UIC John Marshall Journal of Information Technology & Privacy Law

Volume 3
Issue 1 *Computer/Law Journal - 1981*

Article 4

1981

Transborder Data Flow Regulation: Technical Issues of Legal Concern, 3 Computer L.J. 105 (1981)

Eric J. Novotny

TRANSBORDER DATA FLOW REGULATION: TECHNICAL ISSUES OF LEGAL CONCERN*

by ERIC J. NOVOTNY†

Thousands of private organizations and millions of individuals depend on rapid and reliable international data communication for a wide variety of services—airline reservations, foreign exchange and funds transfers, management information, and scientific research. Similarly, governments use high speed data links by satellite and cable for military, diplomatic, and technical communications. These types of international computer communications are known collectively as transborder data flows.[1]

The passage of fair information practices laws in Europe and in North America, the tremendous advances in computer and telecommunications technology, and the expansion of information intensive international commerce together have increased our attention to data flow issues. In the late 1970s, this concern surfaced in the deliberations of international organizations such as the Organization for Economic Co-operation and Development (OECD) and the Council of Europe. Although progress has been made in cooperative

* Research leading to the publication of this paper was supported by National Science Foundation Grant MCS-77-24235 to the George Washington University. The author wishes to thank Dr. Lance J. Hoffman for proposing and supporting this inquiry. Points of view or opinions in this article are those of the author and do not necessarily represent the official position or policies of the National Science Foundation or any other institution. A previous version of this paper was published as Report No. GWU-EECS-80-10 of the George Washington University Research Report Series, November 1980.

† Ph.D. candidate, Department of Government, Georgetown University, Washington, D.C. Manager, Policy Analysis Department, International Communications Services, Communications Satellite Corporation.

1. *See generally* 1 AMERICAN FED'N OF INFORMATION PROCESSING SOC'YS, TRANSBORDER DATA FLOWS: CONCERNS IN PRIVACY PROTECTION AND FREE FLOW OF INFORMATION (R. Turn ed. 1979) [hereinafter cited as AFIPS REPORT]; Novotny, *Transborder Data Flows and International Law: A Policy-Oriented Framework of Inquiry*, 16 STAN. J. INT'L L. 141 (1980).

fair information practices, other major issues as yet have eluded international conciliation.

Political and legal controversies surround the use and content of transborder data flows, despite the steady growth, acceptance, and recognized value of international computer data networks. Within this context, only slight attention has been given to the technical issues and problems of transborder data flow regulation.[2] Policymakers need to examine more fully the technical problems of transborder data flow regulation and to investigate the technical opportunities, constraints, and effects of restrictions on the international transmission of digital information.

I. A STATEMENT OF THE PROBLEM

A. PROBLEMS OF DEFINITION

The literature on transborder data flows contains discussions of widely varying problems, partly due to the fact that data flows are defined and categorized differently (or not at all) by various authors. One must be able to separate data flows relating to international computing activities from other forms of international telecommunication, *e.g.*, voice telephony, TELEX, facsimile, and video. Many of these forms of telecommunication were regulated successfully by the international community for over one hundred years before the introduction of modern digital computers. What makes today's problems different?

To qualify as transborder data flows, the technical process must involve: (1) transmission, (2) storage, and (3) computation. Traditional telegraphy and voice telephony by themselves provide transmission, but provide neither storage nor computation.[3] Data storage provides economical access to large information files, and computation provides the necessary processing component to manipulate the data. Without substantive data files or data bases and a computational function, data flows take on characteristics similar to other forms of electronic communication. Telephone systems, for example, employ techniques that digitize voice transmissions. TELEX

2. AFIPS REPORT, *supra* note 1, at 117; *see also* Turn, *Privacy Protection and Security in Transnational Data Processing Systems*, 16 STAN. J. INT'L L. 67 (1980); Nelson & Reisman, *Consideration of Privacy and Encryption in Personal, National and Multinational Communications*, in PROC. PAC. TELECOM. CONF., 2H.20 (1980); Norman, *A Scheme for Regulating Transborder Data Flows*, in TRANSNATIONAL DATA REGULATION: THE REALITIES 12-1 (1979); Turn, *Privacy and Security in Transnational Data Processing Systems*, 48 AFIPS CONF. PROC., NAT'L COMPUTER CONF. 283 (1979).

3. V. COATES & B. FINN, A RETROSPECTIVE TECHNOLOGY ASSESSMENT: SUBMARINE TELEGRAPHY 186 (1979).

and facsimile systems also can employ digital channels. Yet handling all of these types of telecommunication the same way negates the recent importance ascribed to computer-related data flows and ignores the effect of the consequent national laws and international proposals for regulating them. For example, a personally identifiable dossier can be transmitted easily across a national border via a TELEX message. Such activities have taken place since the inception of such services, but the advent of computation and storage have changed the stakes greatly.

Laws affecting personally identifiable data did not appear until the development of technologies involving data processing, data storage, and transmission rates made it economical to transmit large amounts of data in a short period. Data processing and storage facilities, located in one country, are beyond another country's supervision and regulation.[4] The benefits of increasing data flows and the problems of eroding controls thus become divergent species. Content regulation over the border becomes one way of enforcing such control in the absence of territorial jurisdiction.

Transborder data flows are, therefore, digitally encoded units of information in which the transfer, storage, or processing takes place in more than one nation state. The information can be transported physically by magnetic media, *e.g.*, tapes, disks, or transmitted electronically over a terrestrial line, submarine cable, or satellite link. The most important fact is that the information transported or transmitted by these two modes either undergoes some type of data processing, or is accessed across an international frontier. Although a strict definition of data processing, as contrasted with data communication, has proved to be elusive,[5] Seitz proposes a mathematical definition.[6] He views data communication as a function in which entropy is preserved without significant alteration of its content or meaning. Data processing, on the other hand, changes the level of entropy by transforming or manipulating the data. This view is sim-

---

4. As Smith writes:

> When the source of the telecommunications is beyond the boundaries of the State, problems of control arise that have yet to find an adequate solution in terms of international law. It becomes necessary to distinguish between the right of a state to do what it pleases within its own territory, and the claim of that State to legally object to an activity originating beyond its borders but which has an internal effect.

INTERNATIONAL TELECOMMUNICATION CONTROL 2 (1969).

5. Amendment of Section 67.702 of the Commission's Rules and Regulations (Second Computer Inquiry), 72 F.C.C.2d 368 (1979); Computer Inquiry, 28 F.C.C.2d 267 (1971).

6. Seitz, *Data Communication and Data Processing—A Basis for Definition*, 5 TELECOM. POL'Y 49 (1980).

ilar to the IBM "encryption test" used to distinguish between data communications and data processing.[7]

At first glance, this distinction runs counter to prevailing notions that previously diverse types of telecommunication technologies are being merged into integrated services, and consequently made indistinguishable. There is little doubt that new, high-capacity facilities can attract voice, record, and data traffic integrated in the same channels and made largely inseparable.

One may reject the notion, however, that integrating transmission media will allow diverse forms of telecommunication to be treated the same. Governments have singled out computer-related data flows for separate treatment. This trend will not diminish as transmission media allow data communication to be integrated with other services. Rather, the combination of different services actually may lead to situations where data flows are identified and controlled more aggressively.

What is different about the transborder data flows problem, therefore, is that the information transmitted is *changed* at one or more nodes in an end-to-end communication path. That change, in the form of computation, occurs at some point before or after transmission from storage generates the data flows.

B. Four Generic Problems

Some of the technical problems in transborder data flow regulation are expressed, solved, or affected by both the technologies of data processing and of telecommunication. These problems include:

- Technical compliance with specific data protection or privacy laws
- Attaining and maintaining data security
- Monitoring and surveillance of data flows
- Impacts on computer network planning

Each of these problems will be considered from the perspective of the regulated and the regulating entity. The regulated entity may be a multi-national enterprise, telecommunication carrier, computing service bureau, or other organization that is the subject of data flow regulation. The regulating entity is always a national government.

Each of these perspectives, regulated and regulating, contain different and occasionally conflicting technical issues. One may afford technological opportunities, while another imposes constraints.

---

7. See *In re* Amendment of Section 64.702 of the Commission's Rules and Regulations (Computer Inquiry), 64 F.C.C.2d 771 (1979) ("[A] service would be tariffed only if the user could send encrypted information knowing that the information would emerge at the addressee's location in the same encrypted form.")

Decisions or legal policies may have technical implications for either the regulated or regulating entities. Technical problems also may have financial implications as their costs of implementation vary.

Compliance with specific privacy or fair information practices laws embraces several technical problems.[8] Regulated entities, such as multinational enterprises, have problems preventing unauthorized disclosure, accounting for third party disclosure, providing persons access to their own files, and complying with other familiar provisions of privacy legislation. These privacy concerns can affect system and data base design and, in an international context,[9] the requirement that an organization observe more than one law when engaging in transborder processing can cause further complications.

Some of these laws also contain security requirements that regulated entities must meet. Regulating entities often may conduct inspections or audits to see if compliance is observed. Sometimes, however, for reasons independent of legal compliance with data protection laws, organizations use cryptographic methods to protect information during transborder transmission. There are often technical problems in ensuring cryptographic protection when governmental restrictions inhibit the use of such technology by private organizations.

Monitoring and surveillance of transborder data flows is another generic problem for the regulating entity. Technical proposals have been advanced, for example, to identify data flows with some type of digital "license tag" to identify the source, content, value, and destination of such flows.[10] Some have argued that such surveillance is, in practice, unworkable.[11] Regulating entities, however, require some surveillance techniques to police compliance with national data flow policies.

Data flow restrictions also can have effects on the organizational planning of computer and telecommunication networks. Of course, overall planning takes place in the context of available and planned telecommunication facilities; regulated entities, however, in re-

8. *See generally*, PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, app. 5 (Technology and Privacy) (1977); COMPUTERS AND PRIVACY IN THE NEXT DECADE (L. Hoffman ed. 1980).

9. *See* Gassmann, *Privacy Implications of Transborder Data Flow*, in COMPUTERS AND PRIVACY IN THE NEXT DECADE, *supra* note 8, at 109; Safirstein, *How Do We Best Control the Flow of Electronic Information Across Sovereign Borders?*, 48 AFIPS CONF. PROC. NAT'L COMPUTER CONF. 279 (1979).

10. Norman, *supra* note 2, at 12-15.

11. I. POOL & R. SOLOMON, TRANSBORDER DATA FLOWS: REQUIREMENTS FOR INTERNATIONAL COOPERATION 48 (1978).

sponse to existing or anticipated restrictions on transborder data flows, may be forced to change their plans for international networks.

C. Scope and Limitations

Other technical problems associated with transborder data flows have not escaped notice. Among such allied topics are the problems of international copyright or patent protection for software,[12] of capacity planning, and of data transmission protocols and standards. The recurring problem of competing definitions of data processing and data communication has been mentioned previously. While these are important and interesting problems in the international use of information technology, they will not be discussed in detail. Rather, this Article will attempt to cover issues that relate more directly to the use and content of the data flows themselves, and that have not yet received extensive attention in the literature.

Another deliberate limitation of this Article is the omission of technical problems inherent to general computer security issues. There is abundant literature on security problems that have no appreciable differences in a local, national, or international context.[13] This Article concentrates on issues unique to international computing.

D. Types of Transborder Data Flow Movements

To better understand the technical aspects of transborder data flow problems, several types of data flow patterns that may influence a given regulatory situation will be discussed. These are shown in Figure 1. For the purpose of this discussion, these generic types of data transfers will represent portions of a given organization's network structure, segmented into categories that simplify actual, aggregate international flow traffic.[14]

Type 1 in Figure 1 describes a simple subsidiary reporting relationship. A subsidiary entity in country A transfers information one-way to a headquarters user in country B. The headquarters consolidates such data from a number of subsidiaries. One applica-

---

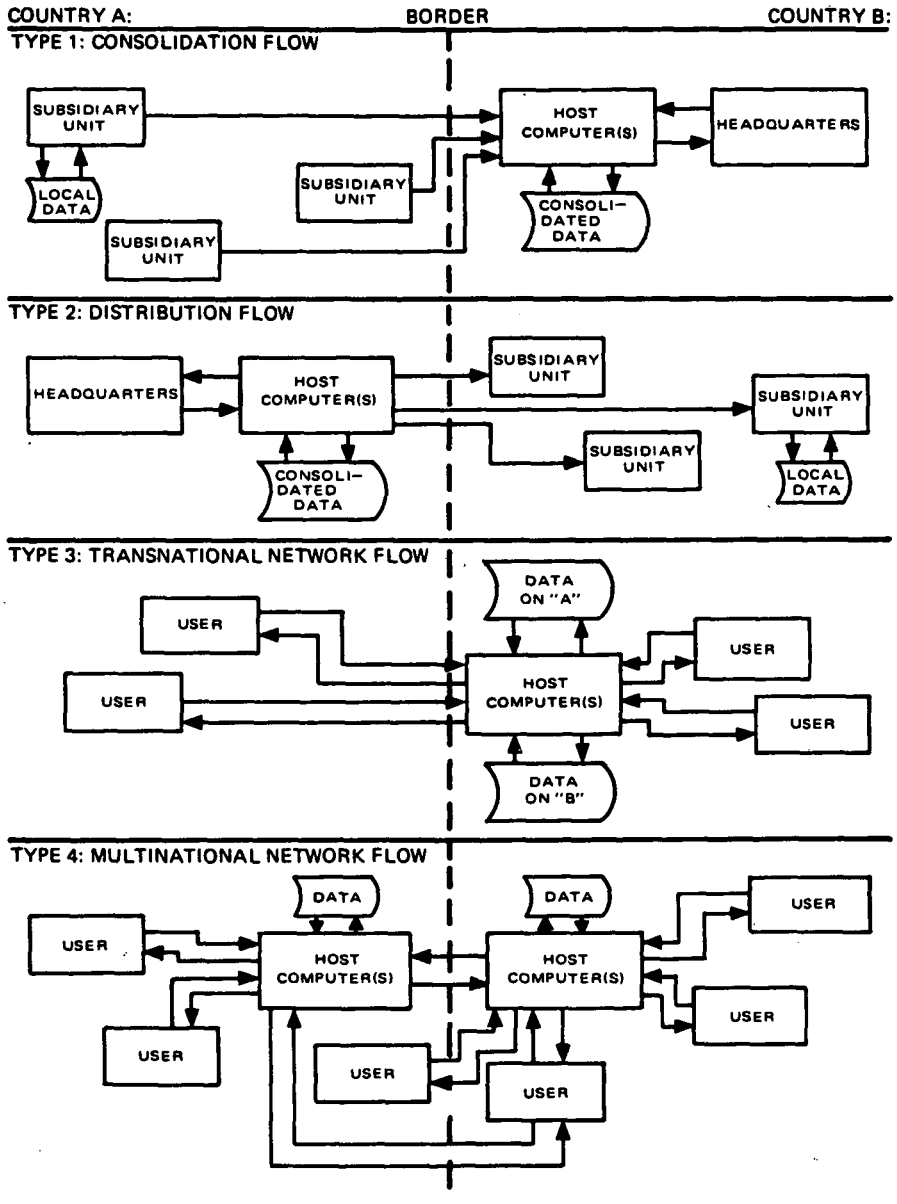
12. *Id.* at 56.

13. *See* Cerf & Kirstein, *Issues in Packet-Network Interconnection*, 66 IEEE Proc. 1386 (1978); L. Hoffman, Modern Methods for Computer Security and Privacy (1977); Nelson & Reisman, *supra* note 2; Popek & Kline, *Encryption and Secure Computer Networks*, 11 Computing Surveys 331 (1979).

14. Case studies of actual networks are available. *See* Organisation for Economic Co-operation and Development, The Usage of International Data Networks in Europe (1979) [hereinafter cited as OECD].

FIGURE 1

TRANSBORDER DATA FLOWS CAN BE GROUPED INTO FOUR TYPES



tion of this type of data flow would be operational reporting by a subsidiary business in country A to the main office in country B. Some credit transactions take a similar path. A citizen of country B who uses a credit card in country A will have a record of transaction transferred to country B for processing and billing.

Distribution flow, the second type of transborder data flows, occurs when a centralized entity distributes data to several subsidiary entities. These subsidiaries can also engage in their own local processing. Applications of this type of flow include updates to local files and data bases, orders and financial reports, and similar instructions or information transmitted to subordinate units. Consolidated data files typically are held in the headquarters country.

The third type of transborder data flows is common and involves transnational processing, such as a service bureau arrangement. Here, subscribers or users in one country use host computer facilities in another. Two-way traffic occurs since the main purpose of accessing the host is to use its computing facilities or data bases. There may be dedicated applications, of course, as in an interactive reservation system, but the pattern is essentially the same. Data needed by subscribers in one country may reside with a host in another. One other variation would include a mailbox system or a message-switching arrangement. A limited definition of data flows, however, may exclude some store-and-forward message switching due to the lack of a computational element.

A more complicated pattern, typified in practice by many unique variations, is the multinational data network exemplified by the fourth type diagrammed in Figure 1. Data flows are characterized by multiple-user, multiple-host interactions, where information and processing can be centralized, distributed, or both. Large service bureaus or time sharing networks can operate in this fashion, yet one should distinguish between a situation where the user or subscriber is dependent on computational or data base resources in another country, from that where the user has access to a multinational network.

These examples illustrate very simply some generic types of data flow patterns. The aggregate data flows actually may combine several of these simplified component patterns. An important consideration is whether a particular type of data flow arrangement affects legal compliance problems. At a general level, regulatory conditions and, hence, technical concerns, are influenced greatly by the direction of the transmission, the geographic location of computation and storage functions, and, most importantly, the location of the user.

II. COMPLIANCE WITH NATIONAL DATA PROTECTION LAWS

An organization that collects, exchanges, or transfers personally identifiable data (or in some countries data on legal persons),[15] such as a multinational enterprise that transfers employee data, may be regulated by the provisions of "data protection" or fair information practices laws that sometimes restrict transborder data flows. A regulated entity that operates within a given country is subject to the applicable requirements imposed by that country's national data protection law. Indeed, compliance requirements within each country may prove to be more expensive and restrictive for an organization than those restrictions imposed by transborder data flow regulations. The general problems of compliance with domestic laws and regulations are not treated here except insofar as extraterritorial users are concerned.

In the international context, a regulated entity faces two compliance problems:

1. National laws may prohibit, restrict, or control the transborder transfer of personally identifiable information. An organization that transfers data (as in Figure 1) may not be able to transfer certain information in a specific direction for a specific purpose;
2. National laws may have different compliance requirements. An organization that transfers personally identifiable information across national boundaries could be subject to different compliance requirements that affect the overall design and operation of a network or data base arrangement.

A. EXPLICIT RESTRICTIONS ON TRANSBORDER DATA FLOWS

Existing fair information practices laws are among the legal restrictions on transborder data flows that are based on the content and use of the information being sent. Other restrictions that put limitations on the entry, exchange, or exportation of computer-processed data usually are related to telecommunication facility access, tariffs, standards compatibility, or national security.

Current French law[16] requires government approval to transmit personally identifiable information outside France, but does not otherwise deny extraterritorial processing. In Norway,[17] certain personal information cannot be transferred out of Norway without per-

15. Austria, Denmark, Luxembourg, and Norway have provisions for legal persons. For a compendium see Novotny, *Restrictions on the Transnational Flow of Corporate Information*, 7 EDP AUDITOR 13 (1979).

16. Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, [1978] J.O. 227 (France).

17. Norwegian Act of 9th June 1978 Relating to Personal Data Registers (Norway).

mission of the King. Personal data processed by a service bureau cannot be held by a private organization in Denmark.[18] In Austria, there are no blanket restrictions against extraterritorial processing, but approval to export personally identifiable data is required from the Austrian Data Protection Commission (except in specified circumstances).[19] Prior approval for such transfers also is required under Swedish law.[20]

No comparable legal provisions exist in any United States statutes affecting information practices. The Canadian privacy law does not impose such restrictions either.[21] In those countries that restrict transborder data flows, the thrust of the claim seems to be made in the name of fair information practices, yet these restrictions leave much to the discretion of administrative entities charged with legal compliance. In most cases, the emphasis is on prior approval or licensing, and not on outright prohibitions on data flows. When this observation is combined with an analysis of actual fair information practices rules, the following observations emerge:

1. Organizations that engage in transborder data flows of personal information are less likely to encounter unacceptable consequences from international data flow exchange restrictions than from specific domestic compliance rules;
2. Since the emphasis of data flow restrictions seems to be on prior approval, system designers can anticipate (based on past approvals and disapprovals) the conditions under which approval is likely or unlikely.

On its face, it seems that the domestic features of fair information practices laws will have a greater impact on the operations of multinational organizations than will prohibitions against transborder data flows. Transfers probably will be granted except in cases of direct violation of established fair information practices principles, or in cases where an organization attempts to evade one country's laws. Consider this problem in more detail, as in Figure 2.

---

18. Private Registers Etc. Act, Act. No. 293 (1978) (Denmark).

19. In the following cases however, transfer by persons covered by Part 3 shall not require the consent of the Data Protection Commission: where the person responsible for the data processing is himself the person affected by the data transferred, or where the transfer is to a State which affords such data comparable protection to that provided by this Act, or where so provided by international agreement.

Data Protection Act, part 4, § 32(2) (1978), *printed in* BGB1 No. 565/1968 (translation approved by the Austrian authorities) (Austria).

20. Data Act, § 11 (1973) (Sweden).

21. An Act to Extend the Present Laws in Canada that Proscribe Discrimination and that Protect the Privacy of Individuals, 2d sess., 30th Parl., 25 Eliz. II (1978) (assented to 14 July 1977) (Canadian Human Rights Act, c. 33, Can. Stat. 887 (1977)).

FIGURE 2

COMPLIANCE PROBLEMS CAN RESULT WHEN TRANSACTIONS AND PROCESSING TAKE PLACE IN MULTIPLE JURISDICTIONS

(Personally identifiable information about a citizen of Country "A")

		Information is collected in:	
		COUNTRY A	COUNTRY B
Information is transferred for processing or storage to:	A	No transborder data flows occur. Country A's laws apply.	Country B's transborder transfer restrictions may apply, but Country A's domestic laws may apply to citizens of Country A when the data are in Country A. Country B's laws may apply at the time of collection while in Country B, but only if Country A's citizens are covered.
	B	Country A's transborder transfer restrictions may apply, but Country B's domestic laws apply if a citizen of Country A is under the jurisdiction of Country B's laws.	A citizen of Country A has no protection under Country A's laws. If Country B's domestic laws do not extend to citizens of Country A, then Country B's laws may not apply either.

Figure 2 exemplifies the difficult and complicated nature of technical fair information compliance in an international context. One overriding complication arises in applying the laws of country B to data concerning a citizen of country A that is collected in country A and processed or stored in country B. To protect citizen A's fair information rights, country A must supervise the exportation of data from country A to country B. In this situation, country B's fair information practices laws would apply to a citizen of country A. If country B's laws do not afford protection comparable to that guaranteed by country A's laws, data flow restrictions can result. For reasons of national security, jurisdiction, and international custom, a country cannot always grant citizens of a foreign state the same legal protection it offers its own citizens.

Further, when citizens of country A have information collected

about them in country B that is also processed in country B, they tend to lose protection of country A's fair information practices. Only when citizens of A have recognized rights under country B's laws would the provisions of country B's laws apply.

One solution to these multiple compliance problems might be to apply those legal provisions that are technically enforced at the place where the information is collected, or where the transaction takes place. Cross-border data processing, however, causes problems with this legal principle:

1. If citizens in country A request information about themselves in a data processing system in country B, country B's transborder data flow restrictions could prevent such a transfer, thus negating A's laws;
2. Even if citizens in country A could exercise their rights to data in country A, that data could be consolidated with other data collected in country B in the same file or even in the same record when shipped to country B. Would the two sets of laws each govern their respective pieces of the record?

These issues might seem at first to be rather arcane and narrow, but as personally identifiable transborder data flows are involved in increasing numbers of international business transactions, the problems of compliance become important. The first step in technical compliance is to isolate the jurisdiction of the particular law in question, if any. In certain instances no national laws may apply to information collected on a citizen of country A in country B and processed in country B.

Compliance is simple to determine in one directional ("type 1") processing where the "user" in country A obtains information about a citizen of country B that is then transmitted to the "home" country, B, for processing. This type of processing is typical of international credit card operations. Compliance with the home country's fair information practice laws is all that is necessary.

In type 2 flows, both the initial user and the processing host are located in one country so data export restrictions are the only rules that menace this type of data flow. In this instance, the fair information practices legislation of the initial user's country would be observed, including any restrictions on transborder data flows. This situation is analogous to a situation where a corporation's subsidiary in country A transmits information about employees and customers to a headquarters in country B. As long as data export restrictions are followed (and these have been shown to be fairly mild), there should be little or no difficulty in transmitting that information.

In two-way data transfers, however, the situation can be very

different. Type 3 flows, which are labeled transnational networks, involve users located in country A who have collected or are using information on citizens of country A. Processing is done in country B, but there are no users, at least no authorized ones, located there. As long as the only purpose for transmission to country B is for data processing, then requiring the user in country A to comply with fair information practices laws of country A should be sufficient. The geographic location of the user of the data, therefore, is very important for enforcing fair information laws in a transborder processing scheme.

When there are users in both countries, as in type 4 flows, the compliance situation is much more complicated. This case is analogous to decentralized data processing in which dispersed users send and receive information from several hosts in an international network. Conflicts of law problems can be avoided by using distributed systems that partition users and hosts.[22] Specific information would be loaded "downline" in hosts for specific uses in one country. Compliance procedures can then be implemented for each applicable distributed system. Consolidated information that does not violate transborder data flow restrictions can be transmitted to a host in another country, presumably the headquarters; the location of the user should determine which data flow restrictions to apply. In this way, the organization could realize the benefits of centralized reporting and meet individual country compliance requirements. It is uncertain as yet whether partitioning users and hosts would lead to unacceptable sacrifices in network efficiency.

B. Compliance with Specific Fair Information Practices

It would require considerable space to make a comparison of the specific requirements in the fair information practices laws of the ten countries that have adopted them. Such comparisons are already available.[23] Do the provisions of fair information practices legislation have special ramifications, costs, or other technical effects in an international context?

As discussed above, one-way transfers of personal information, while being subject to exportation restrictions, are bound primarily by the national compliance rules of the originating country. When information is centralized, dispersed users in various countries may

22. The international community has responded to the choice-of-laws problem by adopting in the OECD a set of voluntary fair information guidelines for transborder data flows. *See, e.g.*, Draft Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, DSTI/ICCP/79.40 (1979).

23. AFIPS Report, *supra* note 1, at 64; Novotny, *supra* note 15.

be compelled to observe different compliance requirements. These requirements would

1. Allow affected persons to inspect and amend their records or to correct errors;
2. Require that disclosures to third parties be recorded and made available; corrections or amendments to records must be communicated to organizations (third parties) that have received the original record;
3. Observe specific security rules to prevent unauthorized disclosure or modification of a data subject's record;
4. Enforce other specific fair information practices policies.

Any centralized system that processes personalized information in compliance with the first two requirements most likely will increase its processing costs if inspection, amendment, and third party disclosure accounting procedures are initiated at the user terminal level but handled through the centralized host. Transmission costs will reflect such increases, but normally will not be significantly large as long as the volume of requests is small. The organization will have to compare the costs of performing some localized processing against the transmission costs of type 3 or type 4 flows. Also, in the centralized system concept, there may be different fair information rules that apply to the same data base, thus requiring records to be segregable according to nationality.

III. ATTAINING AND MAINTAINING DATA SECURITY

By far the most cumbersome compliance problem in the international context is attaining and maintaining data security. Here, we are concerned with requirements set forth in national fair information practices laws and drafts from international conventions. The provisions in most of these rules use language that implies striking a balance between the risks of disclosure, modification, and so forth, and the costs of implementing such controls or of supervising their administration. Hence, the use of words such as "reasonable," "appropriate," and "necessary," in describing the preferred level of security. Typically, a regulated entity will attempt to enforce security controls in those areas that have substantial risks to the organization's operation or integrity, at least to the extent of management's attention to security matters. In the face of external rules that require security compliance at an unspecified level, regulated entities are subjected heavily to the discretionary judgment of data protection authorities. Regulated entities are compelled, therefore, to find that level of security that maximizes compliance while minimizing the costs of compliance.

The problems for the regulating entity are twofold:

1. The regulating entity must determine a set of specific compliance requirements that approximate the "necessary" and "reasonable" levels of security according to generally subjective judgments;
2. The regulating entity must allocate its enforcement resources to minimize the chances of violations.

Together, the problems of finding adequate or optimal levels of protection and surveillance have eluded both theorists and practitioners. Finding an optimal level of protection is not yet quantitatively demonstrable, particularly when defenses must incude physical, administrative, and technical security.[24] Knowing that one cannot yet attain "perfect" security, data protection authorities are compelled either to adopt arbitrary rules or to make rough estimates of where controls should be implemented by using risk assessment techniques. At the present time, there are substantial methodological limitations to such risk assessment techniques. While there have been some strides made in improving security evaluation methods, many problems have yet to be overcome.

In addition to complying with the data security provisions of national fair information practices legislation, multinational organizations occasionally protect their transmissions against electronic interception. One recent survey of European data networks[25] indicated that the number of commercial users employing cryptographic technologies is still very low. Most commercial, encrypted, international data traffic concerns funds transfers or intracorporate messages. Governmental communications use cryptography extensively. Techniques to protect against modification or message retransmission also can use authentication techniques in addition to, or in place of, cryptography; cryptography, however, probably will be more popular and more convenient to implement.

The first question asked about cryptographic protection is usually, "Against what threats is the technique to be used?" Cryptographic defenses may be very effective against commercial espionage and would-be computer-assisted criminals, but a regulated entity may encounter legal restrictions if it seeks to protect its data transmissions against governmental interception. National authorities with the technological capabilities have engaged in electronic surveillance of data traffic for intelligence-gathering purposes.[26] To facilitate the acquisition of such data traffic, and to

24. Glaseman, Turn & Gains, *Problem Areas in Computer Security Assessment*, 46 AFIPS CONF. PROC. NAT'L COMPUTER CONF. 105 (1977).

25. *See* OECD, *supra*, note 14.

26. *See* Kahn, *Cryptology Goes Public*, 58 FOREIGN AFFAIRS 141 (1979); G. LIPSCOMB, PRIVATE AND PUBLIC DEFENSES AGAINST SOVIET INTERCEPTION OF U.S. TELE-

prevent foreign adversaries from concealing their transmissions, such national authorities can demand that:

1. No cryptographic protection be used in commercial data transmission;[27]
2. The encryption key(s) be disclosed to government authorities prior to and during use by a commercial or private organization;
3. The cryptographic methods or algorithms used by private organizations be restricted to particular types prescribed by governmental authorities.[28]

In the United States, although domestic uses of cryptography are not forbidden outright, inventors of certain cryptographic devices and methods have encountered patent and other restrictions, particularly in the name of national security.[29] There also has been a widely-publicized controversy about the Data Encryption Standard.[30] These issues are particularly difficult to assess since much of the technology and practice is shrouded in extreme secrecy. It is not yet known, for example, whether the low usage of cryptographic techniques in international communication by private organizations is due to its discouragement by governments, to a perceived lack of need by commercial organizations, or to the difficulty of technical implementation. The potential international user of cryptographic protection finds matters complicated further because he must comply with the laws of both countries involved in the data transmission.[31] Approval must be bilateral for such use. Thus, in the United States, where controls are not strictly required, an organization desiring to set up encrypted communications must obtain permission from the other country involved. Often this cannot be done. If one country disallows the use of cryptography, the link cannot be protected.

IV. MONITORING AND SURVEILLANCE

Regulating entities must have some means of enforcing transborder data flow regulations and policies. In addition to conducting audits, holding security inspections, and enforcing reporting re-

---

COMMUNICATIONS: PROBLEMS AND POLICY POINTS (1979); *Hearing Before the House Subcomm. on Gov't Information and Individual Rights, Comm. on Gov't Operations*, 94th Cong., 1st & 2d Sess. (1975-76).

27. This is usually in national telecommunications regulations.

28. Kahn, *supra* note 26.

29. *Id.*

30. Diffie & Hellman, *Exhaustive Cryptanalysis of the NBS Data Encryption Standard*, 10 COMPUTER 74 (1977); Kolata, *Computer Encryption and the National Security Agency Connection*, 197 SCI. 438 (1977).

31. Nelson & Reisman, *supra* note 2; Norman, *supra* note 2, at 12-5 to 12-6.

quirements of regulated entities, authorities can monitor the data traffic itself. Pool and Solomon argue that such surveillance is not practical.[32] Intelligence agencies nonetheless have employed highly sophisticated software to identify, sort, and sift through massive amounts of raw, electronically-produced data.[33] These same agencies, in technologically-advanced countries, such as the United States, have pioneered computer technology related to their surveillance missions[34] and, therefore, have well-developed capabilities. It is relatively easy to identify international data traffic because:

1. In some countries, a private organization must obtain, by regulation, certain terminal equipment from a regulating entity before using the public network for data transmission. This action discloses that the user intends to transmit or receive digital information.
2. If a dedicated data line is leased to the user, this is also disclosed to and regulated by the telecommunication administration, and can be subject to restrictions on use.
3. Domestic networks typically feed international gateway switches where incoming or outgoing traffic is concentrated. At these points, surveillance can take place effectively.

This is not to say, however, that monitoring a large amount of international data traffic is elementary. There are substantial expenses involved in widespread surveillance activities. Only governmental authorities that are charged with national security responsibilities in technologically advanced countries have the resources to intercept this traffic usefully. Thus, it is possible that monitoring data flows is not so much a technological problem as one of governmental priorities. To the extent that transborder data flows represent a valuable source of strategic information, the temptation to collect such data will be strong, but investment in such a dramatic program to monitor data flows in order to enforce laws such as those relating to fair information practices is probably not likely and could be supplanted by other means of enforcement. It would seem logical for the regulating entity, therefore, to monitor suspicious targets selectively, rather than to gather large amounts of international data traffic indiscriminately in the hope of finding a violation.

Another proposal for technical enforcement would be to include a stream of identifying information in the transmission sequence of

---

32. I. POOL & R. SOLOMON, 3 POLICY IMPLICATIONS OF DATA NETWORK DEVELOPMENTS IN THE OECD AREA 79 (1980).

33. Kahn, *supra* note 26; *Surveillance Technology*, *Sen. Comm. on the Judiciary*, 94th Cong., 2d Sess. (1976).

34. Snyder, *Computer Advances Pioneered by Cryptologic Organizations*, 2 ANNALS OF THE HIST. OF COMPUTING 60 (1980).

a given message or data packet, *i.e.*, an electronic "license tag."[35] By capturing the contents of this identifying information, the source, destination, and clues to the information content in the bulk of the data could be determined. This proposal has, however, at least three serious problems.

First, strict standardization would be necessary to implement such a scheme. Data could be collected at a terminal session, attached to a data packet, or transmitted with each burst. Complications would be great because of the mixture of traffic that typically characterizes international multiplexed transmissions. Given the differences that exist over interface standards and protocols, it is difficult to conceive how consensus could be reached on a standard identifier. Further, it may only be possible to implement "data tagging" within a network similar to type 4 in Figure 1, and only when that network itself is constructed with strict internal standards. A regulating authority would have to identify those networks that require surveillance and that have the required rigor to be monitored in this way. Public data networks, such as those being planned or used in many Western European countries, would be likely choices, but no large scale plans seem to be developing in this regard.

A second problem is the attention given to messages and packets of data. It might be more effective to keep track of access and use of data files and data bases than to monitor every transborder transaction. Data protection laws typically license, register, or regulate data contained in files, and not transactions. Monitoring such transactions, such as funds transfers, could be feasible. Most international transactions of this type, however, are sent and received in a structured format anyway; there is no need to add redundant identifying data by tagging.

A third difficulty with such message identification is the price paid in increased transmission costs and in the degradation of network performance. Studies done on the effects of adding error correction bits to data transmission packets have shown that including parity bits can add over ten percent to the size of a given packet.[36] Performance degradation also can occur. Adding three bits to an eight-bit/character synchronous line roughly equals the savings in converting from an eleven-bit/character asynchronous line, but three bits is not sufficient for tagging. Assuming that the identifying information was to include approximately ten characters, a packet size of one hundred characters still would be inflated by ten percent.

---

35. Norman, *supra*, note 2, at 12-5.

36. Kimbleton & Schneider, *Computer Communications Networks: Approaches, Objectives, and Performance Considerations*, 7 COMPUTING SURVEYS 129 (1975).

V. EFFECTS ON PLANNING

The effects of data flow regulation on computer and communications planning was alluded to earlier in this Article. Others have examined data flow problems in the context of capacity planning.[37] Data flow restrictions might also influence an organization's network design, particularly its centralization or decentralization. Most of the current controversy still focuses on potential restrictions of operational, financial, or scientific data. To the extent that such restrictions were enforced, it would amount to a denunciation of these activities. Perhaps controls on data flows would be incidental to direct controls on trade and commercial activities that cause concern. More likely is a situation where dependence on certain types of processing, as in the service bureau case, will be managed by controlling facility access and tariffs. Surveillance also may afford a better tool against the regulated entities than would overt data flow restrictions.

This observation leads one to the tentative conclusion that multinational organizations engaging in data flows might consider some type of decentralization of facilities or data bases. This is especially relevant when some information is permitted to flow while other information is controlled. Registration may begin to discriminate among types of data and place different requirements on different segments of an organization's total data resources. As such, regulated entities must weigh the economics of centralized processing against compliance with each country's data protection laws.[38] This strategy may run counter to economic considerations or improved reliability (achieved dynamically through workload distribution by way of a multi-host network, rather than through static assignment of redundant processing resources). Clearly, in the face of increased data flow barriers, a multinational data flow network could be difficult to manage efficiently. One possible solution might be to promote the establishment of an interconnection standard to link domestic systems along clearly defined and controlled paths. Countries could then promote interconnection of national or even private networks, while still supporting geographically distributed data bases or computing resources.

CONCLUSION

This Article has examined a few of the near-term technical and

37. I. Pool & R. Solomon, *supra* note 11, at 32.

38. Sood, *Personal Privacy: Can the MNC's Afford to Respect It?*, 14 COLUM. J. WORLD BUS. 42 (1979).

legal questions raised by transborder data flow regulation. Significant questions remain for further analysis. Comprehensive information about data flow patterns and compliance problems is not yet available.

From the technical perspective, there are at least three issues that merit further research:

Data Network Interconnection—As national data networks, both public and private, begin to grow, there undoubtedly will be increased needs for international interconnection. Standards and protocols will be of concern, yet compliance, security, and surveillance questions will be of considerable importance and will become more complicated. Integrated data services that combine many forms of telecommunication will blur the traditional service distinctions and continue to raise definitional questions regarding data processing and data communication.

Software Protection—As international networking and the general progress of data processing increases, software systems will become more suitable for exporting and shared use in multiple countries. Copyright and patent protection for this aspect of data flow will require resolution.

Impact on Systems Design—As data restrictions spill over into issues involving dependency, vulnerability, and economic advantage, network and database designers will have to respond to national laws and regulations that require decentralization.

One can expect that technical considerations in transborder data flows will continue to be intertwined with political and legal issues. No doubt the increased use of computer communication systems on an international level will not diminish either the political controversies or the technical problems. There are also some obvious normative questions involving the free flow of information and other international legal principles that involve United States foreign policy and comity among nations. Isolating these problems from the practical concerns of legal and technical compliance will not solve them. Rather, one must gain an appreciation and insight into the application of broad political principles into the routine practices of transborder data flows. An important aspect of future cooperation and conflict in international telecommunications will rest on this application of broad political principles.