Incidental Paper:

Contracts for Transnational Information Services: Securing Equivalency of Data Protection

G. Michael Epperson

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

An incidental paper of the Program on Information Resources Policy.

Contracts for Transnational Information Services: Securing Equivalency of Data Protection.
G. Michael Epperson
Incidental Paper No. I-81-7. August 1981.

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Incidental papers have not undergone the reviewing process the Program requires for formal publication. Nonetheless the Program considers them to merit distribution.

Reprinted with permission from the Harvard International Law Journal.
Printed in the United States of America.

Printing 5 4 3 2

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University — Center for Information Policy Research

Contributors

6/7/82

Abt Associates Inc.
Action for Children's Television
Aetna Life & Casualty Co.
American District Telegraph Co.
American Telephone & Telegraph Co.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Automated Marketing Systems
A.H. Belo Corp.
The Boston Globe
Booz-Allen Hamilton
Business Information Publishing Co.
Canada Post
CBS Inc.
Channel Four Television Co. (Ltd.)
(United Kingdom)
Citibank N.A.
Codex Corp.
Communications Workers of America
Computer & Communications Industry Assoc.
Continental Cablevision, Inc.
Continental Telephone Corp.
Copley Newspapers
Cox Enterprises, Inc.
Department of Communications (Canada)
Des Moines Register and Tribune Co.
Dialog Information Services, Inc.
Digital Equipment Corp.
Direction Générale
des Télécommunications(France)
Doubleday, Inc.
Dow Jones & Co., Inc.
Drexel Burnham Lambert Inc.
Dun & Bradstreet
Economics and Technology, Inc.
Equifax Inc.
Federal Reserve Bank of Boston
Field Enterprises, Inc.
First National Bank of Chicago
France Telecom (France)
Frost & Sullivan
Gannett Co., Inc.
Gartner Group, Inc.
General Electric Co.
General Telephone & Electronics
Hallmark Cards, Inc.
Hambrecht & Quist
Harte-Hanks Communications, Inc.
Hazel Associates
Honeywell, Inc.
Hughes Communication Services, Inc.
E.F. Hutton and Co., Inc.
IBM Corp.
Information Gatekeepers, Inc.
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
Irving Trust Co.
Knight-Ridder Newspapers, Inc.
Knowledge Industry Publications, Inc.
Kokusai Denshin Denwa Co., Ltd. (Japan)
Lee Enterprises, Inc.
McGraw-Hill, Inc.
MCI Telecommunications, Inc.
McKinsey & Co., Inc.
Mead Data Central
Minneapolis Star and Tribune Co.
MITRE Corp.
Motorola, Inc.
National Association of Letter Carriers
NCR Corp.
National Telephone Cooperative Assoc.
New York Times Co.
Nippon Electric Co. (Japan)
Norfolk & Western Railway Co.
Northern Telecom Ltd. (Canada)
The Overseas Telecommunications
Commission (Australia)
Pearson Longman Ltd. (United Kingdom)
Pitney Bowes, Inc.
Public Agenda Foundation
Reader's Digest Association, Inc.
Research Institute of Telecommunications
and Economics (Japan)
St. Regis Paper Co.
Salomon Brothers
Satellite Business Systems
Scaife Family Charitable Trusts
Scott & Fetzer Co.
Seiden & de Cuevas, Inc.
Source Telecomputing Corp.
Southern Pacific Communications Co.
Sprague Electric Co.
Standard Shares
Telemation Management Group, Inc.
Time Inc.
Times Mirror Co.
Times Publishing co.
Torstar Corp. (Canada)
United Parcel Service
United States Government:
Central Intelligence Agency
Department of Commerce:
National Technical Information Service
National Telecommunications and
Information Administration
Department of Defense:
Defense Communications Agency
Department of Energy
Federal Communications Commission
Internal Revenue Service
National Aeronautics and Space Admin.
National Security Agency
United States Postal Rate Commission
United States Postal Service
United Telecommunications, Inc.
Voice of America
Warner Amex Cable Communications Inc.
The Washington Post Co.
Western Union

FOREWORD

The possibility of interruption of transborder data flow for personal privacy or national economic reasons is now a major threat to world commerce. Several countries have enacted Data Protection Laws within the last few years, which include restrictions on data exports where privacy infractions may occur.

Now that the Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data have been adopted by 20 of the 24 OECD countries, a common understanding among nations of what is meant by Paragraph 17 is urgently needed:

> A member country should refrain from restricting transborder flows of personal data between itself and another member country except where the latter does not yet substantially observe these guidelines or where the re-export of such data would circumvent its domestic privacy legislation...(Emphasis added.)

This matter is especially important to the United States, since its domestic legal approach to privacy is substantially different from that in Europe. Most European governments believe that data protection in the U.S. is significantly weaker than in their own countries.

The purpose of this paper by Michael Epperson is to analyze alternate means of dealing with questions of "equivalency", or what constitutes compliance with Guidelines. He has prepared for our consideration some possibilities offered by our different legal approach, such as private contractual arrangements and existing private transnational legal mechanisms, for instance, choice of law.

For the United States, as a front runner in international data processing and the use of international telecommunications in business management, the economic stakes are immense. The question of equivalency looms ever larger in the minds of business executives and government officials. It is maintained that many investment decisions are being delayed until the matter is resolved. But, as of 1980, the voluntary Guidelines represented the highest level of consensus feasible among the OECD member countries, and it is unlikely that there will be significant further clarification through formal intergovernmental instruments any time soon.

While this short paper makes no specific prescription, it develops an interesting set of options which should serve to stimulate debate and perhaps also a search for other equivalency means outside the range of renewed government negotiation.

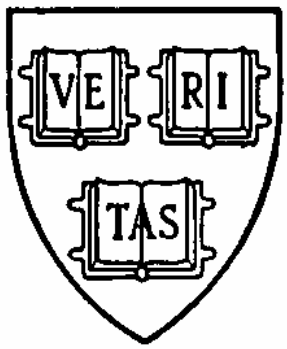
Oswald H. Ganley

HARVARD INTERNATIONAL LAW JOURNAL

NOTES

Contracts for Transnational Information Services: Securing Functional Equivalency of Personal Data Protection

G. MICHAEL EPPERSON



reprinted from
volume 22
number 1
winter 1981

VOLUME 22, NUMBER 1, WINTER 1981

NOTES

CONTRACTS FOR TRANSNATIONAL INFORMATION SERVICES: SECURING EQUIVALENCY OF DATA PROTECTION

INTRODUCTION

In recent years, many European states have enacted "data protection laws" designed to prevent the accidental or willful unauthorized use of personal data stored, processed, and disseminated by computers.[1] These laws are generally uniform among the European states, according a relatively high level of data protection. Many states, however, are concerned lest such protected data enter a second state where the data are less, or differently protected, thereby potentially circumventing the public policy of the sending state.[2] Accordingly, a number of these states have included provisions in their data protection acts which restrict the export of data by various means where privacy infringements may result.[3]

Due in part to the perception that data protection in the United States[4] is significantly weaker than in Europe, United States companies may be significantly affected by these restrictions.[5]

This Note promotes possible solutions to the problem posed by restrictive foreign data protection laws — employing contractual or choice-of-law approaches to achieve functional "equivalency" of United States and foreign law.[6] By either enumerating data protection pro-

1. F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE 1 (1975). *See also* Stadlen, *Survey of National Data Protection Legislation*, 3 COMPUTER NETWORKS 174 (1979); OFFICE OF TELECOMMUNICATIONS, U.S. DEPARTMENT OF COMMERCE, SELECTED FOREIGN NATIONAL DATA PROTECTION LAWS AND BILLS (O.T. Spec. Public. 78-19) (Wilk ed. 1978); Kirby, *Transborder Flows and the "Basic Rules" of Data Privacy*, 16 STAN. J. INT'L L. 27 (1980), and legislation cited therein.

2. Fishman, *Introduction to Transborder Data Flows*, 16 STAN. J. INT'L L. 1, 11 (1980). *See also* Address by Oswald H. Ganley, Dep. Ass't. Secy of State for Technology to the Conference on Transnational Data Flows, Information Gatekeepers (May 16, 1978), p. 4; Turn, *Privacy Protection and Security in Transnational Data Processing Systems*, 16 STAN. J. INT'L L. 67, 74 (1980).

3. Turn, *supra* note 2, at 74.

4. See discussion pp. 160–62 *infra*.

5. See discussion pp. 166–68 *infra*.

6. See notes 71–72 *infra*.

visions in the contract, or stipulating that the sections of the contract concerning privacy protection are to be governed by the law of the exporting state, the parties to the contract can satisfy the law and public policy of the exporting state.

THE PROBLEM

Personal Data

Personal data is information about an individual which is recorded and stored, either on paper or in a computer data bank. For the purposes of this Note, "data" is used in its computerized sense: information about individuals which has been reduced to operands or factors consisting of numbers or symbols which may be fed into and manipulated by a computer, transmitted electronically, to re-emerge upon command in the form of a computer printout.[7] The collection, processing, storage, transmission, and application of these data are today accomplished by combining computer and electronic communication technologies.[8] Thus, the use or transfer of personal information no longer requires the shuffling of paper or the procedure and time involved in mailing. For example, an unidentified person sitting at a computer terminal in Iowa can command a main computer in California to locate personal information about a group of individuals, to withdraw this information from the data bank in which it is being stored in Ohio and to send it to him, all in a matter of seconds. Nor is it significantly more difficult or time-consuming for this individual to subject the data to complex computer analysis. The highly technical, impersonal, and mechanized nature of these activities raises the specter of the personal data of individuals being shifted from computer to computer, altered, lost, read by those lacking consent, or otherwise abused.[9]

---

7. A DICTIONARY OF COMPUTERS 99 (Chandlor ed. 1970), *quoted in* HONDIUS, *supra* note 1, at 84. For a discussion of the technical aspects of data use and transmission, *see* Berman and Oettinger, *The Medium and The Telephone: The Politics of Information Resources*, in A. OETTINGER, P. BERMAN, & W. READ, HIGH AND LOW POLITICS: INFORMATION RESOURCES FOR THE 80's 89–107 (1977).

8. Professor Anthony Oettinger has coined the term "compunications" to describe the merging of the computer and communications technologies. *See generally* HONDIUS, *supra* note 1, at 85–86. *See also* Hurwitz, *On the Road to Wired City*, HARV. MAGAZINE (Sept.–Oct. 1979) at 18; Fishman, *supra* note 2, at 2.

Often transnational data processing involves operations taking place between computer components installed in different states, as with a central processing unit in state A and a terminal in state B. Swissair, for example, coordinates its agencies in over twenty European cities and New York by linking them via their terminals to a central terminal in Zurich which takes care of instantaneous seat reservation, passenger registration, weight calculation, etc. HONDIUS, *supra* note 1, at 246.

9. *See* Kirby, *supra* note 1, at 28.

The concern here is only with non-anonymous personal data, since the disclosure of anonymous data is presumably of little consequence to the "data-subject."[10] Such non-anonymous personal data can range from relatively innocuous records of newspaper and periodical subscriptions and mail order histories to such information as travel reservations, payroll records, and credit card usage to more easily misused data such as credit ratings, tax filings, and criminal histories. While the interest in preventing disclosure or use of any given kind of non-anonymous personal data varies with the individual, such subjective preferences are relevant to data protection laws only definitionally (i.e., in determining which kinds of data merit protection). For purposes of this determination, the sensitivity of data is largely evaluated from the standpoint of a "reasonable man." Once included within the definition, data are, however, for the most part, treated equally.[11]

Data Protection Laws

Personal data are created, stored and used by a variety of institutions such as insurance companies, banks and government agencies[12] who

10. The term "data-subject" is used to refer to the individual from or about whom personal data are collected.

11. The approach of the OECD Guidelines is illustrative. These guidelines reflect United States efforts to anticipate and respond to the negative implications of European data protection laws. *See* discussion pp. 166–70 *infra*. The successful diversion of multilateral negotiations concerning data protection from the Council of Europe, *see* Draft Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, contained in Meeting Report, addendum I, European Committee on Legal Cooperation (CDCJ), EUR. CONSULT. Ass. Deb. 33rd Meeting, CDCJ 80(28) addendum I(July 24, 1980)[hereinafter cited as Council of Europe Draft Convention], to the OECD resulted in a set of voluntary guidelines engineered to harmonize the data protection legislation of member states, the aim being to preserve the free transborder flow of information while giving adequate protection to personal data. Organization for Economic Cooperation and Development, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80)58[Final] Oct. 1, 1980). For a fuller discussion of these guidelines, *see* 22 HARV. INT'L L.J. 241 (1981).

Though not binding on OECD member states, these guidelines represent the broadest consensus yet to emerge among concerned states as to how to deal with privacy issues in the transborder data flow context. Fishman, *supra* note 2, at 19. These guidelines do not require the protection of "personal data which obviously do not contain any risk of privacy and individual liberties. . . ." OECD Guidelines, *supra*, annex at 3, ¶3(b). The decision as to what types of personal data are to be excluded from the scope of a data protection law is left to the discretion of the member state. OECD Guidelines, *supra*, App. at 22–24, ¶4(b).

In contrast to the OECD Guidelines, the Council of Europe has identified personal data revealing racial origin, political opinions, religious or other beliefs, health records, sexual matters or criminal convictions as special categories, presumed to be more sensitive. Council of Europe Draft Convention, *supra*, at 16, art. 6 (Special Categories of Data).

Even under this approach, however, the data are not afforded absolute protection. Rather, the Council of Europe Draft Convention states that such data "may not be processed automatically unless domestic law provides appropriate safeguards." *Id.* art. 6. Usage of data is permissible provided some sort of due process is established to guarantee that the records will be managed fairly.

12. Fishman, *supra* note 2, at 5.

make decisions affecting individuals on the basis of such data, the existence and use of which may be unknown to the data-subject.[13] The widespread perception that the creation, use and abuse of personal data are growing beyond economic or legal control[14] has led to the adoption of specific data protection laws in Western Europe (Europe),[15] Canada,[16] and the United States.[17]

"Data protection" is a European term containing several elements of the American concept of "privacy."[18] Data protection does not,

---

13. *Id.*

14. *Id.* For example, one commentator has characterized a segment of the recent United States privacy legislation as "Watergate legislation", meaning the law resulted from the fact that government agencies kept the existence and use of records about individuals secret, and in some cases, used such personal data, especially tax information, improperly. "Watergate Legislation in Retrospect" Remarks of Benjamin R. Civiletti, Attorney General of the United States, at the University of Chicago Law School and Alumni Ass'n, Hyatt-Regency Hotel, Chicago, IL (Apr. 25, 1980).

15. Kirby, *supra* note 1, at 27. As of July, 1980, Austria, Denmark, France, the Federal Republic of Germany, Luxembourg, Norway, and Sweden have enacted data protection laws. Explanatory Report contained *in* Council of Europe Draft Convention, *supra* note 11, at Appendix IV, 27. In other states such as Belgium, Iceland, the Netherlands, Spain, and Switzerland, data protection laws are in preparation or are in the advanced stages of the legislative process. *Id.* Furthermore, three states (Spain, Portugal, and Austria) have established data protection as a fundamental right by incorporating it in their national constitutions. *Id.*

16. *See* Canadian Human Rights Act, ch. 33 [1976–1977] Can. Stat. 887 (1977).

17. The basic United States response was the passing of the Privacy Act of 1974, 5 U.S.C. § 552(a) (1976). For a discussion of this act, *see* Kirby, *supra* note 1, at 36–39. Other United States legislation involving privacy rights include the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (1976); Fair Credit Reporting Act, 15 U.S.C. § 1681 (1976); Right to Financial Privacy Act of 1978, Pub.L. No. 95-630, §§ 1100–22, 92 Stat. 3697 (*codified in scattered sections of* 5, 12, 18, 31, 42, U.S.C.); Tax Reform Act of 1976, 26 U.S.C. § 6013 (1976); Freedom of Information Act, 5 U.S.C. § 552 *as amended by* the Government in the Sunshine Act, 5 U.S.C. § 552(b) (1976).

18. Turn, *supra* note 1, at 69. The American concept of privacy embraces several concepts. *Compare* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)(the right to be left alone) *and* Comment, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CAL. L. REV. 1447 (1976) *with* L. TRIBE, AMERICAN CONSTITUTIONAL LAW 887–88 (1978) (pointing not only to the right to be free from stimuli that impact on oneself, but also to the interest in having impact on others — particularly the interest in influencing one's own public image or reputation) *and* Whalen v. Roe, 429 U.S. 589 (1976) (suggesting that the constitutional right of privacy embraces an "individual interest in avoiding disclosure of personal matters").

In *Whalen*, the state of New York had enacted a statutory scheme for maintaining computerized records of prescriptions for certain dangerous but lawful drugs. The regulation responded to the state's concern that prescription drugs with "illegitimate uses" might be diverted to unlawful channels, 429 U.S. at 591. Specifically, the scheme attempted to prevent the use of stolen or altered prescriptions, to regulate the potentially illicit prescription practices of physicians, and to prevent users from obtaining prescriptions from more than one physician. 429 U.S. at 592. To achieve these ends, records were made of prescriptions issued for certain drugs. These records included the identity of the physician and the patient. The records were then transferred to magnetic tapes for processing by a computer. 429 U.S. at 593. Procedures aimed at safeguarding the privacy of the patient were substantial. 429 U.S. at 594. The Court, relying on the seriousness of the state's concerns and the rigorous nature of the privacy safeguards, concluded that the risk of access or use was too insubstantial to pose a real threat to patient privacy. Consequently, the Court upheld the statute, stating that "neither the immediate nor the threatened impact of the patient identification requirements . . . on either the reputation or the independence of patients . . ." was sufficient to require constitutional protection. 429 U.S. at 603–04.

however, mean that all such privacy interests will be fully protected.[19] The term refers less to absolute prohibition of the accumulation and usage of data than to the establishment of procedures guaranteeing to data-subjects the opportunity to know of the existence of data concerning them and of the uses to which such data will be put, a concept usefully referred to as "fair record management."[20]

The risk of harm to which data protection responds depends generally not on the content of the data but on the context in which they are used.[21] The origin of the concept of fair record management lies in the recognition that computerized recordation and manipulation of information about individuals is an unavoidable concomitant of the increased reliance on computers taking place in both developed and developing states. The telling superiority of the computerized method of storing and processing data is unassailable; the efficiency, accuracy, and economy with which data may be handled have impelled the widespread acceptance of its use. The question is not, therefore, whether to accumulate and use data, but rather how to do so "fairly." Instead of outlawing the accumulation and use of data, data protection laws seek merely to offer a sort of "due process" to the data-subject. As long as the data are used for permissable purposes and managed fairly, their use is lawful.

While both European and United States legislation in this area proceed from substantially the same core of principles of personal privacy protection[22] embodied in the concept of fair record manage-

---

19. For example, in *Whalen*, *supra* note 17, Justice Stevens focused not upon the general right to control the personal information an individual projects upon society, but upon the narrower right to *withhold* information one does not want to share with others 429 U.S. at 599–600. Stevens went on to deny absolute protection to this latter right.

Personal privacy protection in the United States is seen as a matter of civil rights, Fishman, *supra* note 2, at 5, and not as a matter of protection of rights in property. The notion of ownership of information is untenable. *See* HONDIUS, *supra* note 1, at 104. According to Hondius, the law recognizes only certain rights, obligations and interests with regard to information. He offers an example limning the dilemma of ownership of computerized information:

> The question of ownership of computerised information can be demonstrated by two examples. When a doctor in a hospital stores medical information about a patient in the hospital's computer, three ownership theories might be defended: primo, the hospital owns the computer, ergo it owns the information; secundo, the doctor has obtained the information and formulated it in words, so he is the owner; tertio, the patient has generated the information and therefore owns it. In actual fact, none of these three theories is tenable in relation to the other two. The solution lies in the delimitation of the rights and obligations of these various parties with regard to the information. *Id.*

Once disclosed, information, like speech, becomes common and non-exclusive, absent copyright protection.

When a bit of information becomes known to others, the originator of the information cannot, by stating that he owns it, claim the information back and demand that all auditors forget its contents. Similarly, a secret, once revealed, is no longer a secret. *Id.* at 103.

20. Fishman, *supra* note 2, at 5.

21. Council of Europe Draft Convention, *supra* note 11, App. IV at 35, ¶43.

22. Fishman, *supra* note 2, at 11.

ment, their approach, and the scope of protection offered differ significantly.[23] Characteristically, European data protection laws provide substantive safeguards in three major areas. First, the laws establish limits on the collection of data, and require that the purposes to which the data are to be put be specified prior to their actual collection.[24] Any subsequent use of the data must be in accordance with these specified purposes, unless authorized by the consent of the data-subject or otherwise provided for by law.[25] Second, they typically include provisions aimed at ensuring the reliability of the data. These provisions require that individuals be notified that personal data records about them exist, and that they be given both access to their own files, and the opportunity to correct or amend erroneous data.[26] Finally, most of these laws regulate the storage and usage of personal data. In addition to requiring procedures assuring the security of data against loss, destruction, or unauthorized disclosure, these laws require that any use or disclosure be recorded, and that the data-subject be notified of any unauthorized use or disclosure.[27]

Equivalency of Laws

Telecommunications has removed all technical obstacles to the international transmission of data,[28] rendering distance and geographical barriers virtually irrelevant in a cost or operational sense.[29] Customers are increasingly seeking data processing and information services abroad due to the fact that such services can often be performed there more cheaply, or because domestic facilities with the desired technical capabilities or expertise may not be available.[30]

The increasing demand for foreign data processing and information services coupled with the enactment of data protection laws creates the potential problem of "equivalency of laws."[31] That is, if the protection afforded data in the state to which they are being sent is weaker than, or incompatible with, that provided in the home state,[32]

---

23. See discussion at notes 12–22 and accompanying text.
24. *See* Fishman, *supra* note 2, at 11; Turn, *supra* note 2, at 73.
25. *See* Fishman, *supra* note 2, at 11.
26. *See* Turn, *supra* note 2, at 73.
27. *See* Fishman, *supra* note 2, at 11.
28. HONDIUS, *supra* note 1, at 242.
29. Fishman, *supra* note 2, at 8.
30. Alternatively, needed information may be available only in a foreign data bank. Address by Oswald H. Ganley, Dep. Ass't Secy. of State for Technology, to the Computer Business Equipment Manufacturers Ass'n, Transborder Data Flow — Some Problems of Privacy versus Freedom of Information and Economic Issues, in Phoenix Arizona (March 20, 1978). Hondius discusses three stimuli for transborder data flow that are not strictly economic: the internationalization of markets, increasing administrative relationships between states, and the activity of international organizations. Hondius, *supra* note 1, at 242.
31. Turn, *supra* note 2, at 74.
32. *Id.*

the export of data to the former would tend to erode the higher or different standard of the exporting state.[33] In an attempt to stem this erosion, many states have insisted on equivalency of data protection laws between themselves and receiving states before allowing personal data to be exported.[34]

For several reasons, many European states believe that the standard of data protection in the United States is impermissably low.[35] First, unlike the omnibus data protection legislation in most European states, United States law does not cover both the private and public sectors.[36] Currently, United States federal law pertains to only federal agencies, and only twelve states have enacted fair information practices laws.[37] Second, while European legislation extends protection to all persons within the state,[38] the major United States legislation[39] protects only United States citizens and resident aliens. Third, the United States, unlike most European states, has no single agency charged with the enforcement of privacy protection laws.[40] Many European states, therefore, are likely to conclude, if they have not already done so,[41] that the United States data protection regime is not equivalent to their own.[42]

Theoretically, an exporting state can evaluate the equivalency of another state's data protection law to its own either legally or functionally. Under the legal approach, the exporting state will export only to those states whose legal regime for the protection of data

33. Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87, 102 (1980).

34. See note 2 *supra*.

35. *See* Address by Oswald H. Ganley, *supra* note 2, at 4. *See also* Turn, *supra* note 2, at 75.

36. Turn, *supra* note 2, at 75.

37. *Id.* Consequently, state governments and agencies are, in most states, unregulated. Privacy laws relating to the private sector protect only consumer credit, educational institutions, and financial institutions. *Id.*; Fishman, *supra* note 2, at 5. European privacy laws generally cover both sectors completely. Turn, *supra* note 2, at 76.

38. Turn, *supra* note 2, at 76. European privacy laws usually extend to all persons regardless of citizenship and nationality.

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

40. Under the Privacy Act of 1974, 5 U.S.C. § 552(a) (1976), the Office of Management and Budget has a nominal role in coordinating compliance, and the President is to make an annual compliance report to Congress. It is up to the appropriate agency to enforce privacy laws relating to the private sector. This decentralization of authority contrasts with the centralized protection systems of many European states. Turn, *supra* note 2, at 76.

The European agencies have been analogized to consumer protection bodies. Hondius, *supra* note 33, at 95. Their main task is the advising of data users and the government about data protection and potential abuses, although they also have the power to bring legal action and to impose administrative sanctions against data users who violate the law. *Id.* at 101–02. Hondius notes that several European criminal codes now contain computer-related offenses such as illegal intrusion into or divulgence from an automatic file. *Id.*

41. In addition, several of the European (and developing) states have not yet passed data protection laws, although several such laws are in an advanced stage of the legislative process. It is too early to predict what kind of restrictions will appear.

42. Ganley Address, *supra* note 2, at 4. *See* Turn, *supra* note 2, at 75–76; Fishman, *supra* note 2, at 11–12.

substantially replicates its own. Due to the perceived laxity of United States legislation in this area, a European state which adopted this approach might very well deny the export of data to the United States. Presumably the only viable options available to the United States which would result in lifting of the export ban would be either to enact legislation substantially similar to that of the exporting state, or to convince the exporting state that existing United States law is, in fact, substantially similar.[43]

Alternatively, an exporting state adopting the functional approach would permit the export of data in any case in which the data are guaranteed sufficient protection, irrespective of the legal regime of the importing state. Thus, a state requires an equivalent level of protection abroad, but leaves open the means of ensuring that protection, be it by the law of the importing state, by contract, or by other means.

In response to the equivalency problem, all seven of the European states which have passed data protection laws place some restriction on the transmission of personal data abroad.[44] Although these restrictions vary from state to state, the standard of functional equivalency is implicit in the laws of all seven; none flatly prohibits the export of data to states with weaker or inconsistent legal regimes.

Most of these states attempt to achieve equivalency by requiring the issuance of a license or approval by a data protection board or commissioner.[45] The Federal Republic of Germany, for example, allows personal data to be transmitted abroad upon the determination

---

43. In actuality, the privacy protection afforded in the United States may in some instances be *greater* than that secured by the new European omnibus laws. United States laws are broader in scope, reaching to manual as well as automated data systems. Turn, *supra* note 2, at 76. United States laws have developed piecemeal, area-by-area. See note 17 *supra*. They have been tailored to provide protection in the specific context, whether it be educational, credit, or governmental records. The United States as a general matter fears abuse of personal data sooner from the public than from the private sector. See note 14 *supra*. The practice, adopted by several European states, of using universal "personal identification numbers" (PINs) as a means of achieving centralized control of personal data, has, due to its Orwellian intimations, been deemed unacceptable in the United States. Turn, *supra* note 2, at 76.

However, the absence of blanket legislation in the private sector constitutes an infirmity only if some context posing dangers to data-subjects is left uncovered by piecemeal legislation. Moreover, the conclusion that personal data stands unprotected can not be drawn from the mere absence of a statutory enactment covering the data. Common law protection of individual liberties and requirements of openness in governmental decision-making offer a variety of remedies to the data-subject. *See id.* The combination of statutory plus common law remedies pursued through the courts renders omnibus legislation unnecessary. The difference between the United States and Europe with respect to data protection, therefore, is quite possibly not so much a difference in rigor as one in approach, which can be understood partially as a reflection of the different legal systems — civil versus common law. Thus, it remains open to try to convince the relevant exporting state to temper its demands by recognizing the functional equivalency of United States data protection legislation.

44. Turn, *supra* note 2, at 72.

45. *Id. See also* Hondius, *supra* note 1, at 248; Council of Europe Draft Convention, *supra* note 11, App. IV at 27.

that the data-subject will not be "harmed" thereby.[46] Section 11 of the Swedish Data Act[47] provides:

> if there is reason to assume that an item will be used for data processing abroad, it may be released only after permission by the Data Inspection Board. Such permission may be granted only in cases where it can be assumed that the disclosure will not entail undue encroachment on privacy.[48]

Nonetheless, these laws establish only the contours of an equivalency standard. "Harm" to the data-subject and "undue encroachment on privacy" are unnecessarily vague. It is incumbent upon the various data protection agencies to give content to these, and similarly indefinite terms that make the reach of these laws uncertain.[49] Since under the licensing approach, these agencies must examine and approve the operations and procedures of data banks and data processing firms before they may utilize domestic data,[50] not only will proper procedure be guaranteed in individual cases, but a more ascertainable general standard will be established thereby.

Notwithstanding this, licensing of foreign databanks poses its own special problems. For example, even if a foreign company is willing to establish the proper procedures necessary to get a license,[51] the data protection agency might still refuse to issue an authorization, due to the inability to ensure compliance by ordinary means of supervision, inspection, and audit.[52] Additionally, there is no precedent regarding the enforcement of data protection laws in the transnational context.[53] Presumably, the license would be subject to revocation in the case of a violation, but whether further remedy would be available is unclear.

A Hypothetical

The following relatively simple hypothetical[54] may help to illustrate problems of transnational data transfers. A foreign state, known as

---

46. Federal Data Protection Act, [1977] BGBlI 201 (West Germany); *see* Ganley Address, *supra* note 30, at 4.

47. Data Act of 11th May, 1973, § 11, *as amended on* Jan. 19, 1977 (Sweden).

48. *Id.*, as translated in Hondius, *supra* note 1, at 248.

49. The efforts undertaken by the Securities and Exchange Commission to give content to the 1933 and 1934 Acts provide a possible example of what is required.

50. *See* Hondius, *supra* note 1, at 221–227.

51. Two types of licenses may be distinguished: the specific transaction may be licensed, or the specific company or databank may be licensed. The latter form presumably allows multiple transactions to occur under a single license. Decisions regarding types of licenses to be issued are a matter of agency discretion.

52. Hondius, *supra* note 1, at 227–235.

53. Ganley Address, *supra* note 30, at 5.

54. The hypothetical is simple in that it involves the movement of data from only one state into one other. Fishman presents what is perhaps a more realistic hypothetical:

"Exporter," has a data protection law requiring periodic disclosure to data subjects of the fact and nature of any utilization of data concerning them. The law also contains a provision permitting the export of personal data only if "DataBoard," a data protection board established by the law finds that such export will not materially lessen effective disclosure of data usage to the data-subject. "Customer," a corporation in the state of Exporter, wants to contract with "Data Bank," a United States data processing corporation, for various information services. One or more of these services involves the transmission of personal data of the customers of Customer by Data Bank to its storage facilities in the United States. DataBoard, pursuant to the export provision in the data protection law, refuses to approve the contract between Customer and Data Bank on the grounds that United States laws require materially less disclosure of data usage to data-subjects than does the data protection law of Exporter.

Negative Implications of Transborder Data Flow Restrictions

Restrictions on the transborder flow of data involve serious costs to both exporting and importing states; in the hypothetical set out above, both Exporter and the United States stand to suffer harm.

Data Bank and the United States

DataBoard's refusal to approve the contract will result in a loss of access to the markets of Exporter by all companies, like Data Bank, that depend on computer facilities or data banks situate within the United States. Since a great quantity of foreign data is currently

---

A hypothetical will illustrate the problems involved. The health records of a Swiss national are collected by his employer in Switzerland. Using leased private (dedicated) lines procured from a series of European PTT's, the employer transmits the data to corporate headquarters in Amsterdam where they are processed, stored, and aggregated with health records of other nationals working in other countries. The aggregated, partially processed data, after being stored in Amsterdam, is then sent on, via international facilities jointly owned by numerous countries, to a U.S. owned data processing service whose primary facilities are in the U.S. When the data arrive at this facility they are held in a buffer or electronic storage system. Holding time can vary from milliseconds to minutes or hours. While being held the main computer breaks down and an automatic switch sends the data through international telecommunications facilities onto a secondary processing facility in Hong Kong. There the data are processed and returned to the primary facility where they are stored for a short time in the now functional primary computer. A copy of the processed data is sent to storage at the primary site, and the data are returned to Amsterdam. The employer, having received the fully processed health data, now sends it along via EURONET to the employer's insurance carrier, and Italian firm whose primary data processing facilities are located in Spain. The insurance carrier again processes the data, stores them in Madrid on magnetic tape and issues the appropriate group health policy to the employer. Fishman, *supra* note 2, at 21. *See also* Hondius, *supra* note 33, at 103–04 (1980). For other situations in which the equivalency problem arises, see Turn, *supra* note 2, at 77–80.

processed within the United States, the economic effect of this loss of access and the attendant substantial losses of revenue would be monumental.[55] Primarily affected would be United States-based data processing and information services,[56] as well as those transnational corporations having lines of business supported by flows of personal data across international boundaries, such as credit card issuers.[57] The United States firm, in order to retain its business in the exporting state, would have to establish a subsidiary therein, or in the case of a multinational corporation, completely regionalize its record-keeping operations outside the United States.[58]

Another consequence of these restrictions would most likely be assaults by foreign competitors on the dominant worldwide position held by the United States today as a provider of data processing services.[59] Given restricted United States competition, domestic information service providers certainly stand to gain a larger segment of the local market. The restructuring by United States firms of their record-keeping operations to take place entirely within the foreign

---

55. Ganley Address, *supra* note 2 at 5. For a discussion of the commercial implications for the United States of international data processing, *see* Ganley Address, *supra* note 30.

According to Ganley, American interests in international data processing are "enormous". *Id.* at 2. Department of Commerce data for 1975 show earnings in the OECD countries alone of nearly $1 billion, shared among American common carriers providing transoceanic transmission for data processing, independent service bureaus selling data base or software services, manufacturer services bureaus of major computer manufacturers providing data processing services either directly or through subsidiaries, and software vendors operating in Europe. *Id.* The $1 billion figure for 1975 did not include the transborder transmission of information in the course of the business of general United States industries, such as airlines, auto manufacturers, banking and finance corporations, hotels and major trade associations. *Id.* at 2–3.

See also "Transborder Data Flow — A Significant Factor in World Trade?", Address by Oswald H. Ganley, Harvard University Program on Information Resources Policy, before the Second Annual Conf. on Transnational Data Flows, Information Gatekeepers, June 18, 1979; "Transborder Data Flow: Competition or Strangulation?", Address by Oswald H. Ganley before the United States-Japanese Symposium, International Communications: New Challenges and Responsibilities, in Boston, Oct. 11, 1979, at 5–8.

56. Ganley has identified two additional areas where the adverse implications of non-equivalency could be great. These are governmental agencies, and Research and Statistical Data Banks. Ganley Address, *supra* note 2, at 8–9.

57. *Id.* at 6. Credit card issuers affected would include entertainment and travel card issuers, e.g. American Express, Diners Club, and the United States flag commercial carriers (TWA, etc.), as well as the bank card issuers, such as Visa and MasterCharge. In each case, the issuer could be prohibited from communicating transactional data to the United States. *Id.* at 6–7.

Another aspect of the problem involves the transborder flow of data produced by a United States citizen in a foreign state. The data protection laws of many European states apply to the export of data about all persons present in the state, both citizens and aliens alike. Export of data about the use by a United States citizen of his card could be prohibited. Yet the majority of United States credit grantors depend on having access to the complete history of a United States card holder's use of his credit privilege. *Id.* at 7.

Other problems could arise for multinational corporations which process their employee records in the United States. *Id.*

58. *Id.* at 6, 7.

59. *Id.* at 5.

state would bring to that state employment opportunities, increased revenue from taxes, increased national product, and a more favorable balance of payments.

These numerous benefits demonstrate that economic motivations may lie behind a state's enactment of legislation restricting transborder data flows. Many fear that European states, mouthing the shibboleth of data protection, could establish barriers to the free flow of data that are aimed at gaining economic advantages[60] rather than protecting the data-subject.[61] Moreover, because the indeterminate language of the data protection laws and the wide discretion left to the data protection agencies will allow, as a practical matter, the constriction of data flows whenever harm to the data-subject is even remotely possible, the mechanism necessary for the establishment of such barriers already exists.

One need not assign ulterior motives to the data protection agencies or their members in order to understand this concern. Data protection agencies, like administrative agencies generally, may be susceptible to "capture" by those industries it regulates and those interests it protects.[62] At the very least, the inclination to act in favor of those domestic interests with whom the agency must deal on a daily basis, and to the detriment of foreign, distant corporations, might well be great. In any event, the United States must endeavor to reduce the establishment of non-tariff barriers whatever the actual motivations; the staggering economic consequences of such restrictions would be the same whether they were produced in good faith by overzealous data protection boards, or whether they emanated from ulterior economic motives unrelated to data protection.

Customer and Exporter

The major non-economic gain to Exporter from its prohibition of the export of personal data to the United States is the absolute assurance that its data protection policy will not be undermined by potential abuse in the United States. This does not mean, however, that harm would have occurred to data-subjects in Exporter had the data in fact travelled to the United States, or even that it was likely to occur. Still, even conceding that such prohibition of transborder flows of personal data promotes Exporter's policy of data protection, that gain

60. The economic motivations for restricting data flows are numerous. *See generally* HOUSE COMM. ON GOV'T OPERATIONS, INT'L INFORMATION FLOW: FORGING A NEW FRAMEWORK, H.R. REP. NO. 96-1535, 96th Cong., 2d Sess. 5 (1980).

61. *See, e.g.*, Fishman, *supra* note 2, at 12.

62. *See* Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1667, 1667–87 (1975).

is counterbalanced by the economic and political costs both Exporter and Customer stand to suffer from this restrictive practice.

Although, as discussed above, the data service industry of Exporter stands to gain from the prohibition, other sectors of Exporter's domestic economy are unlikely to benefit.[63] Specifically, due to the fact that the leading suppliers of data services are United States-based companies like Data Bank,[64] Exporter's prohibition against doing business with these companies may inflict serious economic costs on those domestic enterprises which, like Customer, have a need for data services, or could do so only by incurring an unacceptable loss of productivity, their only viable alternative would be to engage another (non-United States) data service company, a company which it presumably initially passed over in favor of Data Bank.[65]

All the costs associated with the refusal of DataBoard to approve the contract between Customer and Data Bank underscore the tension between the goals of safeguarding privacy interests and maintaining the free flow of data. This tension has been of major concern to the developed states, who recognize that the unrestricted transborder flow of information is a fundament of international commercial interchange and growth.[66] Reflecting this concern, two major multilateral attempts have been made to harmonize national data protection legislation.[67] Both the Draft Convention of the Council of Europe,[68] and the Guide-

---

63. HOUSE REPORT, *supra* note 60, at 5.

64. *See generally* Ganley Address, *supra* note 2, at 3.

65. Such a company may offer less capacity, flexibility or expertise to Customer, or be more expensive due to smaller volume or inferior technology. Moreover, if Customer competes with foreign enterprises which have free access to United States data service companies, Customer might be placed at a competitive disadvantage.

66. *See* Kirby, *supra* note 1, at 27–28; Turn, *supra* note 2, at 75.

67. Remarks of William F. Fishman, of the National Telecommunications and Information Administration, presented to the American Society of International Law, in Washington, D.C. (Apr. 18, 1980) at 4–5.

68. Article 12 of the Council of Europe Draft Convention provides:

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

lines promulgated by the OECD[69] state explicitly that the goal of data protection should not unduly restrict the transborder flow of information.

Though non-binding, both documents begin by establishing, as the general rule, the proposition that states should not prohibit or restrict the free flow of transborder data, although exceptions are permitted in situations where the export of personal data would contravene the privacy legislation of the exporting state. Under settled rules of international treaty construction such exceptions will be scrutinized and construed narrowly.[70] Furthermore, the language of both documents provide that there are no such exceptions where "effective" or "equivalent" (i.e., functional) equivalency of privacy legislation exists. Thus, both approaches strike a balance by recognizing that the free flow of information should be impeded only when absolutely necessary to preserve the policy of data protection. As shown above, there is also a consensus that this balance is best achieved not by rigid requirements of legal equivalency, but through solutions which effect a functional equivalency of privacy legislation.

---

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

Council of Europe Draft Convention, *supra* note 11, Appendix III at 18.

69. Part three of the OECD Guidelines pertains to the free flow of information:

BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

OECD Guidelines *supra* note 11, at 6. For a discussion of these guidelines, *see* 22 HARV. INT'L L.J. 241 (1980).

70. Provisions of an international agreement which could be interpreted so as to impose obligations on, or otherwise impinge upon the sovereignty of either party will not be so interpreted in the absence of an express intent of the parties. *See, e.g., River Oder Commission Case*, [1929] P.C.I.J., Ser. A, No. 23, at 26; *Frontier between Turkey and Iraq*, [1925] P.C.I.J., Ser. B, No. 12, at 25; 5 HACKWORTH, DIGEST OF INTERNATIONAL LAW 609 (1973). This accords with the rule in the *S.S. Lotus*, (1927) P.C.I.J. Ser. A, No. 10, at 18, that "Restrictions upon the independence of states cannot . . . be presumed."

SECURING FUNCTIONAL EQUIVALENCY

It is possible to establish functional equivalency by resort to either of two approaches — contractual or choice-of-law. Neither of these approaches will ensure the ironclad protection of data guaranteed by a rigid requirement of legal equivalency, but because such a rigid requirement is untenable, Exporter must accept solutions that promise to afford functional equivalency. For the reasons discussed below, both the contractual approach and the choice-of-law approach should give adequate assurance to Exporter that it will be possible to monitor compliance and obtain effective legal remedies in the event of non-compliance.

Exporter's sole concern should be that adequate data protection is *in fact* provided. Under both the contractual and choice-of-law approaches, the sufficiency of such protection is contingent upon the existence of two factors: standing to sue for either DataBoard, Customer, or data-subject(s); and an effective remedy which the courts are able and willing to apply. In evaluating these potential problems, attention will be focused only upon their resolution in United States courts. Presumably, they present no obstacle where suit is brought in Exporter under Exporter's data protection law.

Under the contractual approach, the parties specify the respective rights and duties necessary to comply with Exporter's data protection law in the contract itself. This may be achieved in either of two ways. First, the parties might spell out the commitments and procedures to which they must adhere in order to satisfy Exporter's law.[71] Alternatively, they may incorporate the law of Exporter, either in actuality or by reference.[72] In either case, the same problem of standing exists.

As a party to the contract, Customer is entitled to sue for a breach thereof. However, only when Customer stands to suffer economically, for instance where Customer's clientele have been angered by Data Bank's disclosure of information about them and withhold their business, does Customer have any incentive to sue Data Bank. But, in many cases, Customer, unlike the data-subjects or DataBoard, has no such incentive to sue, and therefore cannot be relied upon to police Data Bank's compliance with Exporter's data protection law.

---

71. That is, Data Bank will scrutinize Exporter's data protection law and determine what procedures will be required in order to comply with this law. Data Bank will then covenant that it will establish and maintain the necessary procedures, spelling out in detail its commitments and duties.

72. *See, e.g.* E. Gerli & Co. v. Cunard Steamship Co., 48 F. 2d 115, 117 (2d Cir. 1931) (L. Hand, J.). Incorporation of the terms of Exporter's data protection law requires merely the duplication of that law and the inclusion of these pages in the contract. More simply still, the parties might merely incorporate the law by reference.

Generally, only the parties to a contract are deemed to have a sufficient interest to be allowed to sue for a breach thereof.[73] Though not parties to the Customer-Data Bank contract, both the data-subjects and DataBoard may nonetheless be granted standing to sue for Data Bank's breach of the data protection terms stipulated in the contract. One or more data-subjects will be entitled to sue as third party beneficiaries of the contract between Customer and DataBank.[74] Yet it is quite impractical to expect Exporter's data-subject(s) to sue individually in the United States, given the expense and inconvenience this would entail. Because of this, DataBoard must be able to secure standing for itself in United States courts. First, it is possible that a court might recognize DataBoard as representative for a *class* of data-subjects alleging harm resulting from a Data Bank breach. Another method, by which DataBoard could virtually assure its standing to sue, would be for it to require, as a precondition to its approval of the Customer-Data Bank contract, that Customer assign its cause of action thereunder (in the event of a breach by Data Bank of the data protective provisions) to Data Bank.[75]

Assuming DataBoard has standing to bring suit, concern remains that an effective remedy be available. Such a remedy might take several forms. First, the parties should include a liquidated damages provision in their contract, stipulating a schedule of damages to apply to specific acts of breach.[76] While this situation is one in which liquidation of damages seems appropriate, such provisions are not invariably upheld by the courts.[77] Second, lacking such remedy at law, it seems likely that a court would grant DataBoard an equitable remedy, such as an injunction against the continued violation by Data Bank of its contractual commitments.

Where the parties seek to order their conduct in accordance with Exporter's law contractually, then, DataBoard may be reasonably certain of policing compliance through resort to United States courts, as well as through its own legal system. Therefore, DataBoard should conclude that, the data protection provided in the Customer-Data Bank contract, will be functionally equivalent to that the data-subjects would receive under Exporter's law.

Instead of seeking functional equivalency through purely contractual means, the parties might alternatively employ a choice-of-law clause approach. In the hypothetical situation described earlier, the presence

---

73. 17A C.J.S. *Contracts* § 518 at 940 (1963).

74. 4 A. CORBIN, CORBIN ON CONTRACTS § 775 at 8–9 (1964).

75. *See generally* 4 A. CORBIN, CORBIN ON CONTRACTS § 856 at 404–409 (1964).

76. *See generally* 5 A. CORBIN, CORBIN ON CONTRACTS §§ 1057–63 at 332–69 (1964).

77. 5 A. CORBIN, CORBIN ON CONTRACTS § 1058 at 337, 338 (1964). *See also id.* § 1063 at 362 (liquidated damages clause stricken where amount agreed to is grossly disproportionate to the actual injury).

of a choice-of-law clause in the contract would direct a United States court to apply Exporter's law to any dispute over data protection arising between Data Bank and either DataBoard or Customer. Under United States law, parties are generally free to stipulate the law governing the contract as a whole,[78] or individual clauses,[79] such as those relating to compliance by Data Bank with data protection requirements.

The major limitation on this autonomy of the parties with regard to governing law is that of public policy, the dictates of which may restrain a United States court from enforcing even the explicit wishes of the parties.[80] However, no United States policy, nor the policies of any of the states, would likely be prejudiced by the application of Exporter's privacy laws to a transnational contract to provide information services to Exporter.[81]

Given that the court will uphold the choice-of-law clause, the same questions of standing and remedy remain. Assuming jurisdiction exists,[82] DataBoard will assert that standing is conferred upon it by the

---

78. *See, e.g.*, A. EHRENZWEIG, CONFLICTS OF LAWS § 176 at 467 (1973); R. WEINTRAUB, COMMENTARY ON THE CONFLICT OF LAWS 269 (1971); Lowe, *Choice of Law Clauses in International Contracts: A Practical Approach*, 12 HARV. INT'L L.J. 1 (1971); RESTATEMENT (SECOND) OF CONFLICTS OF LAWS § 187 (1971).

79. *See, e.g.* Reese, *Depecage: A Common Phenomenon in Choice of Law*, 73 COLUM. L. REV. 58 (1973); Bayitch, *The Connecting Agreement*, 7 MIAMI L.Q. 293, 311 (1953).

80. Most courts and commentators recognize certain limitations on the autonomy of the parties to select the law governing their contract. Thus, a stipulation regarding governing law will not be upheld where there is no reasonable basis for the parties to choose the law stipulated, *see* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187(2)(a), and Comment f (1971), or where the stipulation was secured by misrepresentation, duress, or mistake. *Id.* at § 187, and Comment b.

However, the most commonly invoked limitation on the parties' autonomy is that of public policy, i.e., that a choice of law clause will not be enforced where application of the chosen law would offend a fundamental policy of the state of the otherwise applicable law, *id.* at § 187(b)(2), or of the forum. *See, e.g.*, Massengale v. Transitron Electronic Corp., 385 F.2d 83, 86 (1st Cir. 1967). The more closely the state of the chosen law is connected to the parties and to the contract, the more fundamental must be the policy of the state of the otherwise applicable law or of the forum to justify denying effect to the choice-of-law provision. RESTATEMENT, *supra*, at § 187, Comment g.

Thus, a United States court would have to find both:

(1) that the (United States) state of the otherwise applicable law had a greater interest than did Exporter in the issue of disclosure and privacy protection; and

(2) that application of Exporter's data protection law to the transaction would violate a "fundamental" policy of that United States state.

81. In general, it seems unlikely that a fundamental policy of any United States state would be violated by a contract to provide information services in a foreign state. Those whose data are being protected live in Exporter. Adaptations required under Exporter's data protection law would affect only Data Bank, who will have agreed to establish the necessary procedures and communicate periodically with data-subjects in Exporter. Even where a United States federal or state privacy statute extends protection to the data, it is doubtful that such laws will be construed as establishing maxima on data protection. In fact, the present concern is with minimum procedures, and the minima in European data protection laws are uniformly compatible with, if not more demanding than, that of United States laws.

82. A court would have subject matter jurisdiction under 28 U.S.C. § 133(a)(2), which refers to suit by an alien against a United States citizen.

data protection law of Exporter. But the matter of standing is purely procedural, to be determined according to the law of the forum state.[83] DataBoard will argue that the statutory conferral of standing is analogous to that frequently accorded federal agencies under United States law. It is likely that this argument will, in the absence of a strong public policy to the contrary,[84] convince a United States court to grant DataBoard standing, in light of the clearly expressed intent of the parties. Due to its assent to the inclusion of the choice-of-law clause, Data Bank would be estopped from contesting DataBoard's standing. Moreover, even if Data Bank were to attempt, on some procedural ground, to prevent DataBoard from suing for alleged noncompliance, any claim that functional equivalency can be established by choice-of-law clause would no longer be credible, and DataBoard would in the future be justified in refusing to license such a transaction, since resort to United States courts would not be a viable means of assuring compliance.

For these reasons, DataBoard will likely have standing to sue. Whether a remedy will be granted by a United States court however, depends in large part on the nature of the remedies provided for in Exporter's data protection law. First, foreign criminal penalties will virtually never be enforced extraterritorially by a United States court.[85] And although a schedule of civil fines is likely to be enforced, if reasonable,[86] where Exporter has established stiff fines in order to deter Data Bank's non-compliance with its data protection law, Data Bank may argue that the damages are excessive and constitute unenforceable penalties. But this argument should not prevail given the fact that the choice-of-law clause did not specifically exclude the enforcement provisions. Finally, the data protection law may provide for injunctive relief in the nature of an order that Data Bank alter its procedures or refrain from continuing the conduct complained of. The intent of the parties notwithstanding, a United States court may be reluctant to give extraterritorial effect to the equitable provisions of foreign law.

In sum, while DataBoard will likely have standing to sue under both the contractual and the choice-of-law approach, the granting of an effective remedy is more probable in the contractual situation, but only where the parties have enumerated their rights and obligations, rather than merely incorporating Exporter's entire data protection law.[87] A major advantage of the choice-of-law solution, however, is

83. *See, e.g.*, R. LEFLAR, AMERICAN CONFLICTS LAW § 122 at 293–94 (1968).

84. See discussion at note 81 *supra*.

85. A. VON MEHREN AND D. TRAUTMAN, THE LAW OF MULTISTATE PROBLEMS, 84–86, 793–97 (1965).

86. Loucks v. Standard Oil Co. of New York, 224 N.Y. 99, 102–06, 120 N.E. 198–200 (1918) (Cardozo, J.).

87. The contractual approach is deemed more effective because it is more likely to obtain

that it is significantly more convenient than the ordering of the terms of an agreement in a manner calculated to comply with the data protection. While incorporation is equally convenient, it is less desirable in that incorporated terms will be interpreted according to forum, (i.e., United States) law, which may not provide the protection Exporter's courts would in interpreting their own statute.[88]

CONCLUSION

This Note has promoted possible solutions to the problem of non-equivalency of data protection laws. It has not been argued that restrictions on the flow of personal data as a result of findings on non-equivalency are presently commonplace in number or severe in nature. It has, however, been argued that both the potential and the mechanism for damaging restrictions exist. Moreover, the negative implications of non-equivalency are far-reaching and compelling. They affect the United States, the country restricting data flows, their industries and to some degree all economies of the world. Despite the magnitude of the adverse effects of restriction, European data protection laws contain little in the way of constructive solutions to the non-equivalency problem. Stemming the data flow is a crude and ultimately counterproductive response. It is to be fervently hoped that more sophisticated measures will be forthcoming.

In the meantime, it is incumbent upon the specially constituted data protection agencies to make workable interim solutions to the equivalency problem. Parties should be allowed to maintain transborder flow of data under contracts which, by their terms or by inclusion of a choice-of-law clause, secure functional equivalency of personal data protection.

G. Michael Epperson

injunctive relief. Whether it would be more effective in obtaining money damages than the conflict-of-laws approach is unclear.

88. Incorporated terms would not be as effective as a choice-of-law clause for securing the protection of Exporter's data protection laws. Incorporated language must be interpreted by a court according to the "governing law," which, in the absence of a finding that the parties clearly intended foreign law to govern, will be *lex fori*. *See* DICEY, CONFLICT OF LAWS 587 (1949); Bayitch, *supra* note 79, at 296. A choice-of-law clause affords the parties the security that their obligations will be determined by Exporter's privacy protection laws.