content, system structure, security measures, dependence on staff, mechanical and manual standby routines, emergency planning, integration with and dependence on other data-processing systems, and the geographical location and so-called suitability of data-processing operations abroad.[148] Both register content[149] and data-processing operations abroad[150] would be subject to restriction. Such restrictions would apply to both personal and other data, but would not apply uniformly to the public and private sectors.[151] A governmental agency would be responsible for disposing of the information disclosed.[152] The SÅRK has already drafted enabling legislation, entitled the Vulnerability Act, that speaks to the proposed licensing procedure.[153] The Committee recommends the postponement of any action on the Vulnerability Act or similar measures until the Government and the Parliament have defined their positions vis-à-vis the Committee's proposals.[154]

In the United States, computer vulnerability and related subjects have traditionally been considered matters of national security. Consequently, they have remained nearly exclusively within the domain of the military and intelligence communities, primarily the National Security Agency. There is a growing need, however, to include members of the commercial sector and the public as participants in the discussion of computer and communications security. Often the requirements of business, whether legal or economic, conflict with the responsibility of the state to protect its secrets, which now include information about the nation's agricultural and intellec-

threatens the computer systems of the United States as much as it threatens those of Sweden. *See* SÅRK report, *supra* note 120, at 125-29. In a rare discussion of this sensitive topic, the then Director of the U.S. National Security Agency stated that "[t]here is a growing recognition of the potential vulnerability of our communications system within the United States to exploitation, both by foreign powers and by domestic law-breakers." Address by B.R. Inman, Vital Telecommunications Issues Symposium, U.S. Dep't. of State (Jan. 1979), *printed in* SIGNAL, Mar. 1979, at 6, 8 [hereinafter cited as Inman Address].

147. Summary report, *supra* note 120, at 16-18. *See also* SÅRK report, *supra* note 120, at 261-64, app. I.

148. Summary report, *supra* note 120, at 16.

149. *Id. See also* SÅRK report, *supra* note 120, at 255-56.

150. Summary report, *supra* note 120, at 16. *See also* SÅRK report, *supra* note 120, at 252, 262.

151. Summary report, *supra* note 120, at 17.

152. *See* notes 136-37 *supra* and accompanying text.

153. Summary report, *supra* note 120, at 16.

154. *Id.*

tual resources as well as more conventional secrets.[155] At present, the conflict centers on the technical standard for encryption.[156]

The United States National Bureau of Standards has developed the so-called Data Encryption Standard to serve as the standard for protection by encryption of information in computers purchased or used by the Federal Government.[157] The Data Encryption Standard is also available to businesses for their confidential data.[158] Increasingly, private entities, particularly banks and insurance companies, must protect transmitted data by using encryption. Research supporting the cryptographic needs of both the private and the public sectors have been prolific, and grants from the National Science Foundation have supplied part of the necessary financing. Although the National Security Agency denied, in 1979, any involvement,[159] there is growing recognition that the Agency is restricting these grants[160] and, furthermore, that the Agency may seek to wrest from the National Science Foundation the authority to award them.[161] The Agency apparently fears that increased private, academic (and therefore published) cryptographic research will contribute to the development abroad of sophisticated cryptographic technology. Furthermore, this sophistication might render United States security techniques more vulnerable, a possibility that led the Director of the Agency to declare that "unrestrained nongovernmental cryptologic activity poses a threat to national security."[162]

The defense and business communities are also divided over the role national security has to play regarding trade and the transfer of technology, particularly as these concern the Communist countries. The United States Government often restricts these transfers severely on the ground that they would pose a threat to national security by aiding the military operations of a hostile power.[163] Others maintain, however, that foreign suppliers step into the breach

155. Walter B. Wriston, Chairman of the Board of Directors of Citibank, cites encryption as an example. He notes that some governments encourage the use of encryption by private communicators to protect privacy, while other governments, for reasons of national security, prohibit this use. In addition, he notes that emerging regulations for the security of nonpersonal data bases may imperil the private use of encryption, because regulators will have to know the content of the files they seek to protect. Letter of Walter B. Wriston, note 55 *supra*.

156. *See* N.Y. Times, June 1, 1981, at A14, col. 1.

157. Inman Address, *supra* note 146, at 8-9. *See also* U.S. NEWS & WORLD REPORT, June 26, 1978, at 45, 48.

158. U.S. NEWS & WORLD REPORT, *supra* note 157, at 48.

159. Inman Address, *supra* note 146, at 9.

160. Wash. Post, Aug. 28, 1980, at A9, col. 1. *See* 208 SCIENCE 1442 (1980).

161. 210 SCIENCE 511 (1980).

162. Inman Address, *supra* note 146, at 13.

163. Norris, *High Technology Trade With the Communists,* DATAMATION, Jan. 1978, at 99. *See, e.g.,* Electronic News, Oct. 8, 1979, at 6, col. 1.

created by governmental prohibitions of the transfer of technology from United States corporations.[164] The upshot, they argue, is merely lost jobs in the United States.[165] We need to fashion a more refined formula for balancing political and economic security across a broader spectrum of vulnerability concerns.

## V

## NATIONAL SOVEREIGNTY AND INFORMATION

Sovereignty in its fullest sense is the "supreme, absolute, and uncontrollable power by which any independent state is governed . . . ."[166] Many nations, or at least their prominent national leaders, increasingly invoke the term sovereignty when discussing information issues.[167] They fear that sophisticated computer and telecommunications technology may bring about a general loss of national independence or autonomy.[168]

Sweden, as noted, has examined the ways in which information technology has undermined its national security.[169] Canada has adopted a very broad definition of sovereignty: " 'the ability of Canadians [both in government and in the private sector] to exercise control over the . . . direction of economic, social, cultural, and political change.' "[170] By using this expansive definition, the Clyne Committee was able to employ the concept of sovereignty to justi fy even recommendations concerning foreign programming on Canadian television.[171] Potentially more significant, some developing countries argue that so-called electronic colonialism or electronic imperialism compromise their cultural and political integrity. These stirring phrases also express perceived threats to national sovereignty.

The international resolution of information issues, especially in the area of earth-sensing technology, may eventually expand the accepted legal meaning of sovereignty. Charges of electronic colonialism may sound extreme, but they are often accompanied by the

164. *E.g.,* Electronic News, Oct. 8, 1979, at 6, col. 1.

165. *E.g.,* Norris, note 166 *supra*.

166. BLACK'S LAW DICTIONARY 1252 (5th ed. 1979). Professor Starke suggests that this definition of sovereignty is anachronistic: "[I]t is probably more accurate today to say that the sovereignty of a State means the *residuum* of power which it possesses within the confines laid down by international law." J. STARKE, AN INTRODUCTION TO INTERNATIONAL LAW 113 (8th ed. 1977).

167. *See, e.g.,* Clyne Committee report, *supra* note 77, at 1-9, 30-31, 41-42, 63-65, 75-76, 79; Address of F.A. Bernasconi, *supra* note 21, *printed in* 3 TRANSNAT'L DATA REP. No. 3/4, at 4.

168. *See, e.g.,* note 11 *supra* and accompanying text.

169. *See* notes 120-54 *supra* and accompanying text.

170. Clyne Committee report, *supra* note 77, at 1.

171. *Id.* at 37-46, 80-82.

more reasonable assertion that the primary finders and developers of the world's nonrenewable resources enjoy enviable advantages in the mounting struggle to acquire dwindling resources.[172] According to the Clyne Committee's analysis, in which the developing countries increasingly concur, there will be two classes of people and nations in the information age: the exploiters and the exploited.[173] The developing countries are anxious lest the slower pace of their development ultimately preclude them from ever establishing high technology industries and services of their own. They fear both the exhaustion of vital, limited resources, including the communications spectra,[174] and the practical impossibility of new market entry by the time they are capable of pursuing high technology.[175]

Earth-sensing technology is an important tool in finding the world's resources. Some argue that the users of this technology achieve unfair advantages by "wresting information about areas from those who have a first claim on such knowledge—the inhabitants of the area."[176] Consequently, some countries have begun to suggest that information itself is a natural resource over which nations may exercise permanent sovereignty.[177] If this principle becomes established, it may develop that sensing nations will have to acquire the consent of sensed nations before earth sensing can be undertaken.[178] The United States has not recognized the validity of

172. H. Schiller, Planetary Resource Information Flows: A New Dimension of Hegemonic Power, or Global Social Utility? (unpublished paper presented at Conference on World Communications: Decisions for the Eighties, Annenberg School of Communications, University of Pennsylvania, May 12-14, 1980) (on file at *Cornell International Law Journal*).

173. Clyne Committee report, *supra* note 77, at 58.

174. *See generally* ACADEMY FOR EDUCATIONAL DEVELOPMENT, THE UNITED STATES AND THE DEBATE ON THE WORLD "INFORMATION ORDER" 36-42 (1978); PANEL ON INT'L TELECOMMUNICATIONS POLICY OF THE AMERICAN SOCIETY OF INT'L LAW, CARNEGIE ENDOWMENT FOR INT'L PEACE, THE INTERNATIONAL TELECOMMUNICATION UNION: ISSUES AND NEXT STEPS 6-13 (1971).

175. *See, e.g.,* Address by Joubert de Oliviera Brizida, *supra* note 8, *printed in* 3 TRANSNAT'L DATA REP. No. 3/4, at 32, 33-34 (1980).

176. H. Schiller, *supra* note 172, at 4.

177. *See, e.g.,* Treaty on Remote Sensing of Natural Resources by Means of Space Technology—Draft Basic Articles in Letter from the Permanent Representatives of Argentina and Brazil to the Secretary General (Oct. 15, 1974), *reprinted in* First Committee of the Committee on the Peaceful Uses of Outer Space, U.N. Doc. A/C.1/1047 (1974). The fifth preambulary paragraph of the draft treaty cites two United Nations General Assembly resolutions concerning sovereignty and natural resources: Permanent Sovereignty Over Natural Resources, G.A. Res. 2158 (XXI), 21 U.N. GAOR, Supp. (No. 16) 29, U.N. Doc. A/6316 (1966); and Permanent Sovereignty Over Natural Resources, G.A. Res. 1803 (XVII), 17 U.N. GAOR, Supp. (No. 17) 15, U.N. Doc. A/5217 (1962). First Committee of the Committee on the Peaceful Uses of Outer Space, *supra,* at 2.

178. Article V of the draft Treaty on Remote Sensing of Natural Resources by Means of Space Technology provides as follows: "States parties shall refrain from undertaking activities of remote sensing of natural resources belonging to another State party, including the resources located in maritime areas under national jurisdiction, without the con-

sovereignty claims of this type.[179] Some developing countries have taken a completely different approach. These nations insist that national sovereignty extends spacially to those parts of outer space where earth-sensing satellites orbit.[180] Again, if sovereignty is extended to cover these orbits, the legitimacy of prior consent restrictions would presumably follow.

In a more general sense, nations may employ the principles of sovereignty in order to justify the introduction of new, abrasive information laws and practices. The concept of sovereignty is universally respected; therefore, it is difficult to protest actions undertaken in its name, regardless of the suspected motive. Sovereignty may, for instance, provide a nation that seeks a period of neoisolationism with an internationally respected shibboleth for drawing an information curtain about itself.[181] Some have invoked national sovereignty in the effort to establish the so-called New World Information Order.[182] If nations succeed in requiring foreign journalists to submit news reports for an assessment of balance and so-called responsibility, their governments may gain a powerful tool for international propaganda.[183] Moreover, if prior consent requirements become established under this rationale, nations might easily extend them to cover the transborder transmission of all information, including commercial data.

If freedom of speech and freedom of the press are to remain unimpaired, there is a clear need to examine the character of the information subjected to prior consent restrictions. Prior consent regulations may severely inhibit these freedoms in nations that adopt these regulations. Moreover, they may weaken the effectiveness of these freedoms in nations that decline to enact prior consent legislation. Thus, ideational information should transit freely. Only information properly characterized as a commodity should be subject to trade negotiations, taxes, customs duties, and if necessary, prior consent regulations. Even if nations accept this basic distinction, technological advances may only exacerbate the problem. As communications technology drives toward the total digitalization of

---

sent of the latter." First Committee of the Committee on the Peaceful Uses of Outer Space, *supra* note 177, at 3.

179. H. Schiller, *supra* note 172, at 5.

180. *See, e.g.,* Legal Sub-Committee of the Committee on the Peaceful Uses of Outer Space, U.N. Doc. A/AC.105/C.2/SR.277, at 2-4 (1977).

181. *See generally* Wash. Post, Dec. 10, 1980, at A31, col. 3; *id.,* Aug. 24, 1980, at A1, col. 4.

182. *See, e.g.,* INT'L COMM'N FOR THE STUDY OF COMMUNICATION PROBLEMS, MANY VOICES ONE WORLD 143 (1980).

183. *See* N.Y. Times, May 18, 1981, at A1, col. 1.

communications, the discrimination of content in pictures, data, voice, graphics, and news will become increasingly difficult.

Of course, censorship has a long history. If, however, the international community accepts as legitimate the invocation of sovereignty in relation to information issues, the consequences may entail more than expanded censorship. The absolute nature of sovereignty may render information issues less amenable to resolution by international agreement and practice. Governments will have a new ground for scrutinizing the practices and agreements of private parties. Arbitrary governmental actions on information matters will not be proper subjects for protest by other governments.

Informatics plans in some respects resemble these assertions of sovereignty, but the motivation behind these plans is essentially economic. If an informatics plan sets as its goal the capture of the world market in the provision of telecommunications services, the plan necessarily contemplates greater international interdependence. The increased invocation of sovereignty in reference to information matters threatens reduced international interdependence.

## VI

## THE UNITED STATES INFORMATION POLICY

Transborder data flow restrictions pose perhaps the greatest threat to the United States, where the communications revolution is most advanced. Yet, because its private sector is diverse and its public sector ever more fragmented, the United States is poorly organized for dealing decisively with the rapidly unfolding problems of transborder data flow. A number of governmental agencies and offices, too many, share authority for international communications and information issues. After a comprehensive examination of the myriad of issues, the House Committee on Government Operations reached the same conclusion:[184]

> The governments of our major trading partners and of the developing world are adopting national policies and comprehensive plans to respond to problems brought about by advances in computer and telecommunications technologies. They view these problems in a spectrum ranging from advertising and television broadcasting, to the use of data processing for keeping records and accounts, to the growth of data communications. They see the international flow of information through telecommunications systems, particularly computer to computer communications, as a major cause for concern and a basis for governmental action. Out of this concern for the effects

184. The Report of the Committee on Government Operations is based on a study made by the Subcommittee on Government Information and Individual Rights. Letter from Jack Brooks to Thomas P. O'Neill, Jr. (Dec. 11, 1980), *reprinted in* 1980 House Report, *supra* note 6, at III.

> of the changing character of the international flow of information, several nations have taken actions creating barriers to that flow.
>
> In the face of these developments, the U.S. Government is unprepared. It has developed neither comprehensive plans or policies nor a coherent strategy for responding to the policies of other nations which may damage U.S. interests. The U.S. Government does not have even the organizational structure to develop such policies, coordinate its actions, and effectively protect U.S. interests.[185]

The House Committee recommended the creation of a Cabinet level Council on International Communications and Information.[186] The proposed Council would be composed of an independent director, the Secretaries of State and Commerce, the Chairman of the Federal Communications Commission, the United States Trade Representative, the Director of the Office of Management and Budget, and the Assistant to the President for National Security Affairs.[187] The proposed Council's principal responsibility would be "to coordinate development and implementation of a uniform, consistent, and comprehensive United States policy in response to the problems raised by barriers to international communications and information flow."[188]

The proposed Council would serve as a coordinator within the Government and between the Government and the private sector:

> The Council should serve as the office to which private sector problems and concerns can be brought and from which responsibility may be delegated to appropriate agencies.
>
> . . . An advisory committee, patterned after the advisory committees for trade negotiations and composed of representatives of the private sector—including manufacturers, providers, and users of international communications and information products and services—should be established to provide policy guidance to the Council.
>
> . . . An inter-agency committee should be established to advise the Council with respect to problems of international communications and information transfer which Federal agencies encounter in the performance of their duties.[189]

Because information issues so pervade the United States' economy and society, the House Committee decided that no single governmental agency could serve as the sole source of wisdom in providing solutions. Accordingly, the Committee would grant the proposed Council a limited life during which it would act as a catalyst and provide an initial policy overview.[190] The real work of solving teleinformatics problems would be left for the various

185. 1980 House Report, *supra* note 6, at 1-2.
186. *Id.* at 10, 56.
187. *Id.* at 10-11, 56.
188. *Id.* at 56.
189. *Id.* at 11, 56.
190. *Id.* at 10, 56.

departments and agencies with primary authority. Whether the House Committee's organizational concept is widely embraced or not, the need for a national communications and information policy is finally gaining recognition.

## CONCLUSION

Taken together, these challenges to the United States assume immense proportions. Moreover, the solutions do not rest with the United States alone. We should consider refurbishing and perhaps restructuring the fora of world government to accommodate the pressures developing over information as a resource. Any change will undoubtedly require considerable humility on the part of the United States or any other major player. We at least need to seek international agreement on subjects ranging from the compatibility of equipment to the confidentiality and security of communicated information. International regulation is inevitable. The only question is whether this regulation is good or bad, well planned or cumbersome in its conception.

This dimension of our foreign relations offers a challenge to our idealism and our ingenuity, our sense of mission and our common sense. It is the challenge of the last quarter of this century.