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
To merit distribution, requirements for formal publication, nonetheless the program considers them incidental. Papers have not undergone the reviewing process the program.
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 Generale
des Telecommunications (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
Sc alte Family Charitable Trusts
Scott & Petzer Co.
Selden & de Quevas, Inc.
Source Telecomputing Corp.
Southern Pacific Communications Co.
Sprague Electric Co.
Standard Shares
Telecommunication 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.
oswald h. gentry

...of renewed government negotiation.
and perhaps also a search for other equivocality means outside the range
an interesting set of options which should serve to stimulate debate
while this short paper makes no specific prescription, it develops
instruments any time soon.
significant further clarification through formal intergovernmental
the OECD member countries, and it is unlikely that there will be
guidelines represented the highest level of consensus feasible among
delayed until the matter is resolved, but, as of 1980, the voluntary
officials. It is maintained that many investment decisions are being
rooms ever larger in the minds of business executives and government
management, the economic stakes are immense. The question of equivocality
processing and the use of international telecommunications in business
for the United States, as a front runner in international data
Notes
Contracts for Transnational Information Services:
Securing Functional Equivalency of Personal Data Protection
G. Michael Epperson

Reprinted from
Volume 22
Number 1
Winter 1981
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-

---


5. See discussion pp. 166–68 infra.

THE PROBLEM

Public policy of the exporting state, the parties to the contract can satisfy the law and concurrent protection provisions to be governed by the law of the contract visions in the contract, or stipulating that the sections of the contract...
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." 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.

Data Protection Laws

Personal data are created, stored and used by a variety of institutions such as insurance companies, banks and government agencies 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 1, European Committee on Legal Cooperation (C/DCJ), EUR. CONSULT. Ass. Deb. 33rd Meeting, C/DCJ 80(28) addendum 1(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)38[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 widespread perception that the data are growing beyond economic or legal control has led to the adoption of specific data protection laws in Western Europe (Europe), Canada, and the United States. 11

"Data protection" is a European term containing several elements of the American concept of "privacy." 8 Data protection does not, of course, preclude the possibility of other forms of privacy law. 10

11. See, 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 secret personal data, especially the names of individuals," in a manner similar to that used by Watergate officials. 12

12. See, 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 secret personal data, especially the names of individuals," in a manner similar to that used by Watergate officials. 13

13. Kirbi, supra note 1, at 27. As of July, 1989, Austria, Belgium, Denmark, France, Germany, and Switzerland have enacted data protection laws. Both the United States and Canada have established data protection laws in recent years. 14

14. See, 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 secret personal data, especially the names of individuals," in a manner similar to that used by Watergate officials. 15

15. Kirbi, supra note 1, at 27. As of July, 1989, Austria, Belgium, Denmark, France, Germany, and Switzerland have enacted data protection laws. Both the United States and Canada have established data protection laws in recent years. 16

16. See, 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 secret personal data, especially the names of individuals," in a manner similar to that used by Watergate officials. 17

17. See, 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 secret personal data, especially the names of individuals," in a manner similar to that used by Watergate officials. 18

18. See, 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 secret personal data, especially the names of individuals," in a manner similar to that used by Watergate officials.
however, mean that all such privacy interests will be fully protected.\textsuperscript{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."\textsuperscript{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.\textsuperscript{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\textsuperscript{22} embodied in the concept of fair record manage-

---

\textsuperscript{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; terto, 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.

\textsuperscript{20} Fishman, supra note 2, at 5.

\textsuperscript{21} Council of Europe Draft Convention, supra note 11, App. IV at 35, ¶43.

\textsuperscript{22} Fishman, supra note 2, at 11.
The increase in demand for foreign data processing and information services has removed all technical obstacles to the international transmission of data, rendering distance and geographic barriers counterproductive. Nevertheless, the adequacy of laws to address the fact that such services can often be performed through channels distant to the user is, if the potential problem of 'equivalent loss of legal effect', or because domestic entities with the desired technical capabilities are not always available. The potential for serious damage to the security and integrity of data is exacerbated when the data is transmitted outside the jurisdiction of the data controller. In such cases, the laws of the foreign data processor may not be adequate to protect the user. Even where laws are adequate, the lack of enforcement mechanisms can render them ineffective.

Equivalency of Laws

Laws of any jurisdiction may or may not be equivalent, and the data subject be notified of any unauthorized use or disclosure. It is important that any laws be adequate to protect the data subject's interests. The adequacy of laws regulating the collection, processing, and transmission of data is also critical. In addition to requiring that the data be protected, laws should require that the data be accurate and complete. Even with these laws in place, the data subject may still be exposed to unauthorized use or disclosure. Therefore, the adequacy of laws is crucial in ensuring the reliability of the data. These laws should be enforced in accordance with the laws of the data processor's jurisdiction, and the data processor should be subject to the laws of the jurisdiction where the data is located. Any subsequent use of the data must be in accordance with the laws of the jurisdiction where the data is located. The laws of the jurisdiction where the data is located should be equivalent to the laws of the jurisdiction where the data is processed. If the laws are not equivalent, the data processor should be subject to the laws of the jurisdiction where the data is located.

European data protection laws provide mandatory data protection principles in line with major areas. First, the laws establish the principles of minimization, accuracy, confidentiality, and integrity. Second, they require data controllers to inform data subjects of the purposes for which the data is to be processed, and the scope of the processing. Third, they require data controllers to provide data subjects with access to their data, and to enable them to request corrections or deletions.
the export of data to the former would tend to erode the higher or different standard of the exporting state. 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.

For several reasons, many European states believe that the standard of data protection in the United States is impermissably low. First, unlike the omnibus data protection legislation in most European states, United States law does not cover both the private and public sectors. Currently, United States federal law pertains to only federal agencies, and only twelve states have enacted fair information practices laws. Second, while European legislation extends protection to all persons within the state, the major United States legislation 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. Many European states, therefore, are likely to conclude, if they have not already done so, that the United States data protection regime is not equivalent to their own.

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

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.
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.
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. Although these restrictions vary from state to state, the standard of functional equivalency, by requiring protection by laws personal data to be transmitted abroad upon the determination.

Most of these states attempt to achieve equivalency by requiring the issuance of a license or approval by a data protection board or the commissioner. The Federal Republic, for example, allows personal data to be transmitted abroad upon the determination.
that the data-subject will not be "harmed" thereby. Section 11 of
the Swedish Data Act 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.

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 in-
definite terms that make the reach of these laws uncertain. Since
under the licensing approach, these agencies must examine and ap-
prove the operations and procedures of data banks and data processing
firms before they may utilize domestic data, 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, 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. Additionally, there is no precedent regarding
the enforcement of data protection laws in the transnational context.
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 may help to illustrate
problems of transnational data transfers. A foreign state, known as

\[\text{46. Federal Data Protection Act, [1977] BGBII 201 (West Germany); see Ganley Address, supra note 30, at 4.}\]
\[\text{48. Id., as translated in Hondius, supra note 1, at 248.}\]
\[\text{49. The efforts undertaken by the Securities and Exchange Commission to give content to the 1933 and 1934 Acts provide a possible example of what is required.}\]
\[\text{50. See Hondius, supra note 1, at 221–227.}\]
\[\text{51. Two types of licenses may be distinguished: the specific transaction may be licensed, or the specific company or databank may be licensed. The latter form presumably allows multiple transactions to occur under a single license. Decisions regarding types of licenses to be issued are a matter of agency discretion.}\]
\[\text{52. Hondius, supra note 1, at 227–235.}\]
\[\text{53. Ganley Address, supra note 30, at 5.}\]
\[\text{54. The hypothetical is simple in that it involves the movement of data from only one state into one other. Fishman presents what is perhaps a more realistic hypothetical:}\]
A proposal would facilitate the problems involved. The health records of a Swiss

United States. Since a greater quantity of foreign data is currently
that depend on computer facilities of data banks within the
access to the markets of Expoters by all companies, like Data Bank,
Data Bank, the United States stand to suffer harm.
both exporters and important states. In the hypothetical set out above,
Restrictions on the expansion of DATA Flow Restrictions

Negative Implications of Transborder Data Flow Restrictions

data subjects, then does the data protection law of exporter.
United States laws require materially less disclosure of data usage to
the contract between customer and Data Bank, but the grounds that
mission of personal data by the customer of customer by Data Bank
formation services. One of more of those services involves the trans-
name to Customer, means to cooperate with "Data
Bank, a United States data processing law requires for various in-
export of personal data only if "DataBank," a data protection board
law also contains a provision permitting the
corrective, "Customer," a effective disclosure of data usage to the data-subject. "Customer," a effective disclosure of data usage to the data-subject.
"Expoter," has a data protection law requiring periodic disclosure
166
Harvard International Law Journal / Vol. 22
processed within the United States, the economic effect of this loss of access and the attendant substantial losses of revenue would be monumental. Primarily affected would be United States-based data processing and information services, as well as those transnational corporations having lines of business supported by flows of personal data across international boundaries, such as credit card issuers. 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.

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. 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.


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 cardholder'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.
personal data promotes exporters' policy of data protection, that gain
still mean conceiving that such prohibition of transborder flows of
data would have occurred to data-subjects in exporter and the data in fact
transferred to the United States, or even that it was likely to occur,
without the United States. This does not mean, however, that harm
due to the United States is the absolute assurance that its data protection
policy will not be undermined by potential export of personal data to the United States is the absolute assurance of the
customer and exporter.

nomic motives unrelated to data protection.
these protection boards, or whether they emanated from international
the same whether they were produced in good faith by overzealous
the aforementioned economic consequences of such restrictions would be
established if there had been no restrictions were greater. In any event, the United States must ensure to reduce the
greater. In any event, the United States must ensure to reduce the
costs of doing business with them. The agency must deal on a daily basis,
domestic interests with whom the agency must deal on a daily basis,
the industry, the international pressure is legitimate and those interests it
its national industries, it is not as a domestic activity. The economic consequences, the administrative agencies, essentially, may be unpredictable
agents in order to understand this concern. Data protection
One need not as a practical matter to the data protection agencies
The possibility is no longer necessary for the establishment of such barriers.
the data-protection laws and the wide discretion left to the data
the data-protection laws. Moreover, because the burden of proof
that are aimed at a genuine economic advantage. Rather, it is the near
meets a strong economic advantage, given that the economic consequences, cultural barriers also
may lie behind a strong economic advantage. Nevertheless, the significant
protection, could establish barriers to the free flow of data
benefits demonstrate their economic motivations
balance of payments. The
neither increase national producer, and a more reversible
increase from taxes, increased national producer, and a more reversible

1697-87 (1977))
22
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. Specifically, due to the fact that the leading suppliers of data services are United States-based companies like Data Bank, 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.

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. Reflecting this concern, two major multilateral attempts have been made to harmonize national data protection legislation. Both the Draft Convention of the Council of Europe, 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.
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;
on the importance of states cannot be presumed. Accord with the rule in 5 3, Law, (1972) El. 1997, 999, laying a 58% increase. The Commission, however, has inter alia in its opinion on an important issue of the present. It is true that the Commission’s opinion, or expression, of opinion, is not necessarily binding where the facts are so complicated that the Court of Justice is not bound to declare the law of data protection.

OECD Guidelines Second edition 1989, 11.6.4 For a discussion of these guidelines, see 7.2

In the guidance, however, the Court of Justice shall have regard to the circumstances of the case, and in particular to whether the data processing is performed for the purpose of decision-making in connection with personal data protection. A Member State may also impose conditions on the exercise of the right of access to personal data, for example, an obligation by the competent authority to ensure that the data are not subject to disclosure, and where the competent authority exercises the right to access, the data shall be made available to a person for the purposes of the exercise of the right to access.

FREE FLOW AND IDENTIFICATION APPLICATION

69. Part three of the OECD Guidelines provides for the free flow of information.

6. Thus, both approaches strike a balance between the interests of the member country in order to avoid the use of personal data and the interests of the contracting party in the use of a non-contraining state for processing.

A functional equivalence of privacy legislation. A functional equivalence of data protection, but through solutions which effect, there are also a conscious that the balance is best achieved. Thus, although the free flow of information should be intended only when absolutely necessary to preserve the policy of data protection. As shown above, the free flow of information should be intended only when absolutely necessary to preserve the policy of data protection.

International Law Journal, Vol. 91 17
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. Getli & 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.
In the hypothetical situation described earlier, the presence of a breach of contract by Data Bank, such as an infringement against the continued violation by Data Bank of its contractual commitments, would result in the issuance of an order by the court for the continued violation by Data Bank of the contract. In the event of a breach by Data Bank of the contract, the customer’s right to terminate the contract is triggered. The customer may be entitled to seek damages for breach of contract. The court may order Data Bank to cease its breach of contract and to pay damages to the customer. If Data Bank is unable to perform its obligations under the contract, it may be subject to legal action for breach of contract. Generally, only the parties to a contract are deemed to have a sufficient interest to be allowed to sue for a breach thereof.
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, or individual clauses, 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. 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.

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


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 CONFLICTS 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. Transitor 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.
The contractual approach is deemed more effective because it is more likely to obtain
A major advantage of the choice-of-law solution, however, is

be selected to give extraterritorial effect to the contract's provisions
be selected to give extraterritorial effect to the contract's provisions, a United States court may
in proceedings of retention from continuing the conduct contemplated by
in proceedings of retention from continuing the conduct contemplated by

Finally, the data bank agreement and the data bank agreement and the data bank agreement provide

For these reasons, Databank would likely have standing to sue.

Moreover, even if Databank were to succeed, Databank would not be entitled to recover

Databank would also be entitled to recover the contract price for the delivery of the goods.

Databank would also be entitled to recover the contract price for the delivery of the goods.

Databank would also be entitled to recover the contract price for the delivery of the goods.

Databank would also be entitled to recover the contract price for the delivery of the goods.
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.\textsuperscript{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 trans-border 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.

\textit{G. Michael Epperson}

\textsuperscript{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 \textit{lex fori}. See Dicey, \textit{Conflict of Laws} 587 (1949); Bayitch, \textit{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.