The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow

*George B. Trubow**

I. INTRODUCTION

We are in the midst of "Europe '92," the year when the European Community (EC) is to take on new shape and substance as it seeks transformation to economic and political strategies intended to enhance its position in international trade and commerce. With respect to matters of information processing and transborder data flow,[1] the Council of Europe has prepared a draft directive concerning privacy and security regarding personal information (Privacy Directive).[2] That draft, under

* A.B., J.D., University of Michigan; Professor of Law and Director of the Center for Informatics Law, The John Marshall Law School, Chicago, Illinois where he teaches the Information Law and Policy, and Privacy Law seminars. During the Ford Administration, Professor Trubow served as general counsel to the Committee on the Right to Privacy, Executive Office of the President. He is also the Editor-in-Chief of *Privacy Law and Practice*, a three volume set published by Matthew Bender.

The author expresses his appreciation and gratitude for the invaluable assistance in preparation of this article of Timothy R. Rabel, Research Director for the Center for Informatics Law.

[1] Lisa J. Damon, Note, *Freedom of Information Versus National Sovereignty: The Need For A New Global Forum for the Resolution of Transborder Data Flow Problems*, 10 FORDHAM INT'L L.J. 262, 263, n.3 (1986-87) (defining transborder data flow also known as transnational data flow as the exchange of information from one country to another).

[2] Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277/03) 3 [hereinafter Privacy Directive]. This Privacy Directive is to give effect to the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 20 I.L.M. 317. *Id.* ¶(22), at 4.

There are eight EC nations that have ratified the Convention: Denmark, France, Federal Republic of Germany, Ireland, Luxembourg, Netherlands, Spain and the United Kingdom. Greg

consideration by the member states, is of great importance to the rest of the world since it contemplates that EC members will not exchange information with nations that do not comply with the directive's protocols.[3] The United States would be in a precarious position were our business communities to be excluded from personal information exchange with European nations because our processing of such information fails to meet the EC privacy tests.[4]

In addition to the Privacy Directive is a companion proposal regarding telecommunications.[5] That draft imposes additional privacy con-

---

Tucker, *International Legal Notes: Privacy Protection and Transborder Data Flows*, 65 AUSTRALIAN L.J. 354, 354 (1991); Rosemary Patricia Jay, *Transborder Data Flows*, NEW L.J., Feb. 22, 1991, at 241, 249. Belgium, Greece, Italy and Portugal are also member states of the EC but have not yet ratified the Convention. Tucker, *supra* at 354.

[3] The EC's law making authority is entrusted to four bodies, the Executive Commission, the Council of Ministers, the European Parliament and the Court of Justice. E.C. DELEGATION TO THE UNITED STATES, A GUIDE TO THE EUROPEAN COMMUNITY 5 (1991)[hereinafter E.C. Delegation]. The Commission consists of 17 members from the various states and is responsible for proposing Community policies and legislation to the Council of Ministers which then enacts the laws. *Id.* at 6, 7. As the communities "public forum," the European Parliament has the ability to amend proposed legislation and the Court of Justice serves as the Community's Supreme Court responsible for interpreting and ensuring proper application of the Community laws and treaties. *Id.* at 8.

There are four types of "legislation" within the Community; regulations which are completely binding and self-executing, directives which leave the states to adopt their own laws to carry out the directives' objectives, decisions which bind those named within the decision and recommendations and opinions which serve as guidance. *Id.* at 9. As the EC's "legislative" process, the Commission submits proposed legislation to the Council which the Parliament expresses an opinion on. The Council then "adopts a common position" which is presented to Parliament for approval, disapproval or amendment. Needing to act within three months or the proposal will die, the Commission through a "second reading" can pass a Parliamentary rejected proposal only with a unanimous vote. Or, if Parliament amends the proposal and the amendments are supported by the Commission, the Council can pass the proposal by a "qualified majority," otherwise a unanimous vote is needed. EMILE NOËL, WORKING TOGETHER - THE INSTITUTIONS OF THE EUROPEAN COMMUNITY 35-36 (1988) (available from Luxembourg: Office for Official Publications of the European Communities, ISBN 92-825-8526-3); E.C. DELEGATION, *supra*, at 7-8.

Although the Council is ultimately responsible for adopting the proposals, the Parliament does carry weight in that it significantly controls the EC budget and can dissolve the Commission with a two thirds vote. NOËL, *supra*, at 35 (control over EC budget); E.C. DELEGATION, *supra*, at 8 ("vote of censure" to dissolve Commission).

[4] Other nations have also expressed concerns over the European directives and the possibility of being denied the transfer of data. For example, on November 23, 1990 Hong Kong Secretary of Home affairs Peter Tsao announced plans to pass legislation that would bring Hong Kong's policy up to the standards required by the European directives. While a Working Group was created to investigate and form a policy for the country, a Law Reform Commission was to re-evaluate the country's general privacy law and to specifically address data protection. *Hong Kong Government Finally Opts for Data Protection*, NEWSWIRE ASAP(TM), Nov. 23, 1990, *available in* DIALOG, (reported by Norman Wingrove).

One Australian commentator notes that although Australia has scattered privacy protection laws, taken has a whole "it may be safely adjudged that this mishmash of laws would not be adequate in all cases." Tucker, *supra* note 2, at 355.

[5] Commission Proposal for a Council Directive Concerning the Protection of Personal Data

straints on the European telecommunications industry. Before we consider the implications of these proposals with respect to the United States we ought to review the recent history and current state of affairs in this country regarding the matter of informational privacy.

First, an explanation of how some words and phrases are used in this article will promote clarity. The general subject of informational privacy deals with the collection, maintenance, use and dissemination of personal information, which is any information describing a natural person. It is the reference and not the content of information that determines its classification as personal, for if information refers to an identifiable individual then it is personal. It does not matter whether the reference is by name or number or other identifying characteristics so long as the reference identifies a specific individual.[6]

Privacy is a characteristic of a natural person, and in informational terms considers how personal information is gathered, stored and used.[7] Confidentiality is a characteristic of information and indicates that certain information is available only to certain people under specific circumstances. Security, a characteristic of information systems, concerns the technology and procedures to assure that information in a system is not lost, altered or disclosed without proper authority. Thus, system security implements the confidentiality of information which in turn protects personal privacy.

A record or file is a collection of information and a data element is a

---

and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks, 1990 O.J. (C 277/04) 12 [hereinafter Telecommunications Directive].

[6] The Privacy Directive uses and defines "personal data" as information that can be associated with a particular individual or data subject by use of an identification number or fact. To "depersonalize" is the process in which personal data is changed to such an extent that great efforts are needed to identify the individual to which the information relates. Privacy Directive, *supra* note 2, ch. I, art. 2, ¶¶(a)-(b), at 5.

[7] In this country, corporations are not regarded as having privacy. *See, e.g.*, Browning-Ferris Indus. of Vermont, Inc. v. Kelco Disposal, Inc., 492 U.S. 257, 284 (1989) (Brennan, J., concurring) (citing United States v. Morton Salt Co., 338 U.S. 632 (1950) (corporation has no right to privacy)); Pacific Gas & Elec. Co. v. Public Utils. Comm'n of California, 475 U.S. 1, 34 (1985) (Rehnquist, J., dissenting) (corporations denied constitutional right to privacy); Noble Oil Co. v. Schaefer, 484 A.2d 729, 730 (N.J. Super. Ct. Law Div. 1984) (quoting Restatement (Second) of Torts § 6521 (1981) (corporation cannot succeed on any of four privacy torts).

However, the European countries may regard corporations as having privacy. Article 3 of the Council of Europe's Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 20 I.L.M. 317, 1981 states that the basic principle for data protection apply to "persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality." *See generally*, David C. Boyle, Note, *Proposal to Amend the United States Privacy Act to Extend its Protections to Foreign Nationals and Non-Resident Aliens*, 22 CORNELL INT'L L.J. 285 (1989) (compares Privacy Act with foreign data protection laws).

"piece" of information in the file.[8] The data subject is the one to whom personal information refers; an identifier is the data element that connects personal information with a specific data subject. The record holder is the person or entity that controls access to a collection of stored information — the Europeans use the phrase "controller of the file."[9] To access a file is to gain entry to the record, and to disclose or disseminate information is to communicate information to a third party — someone other than the data subject or record holder.

This country's development of informational privacy, which was spurred by the rapid advance of computer technology in the early 1970s, attracted the serious attention of our federal government to the matter of data privacy and security. The relative ease with which automated data allows information to be stored, retrieved and disseminated suggests the need to adequately protect that information.[10]

The first comprehensive government inquiry into the question was made by a task force appointed by then-Secretary of Health Education and Welfare, Elliott Richardson, who had become concerned about the vast amounts of personal information stored in his Department's increasingly automated files. That report, issued in 1973, presented a survey of

---

[8] The Privacy Directive also defines "personal data file" as a collection of personal data that either through automation or organization allows for efficient use of the information with and "processing" as "the recording, storage or combination of data, and their alteration, use or communication, including transmission, dissemination, retrieval, blocking and erasure." Privacy Directive, *supra* note 2, ch. I, art. 2 ¶¶ (b)-(c). Also defined in the Privacy Directive is "public sector" which includes all entities in a member state that is regulated by that state's "public law" excluding those entities that "carry on industrial or commercial activity" and entities that, although not regulated by public law, participate in "the exercise of official authority;" and the "private sector" which includes any person or entity and public sector organization that "carry[s] on an industrial or commercial activity." Privacy Directive, *supra* note 2, ch. I, art. 2, at 5.

[9] The "controller of the file" is the entity under Community or member state law that determines the use of, contents of, application to and access to the file. *Id.* ch. 1, art. 2, at 5.

[10] Marketplace is a CD-ROM which Lotus was going to introduce and clearly illustrates the potential privacy invasions that computers and data compilation presents. This computer disk which was to be commercially available contained personal information on 80 million United States Households and profiles on 120 million Americans. Data included names, addresses, ages, genders, marital statuses, household incomes, lifestyles, types of dwellings and buying propensities for certain products. None of these data subjects consented to this potential disclosure. *Data Protection, Computers, and Changing Information Practices: Hearing Before the Government Information, Justice, and Agriculture Subcomm. of the Comm. on Government Operations House of Representatives*, 101st Cong., 2d Sess. 112 (1990) [hereinafter *Data Protection Hearing*] (summary statement of Marc Rotenberg, Director, Washington Office, Computer Professionals for Social Responsibility, Professor Mary J. Culnan, School of Business Administration, Georgetown University and Dr. Ronni Rosenberg, National Science Foundation Fellow, Kennedy School of Government, Harvard University). However, due do the outcry of 30,000 of the data subjects, for at least now, Lotus has canceled distribution of the product. *Lotus Pulls Out of MarketPlace (Cancels CD-ROM Target Marketing Products because Consumers Complain it Violates Privacy Rights)*, MACWEEK, Jan. 29, 1991, *available in* DIALOG (by Carolyn Said).

federal records in HEW and examined the use of the Social Security Number (SSN). The Task Force developed a list of "fair information practices" that have become conventional wisdom regarding records management and privacy. The essence of those principals may be rephrased thus:

1. Maintain no secret information systems. (A "secret" system is one whose existence and purpose is known only to a select few.)

2. Collect only that information necessary to the lawful purpose of a record system, and when feasible collect personal information directly from the data subject.

3. Be sure that the information is relevant, accurate, timely and complete.

4. Provide the data subject with access to information about himself and a procedure by which to challenge and correct that information.

5. Use data only for the particular purpose for which it was initially collected except as permitted by the specific, informed consent of the data subject. (This is generally referred to as the "secondary use" limitation.)

6. Protect data against unauthorized disclosure, alteration or loss. (The "security" principle).[11]

Though these principles are often cited as the foundation for informational privacy, most are common sense which can apply to any record system regardless of the kind of information it contains. These principles were incorporated into the Privacy Act of 1974,[12] legislation aimed to protect personal information in federal records systems.

In addition, the federal effort in the late 1960s to help state and local government fight crime directed a great deal of money to the development of new criminal justice information systems — and that meant computers. The Crime Control Act of 1973[13] required the Department of Justice to develop guidelines to assure the "security and privacy" of criminal history information,[14] and in 1976, after protracted hearings and consultation with state and local law enforcement authorities and with public interest groups, the Department issued its regulations[15]

---

11 Secretary Advisory Comm. on Automated Personal Data Systems, U.S. Dept. of Health, Education & Welfare, Records, Computers and the Rights of Citizens (1973) (OSHEW Publication No. (D)73-94).

12 Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified at 5 U.S.C. § 552a).

13 Crime Control Act of 1973, Pub. L. No. 93-83, 87 Stat. 197 (amending Title I of the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. §§ 3701 - 3795).

14 *Id.* § 523(b) (current version at 42 U.S.C. § 3789(g)(b) (1988)).

15 41 Fed. Reg. 11,715 (March 19, 1976) (codified as amended 28 C.F.R. §§ 20.1 to 20.38 (1991)).

which reflect the general thrust of the fair information practices.[16]

During the years of the Ford presidency (1974-76) the Domestic Council Committee on the Right to Privacy also studied the information practices of federal agencies and supported passage of the Privacy Act. The foregoing principles of fair information practices were the Committee's benchmark against which procedures to protect informational privacy were evaluated.[17]

The EC Privacy Directive discussed herein will be seen to contain little if anything that is new to America in terms of protocol for personal information.[18] Many of the concepts are reflected in other federal legislation such as the Right to Financial Privacy Act,[19] the Fair Credit Reporting Act,[20] and the Family Educational Right to Privacy Act.[21] In those Acts, the right of access and review by the data subject,[22] requirements for data accuracy[23] and limitations on access by third parties are common elements.[24]

---

16 28 C.F.R. § 20.33 (only certain groups are to receive criminal history information); 28 C.F.R. § 20.34(a) (data subject is to have access to his records); 28 C.F.R. § 20.34(b) (data subject can challenge the accuracy and completeness of the records); 28 C.F.R. § 20.37 (agency contributing data must assure the completeness and accuracy of its records.)

17 The Privacy Act of 1974 also established the Privacy Protection Commission which was to conduct a study of various private and governmental data banks, and computer and information processing systems ultimately producing standards to insure the protection of "personal information." Pub. L. No. 93-579, § 5, 88 Stat. 1905. The Commission published its report entitled THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977), and pursuant to Pub. L. 93-579, § 5(g), discontinued operation on September 30, 1977.

18 For example, a common theme running through all U.S. data protection laws is "[a]ny information obtained for one purpose should not be used for another purpose without the consent of the person." *Data Protection Hearing, supra* note 10, at 111 (summary statement of Marc Rotenberg, Director, Washington Office, Computer Professionals for Social Responsibility, Professor Mary J. Culnan, School of Business Administration, Georgetown University and Dr. Ronni Rosenberg, National Science Foundation Fellow, Kennedy School of Government, Harvard University).

19 Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1988).

20 Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1988) (amended Consumer Protection Act, Pub. L. No. 90-321, 82 Stat. 146).

21 Family Educational Right to Privacy Act, 20 U.S.C. § 1232g (1988) (was part of the Educational Amendments of 1974).

22 12 U.S.C. § 3404(c) (can access the records of disclosures); 15 U.S.C. § 1681g (data subject has access right); 15 U.S.C. § 1681i (ability to challenge data accuracy); 20 U.S.C. § 1232(a)(1)(A) (denial of federal funds for refusing student access to his records).

23 15 U.S.C. § 1681e (must "assure maximum possible accuracy"); 20 U.S.C. § 1232g(a)(1)(C)(2) (allow challenges to accuracy).

24 12 U.S.C. § 3402 (restricts government access); 12 U.S.C. § 3403 (release of records prohibited); 15 U.S.C. 1681b (list of only instances of permitted record disclosure); 20 U.S.C. § § 1232g(b)(1), (2) (no federal funds for schools that release records).

II. Summary of the European Draft Privacy Directive[25]

A. General Overview

The treaty which governs the European Economic Community promotes economic and social growth while protecting individual fundamental rights that are found in each member state's constitution.[26] The Privacy Directive seeks to balance the needs of its members to collect and exchange data against the protection of "fundamental rights" that may be infringed by the processing of personal data.[27] The right of privacy is considered a fundamental right.[28]

The Privacy Directive was developed with an awareness that technology has increased to the point that transfer of personal data across national borders has become essential and almost effortless.[29] Noting that because the several Community members' differing approaches to the protection of personal data might impede economic ventures between member states,[30] the Directive seeks harmonization of privacy laws to allow for a proper flow of personal data.[31] While the minimum protections identified in the Privacy Directive are to be recognized by all members, each may provide additional protection to personal data if it so chooses.[32] To prevent a conflict of laws which could develop when files pertaining to the same data subject are maintained in more than one member state, the laws of a jurisdiction control records within that jurisdiction but do not have extraterritorial effect.[33]

The data subject has the right to receive notice[34] of and review[35] records pertaining to him. Generally, personal information can be processed only with the consent of the data subject.[36]

Each member state is expected to have an agency to oversee implementation of the Privacy Directive, and an EC "Working Party on the Protection of Personal Data"[37] would help in harmonization.[38] With

---

25 Privacy Directive, *supra* note 2.
26 *Id.* ¶(1), at 3.
27 *Id.* ¶(2), at 3.
28 *Id.* ¶(7), at 3.
29 *Id.* ¶(4), at 3.
30 *Id.* ¶(5), at 3.
31 *Id.* ¶(6), at 3.
32 *Id.* ¶(8), at 3.
33 *Id.* ¶(10), at 4 (each portion of a file within a state is to be treated as a unique file).
34 *Id.* ¶(13), at 4.
35 *Id.* ¶(15), at 4.
36 *Id.* ¶(16), at 4. Because the Privacy Directive allows for the Community's competing right to freedom of information, the Directive allows member states to exclude the media in an attempt to reach a balance between these interests. *Id.* ¶(18), at 4.
37 *Id.* ¶(23), at 4-5.

January 1, 1993, as the target date, each member state must enact its own laws to conform to the Privacy Directives objectives.[39]

B. Summary of Important Privacy Directive Provisions

Article 3 defines the scope of the Privacy Directive which applies to all files in the private and public sector except records held by an individual and used only for private and personal reasons, the records of public sector entities whose conduct is not subject to Community law, and the records of voluntary members to non-profit organizations.[40] The Privacy Directive's broad scope is intended to cover the main bulk of records maintained within the EC. Article 4 provides that a member state's law controls records located within its territory or anyone who uses terminals within the member's territory to access records.[41]

Article 5 allows public sector entities to maintain only those records necessary to carry out the purpose for which the entity was created. Secondary use of personal information is allowed only if the data subject consents, the use is pursuant to law, will not hinder the data subject's legitimate interests, is required to protect public safety, or to preserve third party rights.[42]

Similarly, Article 8 covers the private sector, and absent consent, allows private entities to create and maintain personal data records in only three instances: if needed to fulfill contractual or quasi-contractual duties; the data comes from public sources; or, the record holder's legitimate interest outweighs the data subject's privacy.[43]

Reflecting the fist fundamental principle of fair information practice, Article 9 requires the private sector record holder to notify the data subject of the existence, function, content and use of the record before information is disclosed to others. If the data subject objects, the unauthorized use must be stopped.[44] At the time information is collected directly from the data subject, unless overburdensome to the entity, Article 13 requires the requesting entity to give similar notice and inform the

---

38 *Id.* ¶(24), at 5.

39 *Id.* ch. X, art. 31, at 12.

40 *Id.* ch. I, at 5-6.

41 *Id.* at 6.

42 *Id.* ch. II, at 6. Article 6 allows Members to determine when the communication of personal data from public sector files is needed to fulfill the public entities responsibilities or the instances when a private sector requestor's legitimate interest outweighs the data subject's interest. The data subject, however, must be given notice of such communication. *Id.* at 6.

43 *Id.* ch. III, at 7.

44 *Id.* at 7. As an exception to Article 9 notice, under Article 10 a member state's supervisory authority can determine when such notice would be impossible, overburdensome or when the controller's or third party's interest outweighs the data subjects's privacy. *Id.*

data subject of his/her data protection rights.[45]

Because disclosure is generally prohibited without the data subject's express consent, Article 12 defines valid consent. The individual must be told the function, contents, use and intended recipients of the information and the name and address of the record holder,[46] which constitutes "informed consent."[47]

Article 16 relates to the quality of data maintained and illustrates the second, third and fourth principles of fair information practice. Personal data must be fairly and lawfully obtained; maintained and used in "a way compatible" to the record's purpose; be complete, relevant, accurate, and timely; and, identifiable to the data subject for only the time necessary to fulfill the reasons for which it is maintained.[48]

The security principle is reflected in Article 24 which prohibits a member state from transferring data to a country considered to have insufficient data protection laws, and requires the member state to report such refusal so that the Commission can consider the status of the requestor.[49] This provision threatens to exclude from the exchange of personal data with the EC the U.S. and any others whose privacy protocols are deemed insufficient.

For oversight, Article 26 mandates that each member state create an independent agency to monitor compliance with the Privacy Directive.[50] Article 27 establishes a Working Party consisting of representatives from each member state to oversee Community law as it relates to the Privacy Directive.[51]

---

45 *Id.* ch. IV, at 8 (notice includes the record's function, the consequences of failing to reply, the information recipients, his rights of access and to correct personal data and the record holder's name and address). Additionally, Article 14 allows the data subject to challenge personal data use; not to have administrative decisions made exclusively from "automatic processing of personal data defining his profile or personality;" to know if a file exists, and if so, its contents, who holds the file and where the file is located. Furthermore, the data subject can correct or delete information, prevent its use and has a judicial remedy for Article 14 violations. *Id.*

46 *Id.* at 7-8.

47 The requirements for valid consent appear in Article 12 under the sub-heading "Informed consent." Privacy Directive, *supra* note 2, ch. IV, art. 12, at 7.

48 *Id.* ch. V, at 9. Article 18 fulfills the sixth principle of fair information use by mandating controllers of files to adopt security precautions necessary to prevent unauthorized access to or change of personal data files. *Id.*

49 *Id.* ch. VIII, at 10. Article 25 allows member states to transfer data to another country that does not have sufficient data protection laws if the receiving country adequately assures protection for the data. *Id.* at 10.

50 *Id.* ch. IX, at 11.

51 *Id.* at 11.

III. The Telecommunications Directive

Whereas the Privacy Directive deals generally with threats to privacy resulting from the processing of personal data, an additional Commission proposal relates to the special privacy threats from the telecommunications industry's use of personal information.[52] The Telecommunications Directive aims to permit growth of the telecommunications industry while protecting privacy.[53] Although the thrust of the Telecommunications Directive is to limit the collection and use of personal data to that which is necessary to provide the telecommunication service itself,[54] it does not stand alone but must be applied in conjunction with the Privacy Directive.[55]

Under the Telecommunications Directive, personal data can be maintained and used only to provide the service[56] but not to create "electronic profiles" of the service subscriber.[57] Once collected, the information can be retained only for as long as needed to provide and charge for the service and resolve billing and service disputes between the provider and the subscriber.[58]

As in the Privacy Directive, a subscriber has the right to know that personal data files exist and to review and correct the record.[59] Without the subscriber's prior consent, personal information cannot be disclosed to anyone, including service supplier personnel who have no responsibility to help provide the subscribed service.[60] Additionally, the security principle is observed by requiring the record holder/service provider to reasonably ensure the security of such data and services.[61]

The Telecommunications Directive also addresses specific types of data and services. For example, it identifies what data can be maintained[62] and what procedures the provider of such services as "Caller-ID"[63] and "call forwarding"[64] must follow, and it describes how unsolic-

---

52 Telecommunications Directive, *supra* note 5.
53 *Id.* ¶(12), at 13.
54 *Id.* ¶(14), at 13.
55 *Id.* art. 2, at 14.
56 *Id.* art. 4, ¶(1), at 14.
57 *Id.* art. 4, ¶(2), at 14.
58 *Id.* art. 5, at 14.
59 *Id.* art. 6, at 14-15.
60 *Id.* art. 7, at 15.
61 *Id.* art. 8, at 15.
62 *Id.* arts. 9, 10, 11, at 15.
63 *Id.* arts. 12, 13, at 15-16. "Caller-ID" is not specifically mentioned in the Telecommunications Directive which uses "calling line identification." However, the service described is similar to the "Caller-ID" service provided in the U.S.. In which case, it is the ability of the receiver of a call to see the number of the person calling. The Telecommunications Directive also discusses the need to provide "blocking," the ability to prevent disclosure of the caller's telephone number. *Id.*

ited sales calls can be curtailed.[65]

IV. The Directive and U.S. Informational Privacy Compared

A. The Public Sector

Unlike the U.S. Privacy Act which pertains only to federal agencies,[66] the Privacy Directive governs public and private sector information processing,[67] but it does exclude files maintained privately for personal reasons, such as one's own address book or telephone list.[68]

It is arguable that the Privacy Act itself largely would satisfy the Directive,[69] especially in light of the Computer Matching Privacy Act.[70] There is not much policy difference between the European and American views on governmental information processing with respect to privacy constraints insofar as the Directives and the Privacy Act are concerned.

Most American states do not have privacy legislation, however, to govern their own information processing protocols, so this aspect of public sector regulation is woefully inadequate. Some of the EC member states are not in adequate compliance with either the Privacy Directive

---

64 *Id.* art. 14, at 16. Also an American service, "Call forwarding" is not specifically used in the Telecommunications Directive either, but what is discussed is the transferring of calls to a third party. *Id.*

65 *Id.* art. 17, at 16.

66 Under the Privacy Act, the definition of agency is found in section 552a(a)(1) which cross references the definition of agency found in the Freedom of Information Act, 5 U.S.C. 552(f). Agency "includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." 5 U.S.C. 552(f) (1988).

67 For Directive application to public and private sectors, *see supra* notes 40, 42, 43 and accompanying text.

68 Privacy Directive, *supra* note 2, ch. 1, art. 3, ¶(2)(a), at 5.

69 For example, § 552a (b) requires the data subject's written permission before the agency can disclose any information about the individual. The Act, however, provides for several exceptions to the written consent requirement. *Id.* § 552a(b)(1)-(12). Section 552a(d) allows the data subject access to and amendment of his records. Section 552a(e) requires the agency to maintain only those records to accomplish the agency's purpose and when possible, collect the information from the data subject. 5 U.S.C. § 552a (1988).

70 Computer Matching Privacy Act, Pub. L. No. 100-503, 102 Stat. 2507 (1988), *as amended by*, Pub. L. No. 101-56, 103 Stat. 149 (1989) (codified within paragraphs of 5 U.S.C. § 552a). As a result of this Act, an agency can disclose records that will be used in a computer matching program only pursuant to a written agreement between the agency and the receiving agency. 5 U.S.C. § 552a(o). The Act specifies the agreement should contain provisions that provide notice, verify accuracy, ensure security and ensure retention for only as long as necessary. *Id.* Additionally, before an agency can make a major decision using the records via a matching program, the Act requires the agency to independently verify the information and give the data subject the opportunity to contest the findings. *Id.* § 552a(p).

or the Telecommunications Directive and will have to correct that, though by and large the European nations have far more informational privacy regulation than we do.[71]

B. The Secondary Use Limitation

A major sticking point, however, concerns the prohibition on the secondary use of information, together with a requirement that information be obtained directly from the data subject. The strict application of these principles can place an unwelcome burden on data subjects who may have to constantly re-supply information that is already on file with a government agency or be pestered by requests for harmless secondary uses. It would be sensible for information to be shared by agencies having a proper interest in the same data and for benign secondary uses to be permitted.

The Privacy Act sought to alleviate this problem for federal agencies through the "routine use" exception to secondary use limitations:[72] if a purpose other than that for which the information was initially collected is a matter of routine business to the record holder then it may disclose the information.[73] There is little satisfactory guidance as to what is a "routine use," however, and the matter generally is left to the discretion of each record holder.[74] As a result, U.S. government agencies designated such broad areas of routine use as to gobble up the secondary use limitation.[75] In terms of the Privacy Act, the limitation is practically useless.

There is legislation currently pending in Congress that would create a federal data protection board and address some of the privacy deficiencies of the Privacy Act; but that proposal falls short when measured against the requirements of the European Privacy Directive. Secondary uses are not defined nor is the practice prohibited; the oversight mecha-

---

71 Information Technology Law Group EUROPE, BULLETIN (Autumn 1991) (European Data Protection Survey Insert) As of February 91, 50% of the surveyed countries had data protection laws and other countries had laws pending.

72 5 U.S.C. § 552a(b)(3) ("routine use" exception to non-disclosure of agency record).

73 As defined by the Act, routine use is "with respect to disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7).

74 The Privacy Act requires only that the agency publish its routine uses in the Federal Register. 5 U.S.C. § 552a(e)(4)(D), (e)(11).

75 137 Cong. Rec. H3449-50 (1991) (Mr. Wise's criticism of "routine use"). *See generally*, The Privacy Protection Study Commission, Personal Privacy in an Information Society 516-21 (1977) (discussing extensive agency reliance on routine use to exchange information); Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right of Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957 (1991).

nism is limited mainly to "jaw boning" and has little enforcement power.[76] It is likely that the U.S. might still be excluded from trans border data flow even if this proposal passes.

C. Private Sector Regulation

The private sector in the United States is largely unregulated in terms of information management. The Fair Credit Reporting Act (FCRA) does provide some rights of access by the data subject to credit records maintained about him or her,[77] but that law falls far short of the constraints of the Privacy Directive.[78] Not only is the secondary use limitation insufficiently satisfied by the FCRA, but the private sector would be permitted by the Privacy Directive to maintain personal records *only* with the consent of the data subject except if (1) necessary to fulfill the record holder's contractual duties, (2) the information comes from a public source, or (3) the record holder's legitimate interest is superior to the privacy interest of the data subject.[79] The FCRA does not place such restrictions on the maintenance of credit records.

The situation in this country regarding incursions on informational privacy will increase markedly with the constant movement toward the point-of-sale electronic funds transfer system. This technology poses the possibility of a minute-by-minute description of a consumer's behavior in fine-grained detail. Such a collection of information, and the wide range

---

76 One measure of H.R. 685, 102nd Cong., 1st Sess. (1991) which was introduced January 29, 1991 by its sponsor Representative Robert Wise, would create a "Data Protection Board." Although the Board is to develop guidelines and models for acceptable routine uses, the act does not require the Board to permit secondary uses only with the informed consent of the data subject. The Board also is mainly an advisory and investigative body whose only real enforcement power is the ability to hold hearings and issue subpoenas requiring attendance or production of files. The Board would not have the ability to sanction individuals, instead, it is to report Privacy Act violations to other offices. H.R. 685, 102nd Cong., 1st Sess. (1991).

Representative Wise also chaired a hearing to address potential consequences in international trade for the U.S. and its businesses if the United States fails to adequately protect privacy from the increased compilations of personal information in public and private sectors. The hearing discussed the creation of a Privacy Protection Commission and a possible Data Protection Act. *See generally*, *Data Protection Hearing*, *supra* note 10, at 2 (opening statement of Robert E. Wise, Jr., chairman of the subcommittee) (the focus of the hearing was Computer Privacy and H.R. 3669 and the Data Protection Act of 1990).

77 15 U.S.C. § 1681g (1988) (disclosure to consumer of information and the source and recipients of the information); *see also*, *supra* notes 22, 23, 24, and accompanying text for Fair Credit Reporting Act rights.

78 Although the Fair Credit Reporting Act provides a list of the only permitted consumer report disclosures, it does not adequately address secondary use. One permitted disclosure is for a "legitimate business need." 15 U.S.C. § 1681b(3)(E) (1988). However, this section does not necessitate balancing the business need against the possible invasion of privacy.

79 *See*, *supra* text accompanying note 43 for when the Privacy Directive allows disclosure in private sector without consent.

of uses made of it by private sector enterprise, are well beyond the most minimal restrictions of the Privacy Directive.[80]

D. Telecommunications and Privacy

There are some U.S. telecommunications regulations regarding privacy and personal information, but not much.[81] Subsequent to the break-up of our Bell System,[82] a variety of entrepreneurs have begun to provide telecommunications services which vary from state to state and are virtually unregulated with respect to customer information practices. "Caller I.D.," for instance, has been approved in some states without any opportunity for the caller to block disclosure of his phone number;[83] other states have required this option.[84] Additionally, the regional Bell companies which replaced the national Bell System have recently been permitted to develop and market data bases so they themselves can supply information about customers;[85] previously, message-switching was the principal function of the "Baby Bells."[86] It is yet to be seen what new dimensions of telephone customer information profiles will be developed and exchanged, but the very idea of doing so is counter to the European Telecommunications Directive.

---

[80] For a discussion of Lotus' Marketplace, a CD-ROM, see *supra* note 10.

[81] Computer Matching Privacy Act, Pub. L. No. 100-503, 102 Stat. 2507 (1988), *as amended* by, Pub. L. No. 101-56, 103 Stat. 149 (1989) (codified within paragraphs of 5 U.S.C. § 552a); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1988) (prohibits disclosure of personal information in video rental records); Electronic Communications and Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.) (regulates interception of wire, oral and electronic communications); Cable Communications Policy Act of 1984 § 631, Pub. L. No. 98-549, 98 Stat. 2779 (codified at 47 U.S.C. § 551) (regulates disclosure of cable television subscriber records); Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (regulates telemarketing and telephone solicitation).

[82] United States v. Western Elec. Co., 569 F. Supp. 1057 (D.D.C. 1983), *aff'd*, New York State Dep't. of Pub. Serv. v. United States, 464 U.S. 1013 (1983) (court approval of AT&T's reorganizational plan).

[83] 1992 Ind. Legis. Serv. P.L. 55-1992, § 2 (West) (to be codified at Ind. Code § 8-1-2.9) (no blocking except for law enforcement and commission certified crisis agencies).

[84] Cal. Pub. Util. Code § 2893 (West 1991) ("individual" blocking with no charge); N.D. Cent. Code § 49-21-01.6 (1991) ("per call" blocking at no charge).

[85] United States v. Western Elec. Co., 767 F. Supp. 308, 332 (D.D.C. 1991), *stay vacated*, 1991 WL 238308 (D.C. Cir. 1991) (although enforcement of the decision was delayed, court removed restriction of consent decree thus allowing Regional Companies into information service market).

Presently, S. 2112, 102nd Cong., 1st Sess. (1991) and H.R. 3515, 102nd Cong., 1st Sess. (1991) are two pending bills which would amend the Communications Act of 1934 and limit the ability of regional companies to provide information services.

[86] Western Elec., 767 F. Supp. at 310, n.4 (consent decree did not allow Regional Operating companies to furnish "information services"). The court also noted, however, that the Regional Operating companies were providing other services including: cellular and cable television services abroad. *Id.* at 318-19.

V. Recent Developments: Weakening the Directive?

At the time this article was about to be submitted for publication the European Parliament (EP), had approved the foregoing Directives but proposed some amendments which would have the effect of diluting the privacy protection proposals.[87] The EP is mostly an advisory body in the EC legislative process. The Council could refuse or modify the amendments and send the Directives to the member states for action.[88] It is probably safe to predict that, given (1) the commitment of the Council to privacy protection as evidenced over the years in which the Directives were fashioned, and (2) the EP's amendments were the result of reportedly massive lobbying by U.S. multinational corporations, the Council will not retreat significantly from its privacy stance.[89] Nevertheless, the overwhelming EP vote in favor of the amendments might indicate some popular support for them back home and they cannot be discounted.[90]

The amendments to the Telecommunications Directive do not appear to be significant in privacy terms and will not be discussed here. The Privacy Directive amendments are another matter, however, and deserve attention. Though some of the amendments seem to strengthen the scope and quality of privacy protection, others have the reverse effect.

A. Removing Distinctions Between Public and Private Bodies

The Privacy Directive had treated separately the public and private sectors, setting out somewhat different standards for each.[91] The amendments would eliminate the differences and treat both sectors alike. As a result, there is sharper focus on the processing of the data without regard to who is doing it.[92] Such amendments do not appear to be objectionable

---

87 *EC Parliament Approves Data Privacy Legislation*, Reuters Library Report, March 11, 1992, *available on* LEXIS, Europe Library, ALLNWS File (EP approved the legislation but several amendments were proposed).

88 For a discussion of the EC legislative process, see *supra* note 3.

89 The Commission has indicated most of the suggested amendments will not be accepted. *Data Protection: EC Proposal on Data Protection Likely to Undergo Modifications*, Millin Publications, Inc., EuroWatch, March 20, 1992, *available in*, LEXIS, Europe Library, ALLNWS File (Commission has not adopted a "common position" as of March 20, 1992).

90 Although the EP unanimously approved of the proposals, criticism from the banks, credit companies and other industries may have influenced the EP's adoption of the amendments. *Id.*

91 Privacy Directive, *supra* note 2, ch. II at 6 (public sector processing); Privacy Directive, *supra* note 2, ch. III, at 7 (private sector processing). For a discussion of these chapters, see *supra* notes 40, 42, 43 and accompanying text.

92 Report of the Committee on Legal Affairs and Citizen's Rights on the Proposal from the Commission to the Council for a Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data (COM(90) 0314 - C3-0323/90 - SYN 287), on the Proposal From the Commission to the Council for a Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated

from a privacy perspective and in fact may be a more straightforward approach to information management.

B. Excluding the "Press" From Coverage.

One amendment excludes from privacy regulation the "press, photography, cinematography, radio or television" ventures which inform the public.[93] Although at first blush it seems that this might be consistent with U.S. First Amendment principles, consider that in this country the press generally has no greater rights than any member of the public. Accordingly, there is no reason, from the U.S. perspective, to give a special pass to the press. Indeed, there is danger that with exemption the news media could become a gaping hole through which personal data could be funneled without restriction. If there is no regulation of the press then presumably it could obtain, process and disseminate personal information as it chooses. Once personal information has been made public by the media, then arguably the privacy interests have been eliminated and the information itself is in the public domain and outside the scope of the Privacy Directive.[94] Such a result ought not be the case in Europe or in the United States, and the amendments deserve careful scrutiny in this regard.

C. Secondary Usage Expanded

Though the general prohibition in Article 8 on secondary use is maintained, the list of permissible disclosures is expanded considerably to include instances where a third party's justified interest has been "convincingly" proven, the information was obtained from public sources, disclosure will protect public or third party interests or the information

---

Services Digital Network (ISDN) and Public Digital Mobile Networks COM(90) 0314 - C3-0324/90 - SYN 288), on the Proposal from the Commission to the Council for a Decision in the Field of Information Security COM(90) 0314 - C3-0325/90) (Jan. 15, 1992) (Rapporteur Geoffrey Hoon) [hereinafter Hoon Report].

For example, Amendments 27, 28 and 29 delete Chapter II of the Privacy Directive which specifically addresses the public sector. *Id.* at 12-14. Other amendments change references to "private sector files" to "data" generally. *Id.*, amend. 4, at 5. Amendment 21 changes the scope of the Privacy Directive which applied to files in the "public and private sectors," to "personal data held by all authorities and organizations constituted under public law, and by other natural and legal persons. . . ."*Id.* at 10.

93 *Id.* amend. 22, at 10-11.

94 An invasion of privacy cannot occur by publishing facts that are already public, they are no longer private. *See, e.g.*, Reuber v. Food Chem. News, Inc., 925 F.2d 703, 719 (4th Cir. 1991) (facts in public domain not private) (citing Florida Star v. B.J.F., 491 U.S. 524, 535 (1989); Heath v. Playboy Enters., Inc., 732 F. Supp. 1145, 1149 (S.D. Fla. 1990) (publishing facts already published in other magazine not invasion of privacy).

consists of names and addresses for direct marketing.[95] Such a list creates endless uncertainty regarding what disclosures might be appropriate, is subject to the same kinds of objection as the "routine use" exception of the Privacy Act and has the potential of emasculating informational privacy safeguards.

Also, another amendment significantly weakens Article 9 which says that upon the data subject's objection, an unauthorized use must be stopped.[96] The amendment would bar only unauthorized *disclosure*[97] which presumably would allow the record holder itself to make offensive secondary use of personal data in its possession.

D. Discretion in Transfers to Nonconforming Countries

Finally, an amendment to Article 24 would allow member states the discretion to prohibit the transfer of certain categories of data to nonconforming countries, replacing the total prohibition on transfer and notice to the Commission which the draft Directive now requires.[98] Such discretion would allow transfer of information to "data haven" nations where, free of privacy regulation, the data could be processed and disclosed to anyone for any purpose. Such a provision could result in a complete bypass of the Privacy Directive regulation.

Though there are EP amendments other than those mentioned above that may or may not pass privacy muster, these particular ones are so offensive to privacy interests and fair information practices as to be likely candidates for Council rejection without much debate. The other amendments do not seem to pose serious privacy threats.

VI. Conclusion

It will be ironic, indeed, if Europe's insistence on the protection of human rights causes this country to pay some real attention to informational privacy in both the public and private sectors. Usually we are in the position of lecturing other nations about the sanctity of fundamental human rights; in the informational privacy dimension we are the ones who must be lectured.

Of course the EC member states have yet to consider fully the Privacy and the Telecommunications Directives and the EP amendments must yet be confronted; it is not likely that these matters will be resolved by January, 1993. But it is also clear that though the EC may step back

95 Hoon Report, *supra* note 92, amend. 32, at 16.
96 Privacy Directive, *supra* note 2, ch. III, at 7.
97 Hoon Report, *supra* note 92, amend. 35, at 17.
98 *Id.* amend. 78, at 31.

somewhat from the requirements of the Directives, the United States is already out of step with much of Europe's informational privacy constraints.[99] At a minimum, the secondary use limitation cannot continue to be short-circuited by American government and completely ignored by our private sector. A protocol between "all" or "nothing" regarding secondary use must be devised if we expect to participate in international transborder data flow of personal information. Given the reality of the "information society" worldwide, this is an arena in which we must play the game and we have to recognize that others may make the rules.

[99] *See generally* David H. Flaherty, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989).