Pace International Law Review

Volume 9
Issue 1 *Summer 1997*

Article 4

June 1997

A Hitchhiker's Guide to Transborder Data Exchanges between EU Member States and the United States under the European Union Directive on the Protection of Personal Information

Patricia Mell

A HITCHHIKER'S GUIDE TO TRANS-BORDER DATA EXCHANGES BETWEEN EU MEMBER STATES AND THE UNITED STATES UNDER THE EUROPEAN UNION DIRECTIVE ON THE PROTECTION OF PERSONAL INFORMATION

By Patricia Mell*

"Information is the lifeblood that sustains political, social, and business decisions."[1]

TABLE OF CONTENTS

* Professor of Law, Detroit College of Law at Michigan State University; A.B. with Honors, Wellesley College, 1975; J.D. Case Western Reserve University Law School, 1978.

[1] Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 987 (1983).

I. INTRODUCTION

In today's world, the borders of the individual's native land no longer limits the individual's experiences or acts as a barrier to the dissemination of personal information. Multinational companies exchange personnel information across national borders to its subsidiaries.[2] Data marketing concerns seek information about potential customers for a myriad of businesses around the world.[3] Credit card systems are international in scope and maintain records concerning millions of credit card holders.[4] Governments have come to rely upon shared information as a basis of efficient decision making.[5] The international exchange of information concerning criminal activity facilitates safety and security worldwide.[6]

---

[2] *See* ERNST LOUWERS AND CORIEN E.J. PRINS, ET. AL, INTERNATIONAL COMPUTER LAW 17-15 (1995). Some personnel data bases hold 140 different pieces of information on each employee. *See* Donald Harris, *A Matter of Privacy: Managing Personal Data in Company Computers*, PERSONNEL, Feb. 1987, at 38.

[3] In 1990, the data marketing industry was estimated to generate 3 billion dollars a year. *See* Jill Smolowe, *Read This!!!!!!!!*, TIME, Nov. 26, 1990, at 62, 66. It was also reported that there were 10,000 data marketing lists commercially available. *See id.*

[4] In the first ten years of its existence, Visa (then known as BankAmericard) grew from having 1 million cardholders worldwide to 30 million card holders. *See* JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE 230 (1974). In 1971, American Express had 3.5 million members. *See id.* By 1990, its membership had grown to include a worldwide membership of 30 million. *See* JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE 198 (1991).

[5] *See* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 4 (1977). In 1976, the federal government held 3.9 billion files on private citizens. *See* 45 U.S.L.W. 2161 (Sept. 28, 1976). In 1989, the federal government held an average of 18 files on each individual while state government held an average of 15 files on each resident. *See* ROBERT E. SMITH, PRIVACY: HOW TO PROTECT WHAT'S LEFT OF IT 82 (1980). *See also* CARROLL, THE PROBLEM OF TRANSNATIONAL DATA FLOWS IN POLICY ISSUES IN DATA PROTECTION OF PRIVACY 201 (Informatics Studies No. 10, 1976).

[6] The best known internal criminal information repository is the International Criminal Police Organization (Interpol). *See* CARROLL, *supra* note 4, at 99-

The merging of computer technology and telecommunications systems allowed the world community to capitalize on information's value as a core resource.[7] This merger has facilitated the replacement of the industrial economy with one based on the exchange and manipulation of information.[8] The demand for better and more complete information by multinational concerns and their cooperation with one another has led to an "internationalization" of data exchanges.[9] At the core of these transactions is the collection, storage, manipulation and dissemination of personal information about individuals.[10] Much of this personal information flows between bureaucracies without the individual's awareness. This phenomenon was described as follows.

> The private and public bureaucracies are the repositories of the planning power in the economy. . . . The two bureaucracies coordinate with each other through a blizzard of forms and reports, and through the revolving door between industry and government. Expertise is exchanged through the purchase of R & D, consulting, and management, and extracted by regulatory commissions, requested by congressional committees, offered gratuitously through lobbying, or simply transferred as a result of people changing jobs.[11]

The cooperation between these bureaucracies allows different countries and companies to effect electronic forays into for-

---

100. Its files contain information concerning the identities, aliases, associates and methods of international criminals. *See id.* Other criminal information systems include the National Crime Information Center (NCIC) in the United States and the Police National Computer (PNC) in the United Kingdom. *See id.*

[7] *See* Anthony Oettinger, *Information Resources: Knowledge and Power in the 21st Century*, SCIENCE, July 4, 1980, at 191. *See generally,* Arthur Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1091 (1969). The number of computers worldwide grew from 4 million to 173 million in a thirteen year period from 1981 to 1994. *See Global Shift: More TV's Fewer Frogs*, DET. FREE PRESS, May 22, 1995, at 4A.

[8] According to EC research, about 80% of the European employees will be employed in jobs based in some form of information technology by the year 2000. *See* INFORMATION TECHNOLOGY LAW GROUP/EUROPE, EUROPEAN COMPUTER LAW 1-3 (1995)[hereinafter EUROPEAN COMPUTER LAW].

[9] *See* LOUWERS, *supra* note 2, at 14-17, (1995).

[10] *See id.*

[11] Marc U. Porat, The Information Economy 41-42 (1976)(unpublished Ph.D. dissertation, Stanford University) (on file with author).

eign turf with a minimum of time and effort.[12] The fluidity of these information exchanges threatens traditional notions of sovereignty.[13] It has created the need for a universal approach to the protection of the individual's informational privacy.[14]

In October 1995, the European Union (E.U.) passed a Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.[15] The Directive establishes the duties of maintaining the security, accuracy and completeness of information assembled by data collectors.[16] It also gives the data subject a considerable amount of power with respect to the treatment of data collected concerning him.[17]

While the Directive requires the creation of laws consistent with its principles within Member States,[18] it also prohibits transfers of personal data to countries which fail to ensure an

---

[12] *See id.*

[13] 'We are not talking about a modest proposition here. Telepower in its various forms - telecommunications, electronic entertainment, computer and information services, robotics, artificial intelligence, and expert systems - is already reshaping the global economy, internationalizing labor, and shifting jobs in space, time, and concept. Some would argue it is rendering the nation state obsolete. JOSEPH N. PELTON, THE GLOBALIZATION OF UNIVERSAL TELECOMMUNICATIONS SERVICES, ANN. REV. OF THE INST. FOR INFO STUD. 141, 143 (1991).

[14] In the United States, the debate on the definition of privacy has raged for over one hundred years. THOMAS M. COOLEY, COOLEY ON TORTS 29 (2d ed. 1880). In 1880, Thomas Cooley penned the phrase the "right to be let alone" as the meaning of privacy. *See id.* The phrase was canonized by Warren and Brandeis in their article on the right to privacy. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). "The phrase 'a right to privacy' as used in law has almost as many meanings as Hydra had heads." Diane Zimmerman, *False Light Invasion of Privacy: The Light that Failed*, 64 N.Y.U. L. REV. 364 (1989).

[15] *See* Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) [hereinafter Directive]. The Directive required Member States of the European Union to amend their national laws consistently with the provisions of the Directive. *See id.* It does not have the force of law; rather the national laws regulate the transactions subject to the Directive. *See* INFORMATION TECHNOLOGY LAW GROUP/EUROPE, EUROPEAN COMPUTER LAW 1.01[2] (1995). For a description of the political process by which the Directive was created, *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995).

[16] *See* Directive, *supra* note 15.

[17] *See* discussion *infra* concerning the provisions of the Directive. Data Subject refers to the individual whose personal information is collected.

[18] *See* Directive, *supra* note 15, art. 32(1).

"adequate level of protection."[19] The United States of America (U.S.) has several statutes which regulate the use of personal information in specific contexts.[20] Much has been written on the issue of whether this panoply of laws significantly protects the data subject's right to privacy in transfers of information occurring solely within the borders of the U.S.[21] However, the passage of the E.U. Directive raises the issue of the adequacy of U.S. privacy protection laws when personal information about E.U. nationals, originating in data banks of Member States, is transferred to U.S. government or business interests.[22]

The Member States have three years to bring their laws into comity with the provisions of the Directive.[23] They are required to adopt each Article of the Directive, but it is clear that only "equivalent" protections must be afforded in each Member State.[24] While this may allow for some variances in the protections afforded by each Member State, the principles of the Directive should probably be considered the minimum standards of protection for the processing of personal information about

---

[19] "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection." *Id.* at art. 25(1).

[20] Among the many statutes are the following: Freedom of Information Act, 5 U.S.C. § 552 (1994); Privacy Act, 5 U.S.C. § 552a (1994); Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a(o); Paperwork Reduction Act, 44 U.S.C. §§ 3501-3520; Privacy Protection Act, 42 U.S.C. § 2000aa-2000aa-12; Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422; Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; Fair Credit Reporting Act, 15 U.S.C. § 1681-1681t; and the Video Privacy Act, 18 U.S.C. § 2710. For a comparison of the provisions of these statutes to the Fair Information Practices guidelines, see Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 82-85 (1996).

[21] *See, e.g.*, ARTHUR MILLER, THE ASSAULT ON PRIVACY 24-53 (1971); Vern Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEX. L. REV. 837, 868-70 (1971); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKLEY. TECH. L.J. 1 (1996).

[22] The 16 member states include Finland, Sweden, Denmark, Ireland, United Kingdom, the Netherlands, Norway, Germany, Belgium, Luxembourg, Austria, Italy, France, Spain, Portugal, and Greece. *See generally* CHRISTOPHER BRIGHT, THE EU: UNDERSTANDING THE BRUSSELS PROCESS (1995).

[23] *See* Directive, *supra* note 15, art. 32. This means that compliance must be accomplished by October 24, 1998.

[24] *See id.*

nationals within Member States. Meeting these minimum requirements should therefore satisfy the requirement of "adequate protections" in non-Member States under Article 25 of the Directive.

It is not too early to scrutinize some of the existing privacy laws in the United States in the attempt to determine their "adequacy" under the Directive.[25] This article begins with a brief comparison of the principles upon which the protection of informational privacy is based in both the United States and the European Union.[26] Next, the article discusses certain major components of the Directive by comparing them to the provisions of federal privacy protection statutes. It is only in comparison to these central provisions that the "adequacy" of any U.S. statute should be judged. The article concludes that in some instances, the laws, though not perfect, are "adequate". Some statutes however, do not rise to the necessary level of acceptability under the Directive and need to be revised.

II. A Comparison of the Principles Underlying the Protection of Informational Privacy in the United States and in the E.U.

A. *Conceptual differences Between the U.S. and the E.U.*

There are significant conceptual differences between the system of law in the U.S. and that of most E.U. Member States.[27] In the U.S. there has been a long and pronounced de-

---

[25] *See* Directive, *supra* note 15.

[26] This is not meant to be an exhaustive review of the long common law history in the development of privacy concepts in the United States and their relation to the protection of computerized information. Rather the focus of this article is the nature of selected federal statutes which regulate the collection, and dissemination of personal information about individuals. *See generally* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962 (1964); Richard Turkington, et. al, Privacy Cases and Materials (1992)(for a more in depth review of the principles of privacy). There is also significant literature dealing with the nature of privacy in the new technological age. *See, e.g.*, Vern Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer,* 49 Tex. L. Rev. 137 (1971); Alan Westin & Michael Baker, Data Banks in a Free Society (1972); Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 Hofstra L. Rev. 893 (1984).

[27] *See* European Computer Law, *supra* note 10 at 1. The U.S. shares a common law tradition with the U.K., and the Republic of Ireland of the EU. *See id.* The remainder of the EU nations have legal systems based on the civil law. *See id.* This means that there are differences in the way in which the common law coun-

bate as to the nature of privacy and its parameters in the context of computerized personal information.[28] The sources of federal "privacy law" in the U.S. are the common law and a variety of statutes.[29] The U.S. Constitution does not explicitly list privacy as one of its guarantees.[30]

The source of the protection afforded personal information in the Directive is Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[31] The Convention guarantees the right of privacy for "private and family life, . . . home . . . and correspondence."[32] Although the Directive does not directly define privacy, its parameters are given through the creation of both substantive rights for the individual and duties for users and collectors of the information. The advantage to this Civil Law approach is that the E.U. avoided the arduous process of creating a comprehensive defini-

---

tries and the civil law countries view the interpretation of statutes, the relative importance of case law, and the importance of academic writings. *See id.*

[28] *See* Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 LAW & CONTEMP. PROBS. 281 (1966); ALAN WESTIN, PRIVACY AND FREEDOM (1967); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421 (1980)(for a variety of definitions of 'privacy').

[29] Although there is no generalized right to privacy under the U.S. Constitution, the First and Fourth Amendments provide for privacy in certain contexts. The U.S. Supreme Court has also recognized a penumbral right to privacy in matters of intimacy and marital choice. *See also* Griswold v. Connecticut, 381 U.S. 479 (1965). The tort of the invasion of privacy was created by Thomas Cooley and redefined by Prosser. *See* THOMAS M. COOLEY, COOLEY ON TORTS 29 (2d ed. 1880). William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). Finally, there are federal statutes, which regulate the processing of personal information in specific contexts. In this article, I evaluate the 'adequacy' of four of these statutes. *See* discussion *infra* part III.

[30] Privacy under the U.S. Constitution comes in the form of protection against unreasonable search and seizure under the Fourth Amendment and the right to free association under the First amendment. In Griswold v. Connecticut, the U.S. Supreme Court created a "penumbral" right of privacy in a narrow area of procreation. *See* Griswald v. Connecticut, 381 U.S. 479 (1965). Other extensions of the right to privacy include the right to an abortion.

[31] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, Europ. T.S. No. 5, 213 UNTS 221 (1950) [hereinafter Convention]. The provisions of the Convention supersede national law and are applicable by their own force and effect. *See generally* M. CHERIF BASSIOUNI, INTERNATIONAL EXTRADITION IN U.S. LAW AND PRACTICE, Vol. II, Chapter IX (1983).

[32] Convention, *supra* note 31, at art. 8(1). These rights are limited under the Convention by the dictates of "law and [are] necessary in a democratic society in the interests of national security. . ." *Id.* at art. 8(2).

tion of privacy which has plagued U.S. law.[33] While the option has been discussed in the U.S., neither the U.S., nor the E.U. has made privacy a property right.[34] Despite these conceptual differences, the economic and societal forces that drove the development of informational privacy protections in both the U.S. and the E.U. are similar. However, the legal method by which the U.S. and E.U. addressed the problem of providing for informational privacy is markedly different.

B. *Economic and Societal Trends Giving Rise to the Information Society*

In the U.S., as in the E.U., the shift from an industrial economy to information economy is the basis of the surge in use of personal information.[35] The "new" world economy is based upon selling personal and professional services rather than selling of manufactured goods.[36] This new economy came to be known as the "Post Industrial Society" or the "Information Economy".[37]

The merging of audio and visual communications with computers has resulted in the development of a flexible and diverse international information-exchange system. This integrated system allows the nearly instantaneous transfer of information through cables, satellites, microwave relays and fiber optics.[38]

---

[33] For examples of the numerous definitions of privacy, see RICHARD C. TURKINGTON, ET. AL, PRIVACY CASES AND MATERIALS (1992).

[34] *See* Diane Lehneer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 667 (1992). *See generally* Mell, *supra* note 20.

[35] *See generally* DANIEL BELL, THE COMING OF THE POST-INDUSTRIAL SOCIETY 47-119 (1973).

[36] *See* Daniel Bell, *Communications Technology-For Better or for Worse*, HARV. BUS. REV., May-June 1979, at 20.

[37] *Id.* at 22.

[38] *See id.* at 21. The growth of this international system was supported by the downward trend in the cost of computer systems. *See id.* The first commercial computer was built in 1951 at a cost of $701,000. *See id.* The computer occupied 10 cubic feet. The same amount of computing power can today be stored in a one-centimeter square silicon chip that costs $19. *See* JAMES V. VERARGI & VIRGINIA SHUE, FUNDAMENTALS OF COMPUTER-HIGH TECHNOLOGY LAW 247 (1991). From 1952 to 1980, the average computer system cost dropped from $1.26 to $0.0025 per 100,000 calculations. COMPUTER-BASED NATIONAL INFORMATION SYSTEMS 4 fig. 2 (Stephen J. Andriole ed., 1984) (citing OFFICE OF TECHNOLOGY ASSESSMENT AND PRESIDENT'S REORGANIZATION PROJECT, FEDERAL DATA PROCESSING REORGANIZATION STUDY: BASIC REPORT OF THE SCIENCE AND TECHNOLOGY TEAM 29-30 (1978)).

The information generates substantial revenues for its collectors.[39] Many states within the U.S. use personal information as a revenue generating resource.[40] The information industry represents a significant source of employment for government and commercial operations alike.[41] In the E.U., economic competition between Member States is not only for jobs created by the information economy, but also for the revenue derived from processing the data itself.[42]

Less technologically advanced countries have become dependent upon the more developed countries for information processing services.[43] The inability of the less developed countries to fully participate in the manipulation of data originating within their borders creates what one commentator referred to as an "information proletariat."[44] Countries that cannot perform their own data processing run the risk of their economies lagging in job development within the information economy.[45]

In the U.S., the drive to exclude access to data collected pursuant to governmental mandate resulted in the imposition of policies that restricted the flow of valuable information. For example, one state government attempted to exclude a private, commercial enterprise from selling data processed by the state.[46] Additionally, the U.S. government controls the export

---

[39] In 1988 alone, the combined revenues of the three largest credit bureaus totaled almost 900 million dollars. *See* Jeffrey Rothfelder, *Is Nothing Private?*, BUS. WK., Sept. 4, 1989, at 80.

[40] 40 states sell the information they receive from dealings with the members of the public to private industry. *See Big Brother May Be Closer Than You Thought*, BUS. WK., Feb. 9,1987, at 85.

[41] The late Commerce Secretary, Ronald H. Brown, remarked that the information sector accounts for more than 10% of the Gross National Product. *See* Commerce Secretary Ronald H. Brown, *Brown Lists Clinton Administration's Advisor on Information Infrastructure*, DAILY REP. FOR EXECUTIVES, Jan 7, 1994. At an address of the National Press Club, Vice President Albert Gore reported that one-half to two-thirds of all U.S. workers are employed in information economy jobs. *See* VICE PRESIDENT ALBERT GORE, THE NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, NATIONAL INFORMATION INFRASTRUCTURE AGENDA FOR ACTION 5 (1993).

[42] *See* LOUWERS, *supra* note 2, at 16-17.

[43] *See* J. BECKER, INFORMATION TECHNOLOGY AND A NEW INTERNATIONAL ORDER (1984). *See also* Ennison, *Legal Aspects of Transborder Data Flow in Developing Countries: Sovereignty Considerations*, 1984 INT'L BUS. LAW. 163.

[44] LOUWERS, *supra* note 2, at 16-17.

[45] *See id.*

[46] *See* Legi-Tech, Inc. v. Keiper, 766 F.2d 728 (2d Cir. 1985). In this case, Legi-Tech sought access to New York State legislative developments. *See id.* It wanted

of technical data through the Export Administration Act,[47] while Germany, a Member State, imposes a duty upon processors to do the work locally.[48]

Since computers were invented in the 1940's, they have been used as a fundamental tool in the operation of government, commercial and academic industries.[49] As in the U.S., the E.U. Member States were forced to find an efficient means of information processing to aid their decision making. Often this need required Member States to rely on information stored on foreign soil. This dependence has the potential to tip the balance of power between sovereign states,[50] as well as creating conflict between western and "third world" nations.[51]

From the individual's viewpoint, the problems of centralization of data are the same in both the U.S. and the E.U. The magnitude and diversity of the population has isolated the government from its constituents while requiring greater contact in the form of government backed support.[52] The collection of this personal information and the maintenance of these files is a significant consequence of the variety and concentration of institutional relationships with individuals.[53] The balance between the institution seeking better information and the individual

---

to market the information for a fee. *See id.* Since the state of New York sold the material itself, it denied access to Legi-Tech. *See id.* The Court held that New York could not deny access to Legi-Tech, but that it could charge Legi-Tech a fee for the data. *See id.*

[47] Export Administration Act (EAA) of 1979, 50 U.S.C. § 2401 (1980).

[48] *See Trade Barriers to Telecommunications, Data and Information Services*, 4 TRANSNAT'L DATA & COM. REP., at 179 (June 1982).

[49] *See* Mell, *supra* note 20, at 19.

[50] "Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supra-national data flows." Statement of Louis Joinet, French Magistrate at the Vienna Symposium of 1977, *cited in* Zimmerman, *Transborder Data Flows: Problems with the Council of Europe Convention, or Protecting States from Protectionism*, N.W. J. INT'L L. & BUS 18 (1982).

[51] This friction has been apparent between the U.S. and Canada. Robinson, *Extraterritoriality and Data Flows*, TRANSNAT'L DATA & COM. REP., June 1986, at 27. A large amount of Canadian data is processed in the U.S. *See id.*

[52] The federal U.S. government collects a average of 18 files on each man, woman and child in the U.S. *See* ROBERT E. SMITH, PRIVACY: HOW TO PROTECT WHAT'S LEFT OF IT 82 (1982). The state government collects an average of 15 files on each resident. *See id.*

[53] *See* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 4 (1977).

seeking to control the dissemination of personal information has shifted in favor of the institution due to the anonymity with which the institutions operate.[54] This imbalance prompted the creation of post-industrial society's label, the "dossier society."[55] The anonymity of the information system's operation divests the individual of any real power over the use of personal information.[56]

C. *Development of Legal Protections of Computer Processed Personal Information*

The international diffusion of data protection policies in the 1960's and 1970's was the result of a series of common events across Western Europe and North America.[57] Four catalysts were identified: the consideration of the creation of centralized data banks; the proposal for the creation of universal personal identification numbers for citizens; the decennial census of 1970; and the publication of several books describing the emergence of a surveillance society.[58] As a result of the policy debates concerning the effect of computers on informational privacy, several statutes regulating privacy on the national level were enacted.[59] In turn, the Organization for Economic Cooperation and Development (O.E.C.D.), the Council of Europe, and the European Union sought to develop guidelines for the consistent treatment of computerized personal information across international borders.

---

[54] *See* SMITH, *supra* note 52, at 90.

[55] Vern Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer,* 49 TEX. L. REV. 837, 837-39 (1971).

[56] *See* KENT GREENAWALT, LEGAL PROTECTIONS OF PRIVACY, FINAL REPORT TO THE OFFICE OF TELECOMMUNICATIONS POLICY EXECUTIVE OFFICE OF THE PRESIDENT 42 (1976).

[57] "Diffusion" refers to the process by which policy innovations spread from one country to another. *See* HAROLD WILENSKY ET AL., COMPARATIVE SOCIAL POLICY: THEORIES, METHODS, FINDINGS IN COMPARATIVE POLICY RESEARCH: LEARNING FROM EXPERIENCE, 389-90 (M. Dierkes, H.N. Weiler, and A.B. Antal eds, 1987).

[58] For a discussion of these factors, see COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 46-55 (1992).

[59] The first such statute was enacted in Sweden in 1973, followed by the U.S. in 1974 and by West Germany and Canada in 1977. *See id.* at 57 *citing* Status of Data Protection /Privacy Legislation, TRANSNAT'L DATA & COMM. REP., various issues.

The O.E.C.D.[60] studied the problem beginning in 1974. Their study resulted in the enactment of the O.E.C.D. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980.[61] These guidelines covered the automatic processing of personal data in both the public and private sectors.[62]

Beginning in the 1960's, the Council of Europe became aware of the threat posed to individuals by the unregulated computerization of personal information files.[63] Their concern was based on the requirements of Article 8 of the European Convention of Human Rights.[64] In response to these concerns, the Council of Ministers adopted two resolutions, one dealing with the private sector in 1973, another in 1974 regulating the activities of the public sector.[65]

The drawing of a distinction between the data processing activities of the private and the public sector was consistent with the U.S. approach. There was considerable debate in the U.S. as to whether a distinction between government (public) information collection and collection by the private industries was justified.[66] In the end however, the U.S. treated the regulation of government data processing activities separately.

By contrast, in 1980, the European Council of Ministers adopted an omnibus approach to the problem of computerized information in the Council of Europe Convention.[67] The Con-

---

[60] The O.E.C.D. is made up of 24 member nations: Australia, Austria, Belgium, Canada, Denmark, Finland, France, West-Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States.

[61] *Organization for Economic Co-operation and Development: Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, O.E.C.D. Doc. C(80)58 (Final) of Oct. 1, 1980, *reprinted in* 20 I.L.M. 422 (1981).

[62] *See* GREENAWALT, *supra* note 56.

[63] *See* LOUWERS, *supra* note 2, at 17-22.

[64] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221.

[65] *See* LOUWERS, *supra* note 2, at 17-22.

[66] *See* GREENAWALT, *supra*, note 58.

[67] For an analysis of both the Convention and the OECD guidelines, see Bing, *The Council of Europe Convention and the OECD Guidelines on Data Protection*, MICH. Y.B. OF INT'L. LEGAL STUD. 271 (1971).

vention had general international application[68] and covered the automatic treatment of data concerning identifiable natural persons. After the adoption of the Convention, the Committee of Experts rendered several recommendations on the protection of various types of personal information processing.[69]

The first comprehensive attempt to develop standards for the protection of computer processed information in the U.S. was the 1973 report issued by the Advisory Committee on Automated Data Systems, a subcommittee of the Health Education and Welfare Committee. The report, entitled, "Personal Data Systems: Records, Computers and the Rights of Citizens," listed five factors considered necessary to protect an individual's interest in personal information collected about him.[70] The federal response to this report was to pass several different statutes; each protecting privacy in one specific context, but each statute was ostensibly based on these five principles.[71]

The European Parliament was also active in advocating the protection of computer processed information. In the 1970's, it began requesting the establishment of rules, which would guar-

---

[68] Opened for signature in January 1981, it became effective when France, Germany, Norway, Spain and Sweden ratified it. *See* LOUWERS, *supra* note 2, at 17-22.

[69] The Committee of Experts submitted recommendations on a variety of types of data including medical data and research and statistical data. *See* LOUWERS, *supra* note 2, at 17-22. The recommendations were not legally binding. *See id.*

[70] The five factors were as follows: 1) The individual should be able to find out what files concerning him exist; 2) When the individual provides information concerning himself, he should know how the information is to be used and how broadly the information is to be disclosed; 3) If the record holder wants to disclose the information more broadly than originally contemplated, consent of the subject of the record should be obtained; 4) The individual should have access to files concerning him and the opportunity to correct outmoded information should be updated; and 5) Files should be afforded adequate security and outmoded information should be updated. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 41-42 (1973)[hereinafter HEW REPORT].

[71] Among the statutes enacted were the following: The Privacy Act of 1974, 5 U.S.C § 552a (1994); Computer Matching and Privacy Protection Act of 1988, 5 U.S.C § 552a(o) (1994); Privacy Protection Act of 1980, 42 U.S.C. § 2000aa-2000aa-12 (1994); Freedom of Information Act of 1966, 5 U.S.C § 552 (1994); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1994); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1994); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681-1681t (1994); Video Privacy Act, 18 U.S.C. § 2710 (1994).

antee the individual protections against the growing perceived threat of computerization of personal information.[72] While individual member states enacted national legislation to prevent data processing abuse, the first European Union effort in this regard was made in 1981.[73] In that year, the European Commission recommended that Member States ratify the 1981 Data Protection Convention of the Council of Europe.[74] This Convention provided guidelines for individual member states to follow in drafting their own legislation. The first draft of the current Directive was presented in September 1990.[75]

D. *An Overview of the EU Directive and U.S. Data Protection Laws*

The Directive is divided into seven chapters and thirty three Articles, which define not only the rights of the data subject, but, also outline the duties of the data collector and processor to both the data subject and to third parties who want access to the data.[76] The Directive places limitations on the permissible content of records and creates substantive rights in the data subject.[77]

The Directive requires member states to modify their national laws to include the minimum standards it has established. This means that despite the Directive's goal of harmonizing European law, the actualization of those principles could vary between member states. This raises the question of whether the adequacy of the third country's data protection provisions are to be judged by the national laws of the individual Member State involved, or whether the minimum requirements of the Directive are the benchmark of adequacy. Due to the Directive's goal of harmonizing the laws of the member states, it

---

[72] *See* 1976 O.J. (C 100) 27; 1979 O.J. (C140) 147; 1982 O.J. (C87) 39.

[73] The Swedish Data Bank Statute, enacted in 1973, served as the model for European data protection laws. *See* WARREN FREEDMAN, THE RIGHT OF PRIVACY IN THE COMPUTER AGE 128-129 (1987). Within four years, West Germany, France and Denmark had enacted data protection legislation as well. *See id.*

[74] Convention for the Protection of Individuals with regard to Automatic Processing of Persona Data, *opened for signature* Jan. 28, 1981, Eur.T.S.No. 108 (hereinafter Convention).

[75] *See* Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277) 3.

[76] *See* Directive, *supra* note 15.

[77] *See* discussion of the provisions of the Directive *infra* Part II. D.

might be that national variances must be viewed as subordinate to the rights extended to the individual under the Directive.

The rights given to the data subject are bolstered by the duties imposed upon the data collector to ensure informational privacy.[78] The substantive rights given individuals under the Directive echo the five principles proposed by the HEW Report.[79] The Directive, however, clarifies the parameters of informational privacy by imposing specific duties, for maintenance of the privacy, on the data collector. Pursuant to the Directive, the adequacy of the protections afforded by the third country is necessarily contextual, considering all of the circumstances surrounding the data transfer exchange. This would include an inquiry into: 1) the nature of the data; 2) the purpose and duration of the proposed processing operation; 3) the country of origin; 4) the country of final destination; 5) the rules of law in force and professional rules; and 6) security measures.[80] Despite the goal of harmonizing the treatment of the processing of personal information, the Directive also provides a series of derogations from compliance with its provisions.[81]

---

[78] Under the Directive, "[t]he collector has the duty to fairly and lawfully process the information, to restrict its collection of data to specified explicit and legitimate purposes, to only take such information as is necessary for the stated purposes, to maintain the accuracy and completeness of the data, and not to maintain the data any longer than is necessary for the stated purposes of the data processing." Directive, *supra* note 15, art. 6.

[79] *See* HEW REPORT, *supra* note 72.

[80] Since context is the key in the determination of adequacy, and because the Directive gives the parties the ability to contract specific terms in the transfer of data, there should not be inordinate difficulty in the US government or businesses trading information with Member States.

[81] Directive, *supra* note 15, art. 26 (1), (2). Pursuant to Article 26, there are several circumstances under which a member state may allow the transfer of personal data to a third country that does not insure an adequate level of protection. Those circumstances occur when the data subject has "unambiguously" given his consent to the transfer; transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures; transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; transfer is necessary on public interest grounds; transfer is necessary in order to protect the vital interests of the data subject; the transfer is made from information which is already public; or the controller, by contract adduces sufficient guarantees. *Id.* The derogations allow a commercial enterprise from a "nonconforming" country to contract for the ability to transfer data from a Member

The U.S. has at least nine federal statutes that regulate some aspect of informational privacy.[82] Some statutes regulate the activities of the federal government, and others regulate the data processing activities of private industry. To determine the "adequacy" of U.S. legislation, the major provisions of the E.U. Directive will be compared with the major provisions of certain U.S. legislation. The analysis assumes that data exchanges are being requested of a mythical E.U. Member State that has adopted the Directive without modification. In this hypothetical, the request is being made by a collector based in the U.S.

The U.S. statutes used in this analysis are The Privacy Act (PA),[83] The Computer Matching and Privacy Protection Act (CMPPA),[84] the Fair Credit Reporting Act (FCRA),[85] and the Family Educational Rights and Privacy Act (FERPA).[86] The purpose of each statute and the nature of the records covered by it are a necessary part of the review. Each of the four statutes deal with a specific type of record or with processing performed by a particular collector.

III. An Assessment of the Adequacy of U.S. Informational Privacy Statutes under the E.U. Directive

A. *Purpose of the Provisions*

The Directive deals with the treatment of personal information or data. Personal data is defined as "any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, mental, economic, cultural or social identity."[87]

State. This allows for widely varying treatment of information. For the purpose of this Article, the derogations provided under Article 26, will not be considered.

[82] *See* list of statutes *supra* note 73.

[83] *See* Privacy Act (PA) of 1974, 5 U.S.C § 552a (1994).

[84] *See* Computer Matching and Privacy Protection Act (CMPPA) of 1988, 5 U.S.C. § 552a(o) (1994).

[85] Fair Credit Reporting Act of 1970, (FCRA) 15 U.S.C. §§ 1681-1681t (1994).

[86] Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g (1994).

[87] Directive, *supra* note 15, art. 2(a).

Article 1 of the Directive establishes privacy with respect to the processing of personal data as a "fundamental right and freedom of natural persons."[88] This right is not absolute. The Directive provides that "[m]ember states shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."[89]

The determination of "privacy" as a fundamental right in E.U. Member States creates presumptions in favor of the individual's power over personal data. By way of contrast, neither the U.S. Constitution nor any of the current federal statutes establish privacy as a fundamental right.[90] Consequently, U.S. law presumed the right of the collector to disclose information in his possession. This presumption of "disclosurability" is evident in most U.S. statutes.

The PA was enacted as an amendment to the Freedom of Information Act (FOIA).[91] Its stated purpose was to give individuals a right to request access to records maintained about them and to prevent agency disclosure of personal information to third parties without the subject's consent.[92] A significant limitation on the protection of the individual's right to privacy is that in a conflict between the PA and FOIA's disclosure requirements, FOIA would generally prevail.[93]

---

[88] *Id.* art. 1(1). This necessarily excludes business entities such as corporations. *See id.*

[89] *Id.* art. 1(2).

[90] *See* discussion *infra* part III.C.

[91] *See* Freedom of Information Act (FOIA), 5 U.S.C. § 552 (1994) (This statute was enacted to promote open government by disclosing information relating to the workings of government). For the specific provision of the PA referred to above, see 5 U.S.C. § 552(a)(3) (1994).

[92] *See* 5 U.S.C. § 552a(d)(1) (1994). This section also requires that the subject be given a written copy of the record concerning him and that the copy be in a form comprehensible to the individual. *See id.* Subject to limitations to be discussed below, the individual must first "discover" that such a record exists before he can request access to it. *See* discussion *infra* part III. D. 1.

[93] "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be— . . . required under section 552(FOIA)." 5 U.S.C. § 552a(b)(2). *See also* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 593 (1995).

The Computer Matching and Privacy Protection Act (CMPPA) amends the PA to restrict the collection of information from individuals.[94] It guides government agencies in the performance of data matching activities about the same individual. The matches are not limited to government data banks, but can include data from commercial enterprises as well. Such far-reaching access can easily impact an E.U. resident.

The Fair Credit Reporting Act (FCRA) regulates the data disclosure activities of consumer reporting agencies[95] (CRA) to third parties.[96] The FCRA requires CRA's to adopt "reasonable procedures" which would meet commerce's need for personal information about individuals but would do so with fairness and equity to the consumer in terms of confidentiality, accuracy, relevance and proper use of the information.[97] The FCRA, like the Directive, seeks to prevent unreasonable or careless invasions of the individual's privacy but not to preclude the dissemination of information.[98]

The Family Educational Rights and Privacy Act of 1974 (FERPA) grants individuals the right of access to their own "education records"[99] and prevents disclosure of those records to

---

[94] *See* 5 U.S.C. § 552a(o) (This statute is used to determine the individual's eligibility to receive federal benefits or to discover fraud). *See generally* Donsia Renee Strong, Comment, *The Computer Matching and Privacy Protection Act of 1988: Necessary Relief From the Erosion of the Privacy Act of 1974*, 2 SOFTWARE L.J. 391 (1988). As an amendment to the PA, it carries the PA's deficiencies in coverage. *See id.*

[95] A consumer reporting agency is defined as "[a]ny person which, for monetary fees, dues or on a cooperative basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681a(f) (1994).

[96] *See* 15 U.S.C. § 1681-1681t.

[97] *See* 15 U.S.C. § 1681(b).

[98] *In re* TRW, Inc., 460 F. Supp. 1007 (D.C. Mich. 1978); Conley v. TRW Credit Data, 381 F.Supp. 473 (D.C. Ill. 1974); Williams v. Equifax Credit Information Services, 892 F. Supp. 951(E.D. Mich. 1995).

[99] "For the purpose of this section, the term 'education records' means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." Family Education Rights and Privacy Act, 20 U.S.C. § 1232g(a)(4)(A).

third parties without consent.[100] Education records include information concerning the student and parent's finances, confidential letters of recommendation, and academic educational records of every level of schooling.[101] Unlike the PA, FERPA is not limited to students who are U.S. nationals or permanent residents.[102] This provision operates when foreign students apply and matriculate in U.S. schools and universities.

B. *Scope of Records Covered by the Directive*

Pursuant to Article 3, the Directive applies to the processing of personal data by computer, whether automatic or partly automatic.[103] Manual data processing is covered only if it is part of the personal data filing system.[104] Also exempted from coverage is processing done by natural persons for personal or household purposes.[105]

Article 7 lists several alternative conditions precedent to the processing of personal data based on the presumption in favor of the individual's power to control personal information concerning him.[106] The first condition is that the data subject has "unambiguously given his consent" to the processing.[107] Implicit in this provision is notice to the individual that data concerning him has been requested. While this does not mean that the individual necessarily had prior knowledge of the existence of the file, this article makes it clear that the individual

---

100 The right of access for students under 18 years of age resides in the parent(s). *See* 20 U.S.C. § 1232g (1994).

101 *See id.* at 20 U.S.C. § 1232g(a)(1).

102 "[T]he term student includes any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution." *Id.* at 20 U.S.C. § 1232g(a)(6).

103 Directive, *supra* note 15, art. 3(1).

104 Personal data filing system is defined as "any structured set of personal data, which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. *See id.* art 2.

105 Directive, *supra* note 15, art. 3(2). "[T]he council and commission consider the expression 'purely personal or household activity' must not make it possible to exclude from the scope of the directive the processing of personal data by a natural person, where such data are disclosed not to one or more persons but to an indeterminate number of persons." Statements for Entry in the Minutes Accompanying the Draft Directive, 4730/95 Annex 1 at 3.

106 *See id.* art. 7.

107 *See id.* art. 7(a).

will be made aware of its existence before a disclosure of the information can be made. Two other conditions under Article 7 permit processing of personal data to facilitate contract obligations of the data subject both before the contract is entered and as necessary for the performance of a contract to which the data subject is a party.[108] These conditions imply knowledge on the part of the data subject, but apparently allow processing without requiring his express consent.

Several of the provisions of Article 7 concern official activities of collectors or third parties when processing personal data. Processing under these provisions do not seem to require prior knowledge of either the existence of the file or the request for the information. These provisions permit processing which is necessary:

> for compliance with the controller's legal obligation;[109] for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;[110] and for the purposes of the legitimate interests pursued by the controller or third party unless they are overridden by the data subject's fundamental rights and freedoms.[111]

The Directive does not indicate how these "legitimate interests" are to be determined.

Article 9 contains exemptions to these conditions. A unique Directive exemption provides for processing personal data carried on for journalistic purposes.[112] There is no single Constitutional or statutory provision in the U.S. comparable to this

---

[108] *See id.* art 7(b).

[109] Directive, *supra* note 15, art. 7c.

[110] *Id.* art. 7e.

[111] *Id.* art. 7f. The explanatory memorandum to the 1992 Draft stated that the "balance-of-interest clause is likely to concern very different kinds of processing, such as direct mail marketing and the use of data which are already a matter of public record." Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Oct. 15, 1992, 1992 O.J. (C311/30) 35.

[112] "Member states shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expressiom onlu if they are necessary to reconcile the right to privacy with the rules governing freedom of expression." Directive, *supra* note 15, art. 9.

Article.[113] This provision has met with the criticism that it is both overbroad and too narrow.[114] Due to the history of U.S. law in this area, it is doubtful that such a provision could be adopted in the U.S.[115]

The Directive has wide and general application to the processing of personal data within the E.U. No single U.S. statute has such general application. However, the Privacy Act is fairly comprehensive in its coverage of governmental data banks. It covers "records" about an "individual" in a "system of records" held by federal agencies. By definition, this excludes the activities of commercial enterprises. The term "records" means any information revealing something about the individual.[116] The PA defines the "individual" as a "citizen of the United States or an alien lawfully admitted for permanent residence."[117] A "system of records" is any group of records under agency control that is indexed and can be retrievable by an individual's name or other identifier.[118]

The PA is a restriction upon the federal government's ability to collect and process information. It does not apply to private industry. An even greater deficiency is that the PA does not apply to nonresident aliens.[119] These deficiencies mean that the PA provides no protection against the disclosure of personal data for the citizens of an E.U. Member State.

While not identical, the records covered by the PA substantially match those protected under the Directive. The limitation of protection for U.S. citizens or permanent resident aliens remains a significant problem. The fact that the PA applies only to federal data systems is relevant only if the statutes regulating non-governmental data processing are found lacking in the protection they afford informational privacy.

---

113 The tension between the freedom of the press and the individual's right to privacy is rumored to have been at the basis of the Warren and Brandeis article on The Right to Privacy. *See supra* note 14.

114 *See* James R. Maxeiner, *Business Information and "Personal Data: Some Common-Law Observations About the EU Draft Data Protection Directive*, 80 IOWA L. REV. 619, 634 (1995).

115 *See* Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption " Won't Work*, 80 IOWA L REV. 639 (1995).

116 *See* Privacy Act (PA) of 1974, 5 U.S.C. § 552a(a)(4) (1994).

117 5 U.S.C. § 552a(a)(2).

118 *See* 5 U.S.C. § 552a(a)(5).

119 *See* 5 U.S.C. § 552a(2)(a).

The CMPPA broadly covers all records held by federal governmental agencies. Its application is limited however to those records which would be used to perform a matching activity.[120] Since it is an amendment to the PA, it too would not protect non-U.S. citizens or non-permanent resident aliens.

The FCRA applies to records about consumers held by consumer reporting agencies.[121] This would also exempt records held by an entity that did not regularly engage in the dissemination of information and those which did not charge a fee for such information.[122] The greatest limitation in FCRA's scope is that it only regulates the use of information primarily for family, household, employment and insurance purposes.[123] This excludes use of information for business purposes.[124] Also excluded are reports concerning authorization and approval of credit card transactions.[125]

Unlike the Directive, the FCRA is not limited to computer stored information.[126] FCRA is also not hampered by the PA's limitation of applicability to U.S. citizens or resident aliens. The three international credit bureaus collect and maintain files of several million individuals around the world.[127] The impact of this statute on E.U. nationals seems evident.

FERPA applies to records maintained by any educational institution, which receives funding from the federal government.[128] There are probably very few educational institutions

---

120 *See* 5 U.S.C. § 552a(o)(1)(A)-(D).

121 *See* Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C §§ 1681-1681t (1994). "The term 'consumer' means an individual." 15 U.S.C. § 1681a(c). "The term 'person' means any individual, partnership, corporation, trust, estate, cooperative association, government or governmental subdivision or agency, or other entity." 15 U.S.C. § 1681a(b). The records are either "consumer reports" or "investigative consumer reports." *See* 15 U.S.C. § 1681a(d)-(e).

122 *See* 15 U.S.C. § 1681a(f) which exempts records concerning a creditor's dealings with its own debtor.

123 *See* 15 U.S.C. § 1681a(d)-(e).

124 *See generally* Zeller v. Samia, 758 F. Supp. 775 (D. Mass. 1991); Williams v. Equifax Credit Information Services, 892 F. Supp. 951 (E.D. Mich. 1995).

125 *See* 15 U.S.C. § 1681a(d).

126 FCRA covers all records or files on the consumer "recorded and retained by a Consumer Reporting Agency regardless of how the information is stored." 15 U.S.C. § 1681a(g). The Directive excludes records if they are not compiled at least partly by automatic means. *See* Directive, *supra* note 15, art. 3(1).

127 In 1988, Trans Union, TRW, and Equifax held a combined 410 million files on individuals. Jeffrey Rothfelder, *Is Nothing Private?,* BUS. WK., Sept. 4, 1989.

128 *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(1).

in the U.S. which do not receive some federal aid. Therefore, this statute probably has universal application to the many E.U. nationals who attend an educational institution in the U.S.[129]

C. *Use of Data and Permissible Content*

Article 6 of the Directive creates duties for the data collector and user that protect the data subject.[130] These duties loosely fall under the heading of "data quality" and are the basic assumptions upon which the substantive rights of the data subject are built. They require that accuracy and relevance be maintained, limitation of collection to specified purposes, expulsion of stale data, delineation of permissible use of the data, and designation of impermissible subject matter for files.[131] The requirements of the U.S. statutes vary, but each shares the Directive's concerns with accuracy and limitations on the uses of data.

Article 6(1) requires that the data be processed fairly and lawfully. It requires that the data be collected for a specified, explicit, and legitimate purpose and not further processed in a way incompatible with those purposes.[132] Finally, the data collected must be adequate, relevant and not excessive for the purpose collected or further processed.[133] Accuracy of the data must be assured by reasonable steps, and inaccurate or incomplete data must be erased or corrected.[134] Finally, the data should not be kept in a form which can identify the subject for any longer than is necessary to accomplish the purpose for which data is collected.[135] Subsection two places the duty of en-

---

[129] Even state universities must comply with the requirements of FERPA. *See* Kestenbaum v. Michigan State University, 97 Mich. App. 5, 294 N.W.2d 228 (1980), *aff'd* 414 Mich. 510, 327 N.W.2d 783 (1982).

[130] The controller is "the natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data." *Id.* art. 2(d).

[131] *See generally* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995).

[132] Directive, *supra* note 15, art. 6(1)(b).

[133] *See id.* art. 6(1) (a)-(e).

[134] *See id.* art. 6(d).

[135] *See id.* art. 6(e). The manner of determining the timeliness of the information is not specified in the Directive.

suring compliance with paragraph one upon the controller of the personal data.[136]

The PA does require that all information collected be relevant for the agency's purpose.[137] The Act also requires the agency to maintain such "accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness" in decisions made about the data subject.[138] A presumption of relevance and propriety of purpose assists the agency in its collection activities. There is no express requirement that "stale" information be purged at any particular time. The CMPPA shares the presumption of relevance with the PA. The agency is required, however, to do an independent check of the information before it can take adverse action against the data subject.[139]

Under the FCRA, the CRA is required to assure the maximum possible accuracy of the information by maintaining reasonable procedures. The verification procedures to be used are not outlined in the statute. Consequently, the reasonableness of the procedures is left up to the CRA. "Reasonableness" has been interpreted to mean what a reasonably prudent person would have done to verify the data under the circumstances.[140] Conversely, if the data is determined to be accurate, then the reasonableness of the CRA's procedures will not be questioned.[141] Contextual accuracy is not required.[142] Unlike the Directive and the PA, the FCRA specifies the time after which the information must be deleted from the file.[143] The FCRA also requires that users identify themselves and certify that they are using the information for proper purposes.[144] It has

---

136 *See id.* art. 2(d). The controller is "the natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data. . ." *Id.*

137 *See* Privacy Act (PA) of 1974, 5 U.S.C. § 552a(e)(1) (1994).

138 5 U.S.C. § 552a(e)(5).

139 *See* 5 U.S.C. § 552a(o)(1)(E), (p)(1)(A)(I).

140 *See* Bryant v. TRW, Inc., 487 F. Supp. 1234 (E.D. Mich. 1980).

141 *See* McPhee v. Chilton Corp., 468 F. Supp. 494 (D. Conn. 1978).

142 Austin v. Bankamerica Service Corp., 41F. Supp. 730(D.C. Ga. 1974). *But see* Koropoulos v. Credit Bureau, Inc., 734 F.2d, 37(C.A. D.C. 1984).

143 Most information is not reported after it is seven years old. Files concerning cases under Title 11 and Bankruptcy remain in the files for ten years. *See* 15 U.S.C. § 1681c.

144 *See* 15 U.S.C. § 1681e.

been demonstrated that the CRA's rarely check the validity of the user's stated purpose.[145]

By its language, the FCRA could be said to meet the Directive's standard of "adequacy." However, the history of the statute shows that in truth, the individual's privacy is not fully protected. The failure of the FCRA to ensure contextual accuracy would seem to be at odds with Directive's requirement of fairness and accuracy. The lax interpretation of "reasonable procedures" also poses a problem for ensuring consistent treatment of individuals. The provisions requiring the certification of the user's identity and purposes for the information request lack the type of strict enforcement which would truly protect the individual's informational privacy.

FERPA does not directly require accuracy to be maintained in the education records. Since it allows easy access and pre-disclosure consent of the data subject, it would seem that the data subject is well positioned to rectify any errors.[146] Despite its silence on the issue, FERPA would probably meet the Directive's adequacy standards.

The Directive also provides for the exclusion of certain data content. Article 8 prohibits the processing of data which reveals the race, ethnic origin, political opinion and religious or philosophical beliefs of the individual.[147] In the U.S., only the Equal Credit Opportunity Act specifically prohibits the collection and use, by creditors, of information concerning the individual's race, color, national origin, religion, sex, marital status, age or receipt of public assistance benefits.[148] Also prohibited from

---

[145] In 1983, a sales manager of a car dealership used his ability to validly access a credit bureau computer's files to perpetrate a fraud. JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE 166-67 (1991). In the attempt to "launder" one individual's credit (offender) he obtained the credit records and social security number of another individual with excellent credit (victim). *See id.* He matched the offender with a victim whose name was very similar and whose profession was the same. *See id.* Next, he assisted the offender in applying for over $25,000 credit under the victim's name. *See id.* The scheme was exposed when the offender defaulted and the victim was notified. *See id.* Hackers also pose a problem to the security of data files. *See id.* Michael Synergy is credited with having successfully retrieved the credit record of former President Ronald Reagan. *Crime Bytes Back*, OMNI, Aug. 1990.

[146] *See* discussion *infra* part III.D.2. on access rights under FERPA.

[147] Directive, *supra* note 15, art. 8(1).

[148] Equal Credit Opportunity Act and Regulation B, 15 U.S.C. § 1691 et seq. , 12 C.F.R. § 202. Two additional prohibitions include the use of information con-

disclosure under the Directive is information revealing the individual's trade union membership and data concerning the individual's health or sex life.[149] These prohibitions are lifted when the individual gives explicit consent or discloses the information himself.[150]

In the U.S., the fact of an individual's membership in a trade union might be protected from disclosure under the Freedom of Association provided by the First Amendment of the U.S. Constitution.[151] The prohibition on the disclosure of matters concerning the individual's sex life is enforced only as it falls under the "penumbral" right of individuals to control their own lives in highly personal matters.[152] The collection of information concerning the individual's character, general reputation, personal characteristics, and mode of living is specifically allowed as an investigative consumer report under the FCRA.[153]

D. *Substantive Rights Afforded the Individual*

Under the Directive, the data subject exercises a considerable amount of control over the treatment of personal information concerning him. Some of the significant rights afforded the data subject are: (1) the right to receive notice of the file's existence; (2) the right to access the file; (3) the insuring of restrictions on the collection of the information; and (4) restrictions on the secondary use of the information. The rights afforded under the U.S. statutes vary substantially on these points.

---

cerning the individual's good faith exercise of rights under the Consumer Credit Protection Act and good faith exercise of rights under any state law upon which an exemption has been granted by the Board. 12 C.F.R. § 202.2(2)(z).

[149] Directive, *supra* note 15, art. 8(1).

[150] *See id.* art. 8 (2). The Directive indicates that under some circumstances, the Member State may provide that consent of the data subject cannot be given.

[151] *See* U.S. CONST. amend. I. The U.S. Supreme Court itself is divided on the issue of what type of association is protected and under what circumstances the protection of the Constitution is to be afforded. *See, e.g.,* Buckley v. Valeo, 424 U.S. 1 (1976) (allowing the release of the names of minorities contributing to minority parties). *But see* NAACP v. Alabama, 357 U.S. 449 (1958) (striking down a requirement that the NAACP disclose its membership rosters).

[152] *See* Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965). *But see*, Bowers v. Hardwick, 478 U.S. 186 (1986).

[153] *See* Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681 (1994).

1. *Notice of the File's Existence*

Article 10 and Article 11 both require the controller to notify the data subject when data concerning him is collected.[154] Whether the information is collected from the subject himself or from another party, the collector must, at minimum, inform the data subject of the identity of the controller and the purposes for which the data is intended.[155] This provision also requires that, as regards the circumstances of the processing, the subject should be guaranteed fair processing.[156]

In contrast, pursuant to the PA, the government agency is not required to supply a specific individual with notice of the existence of a data file concerning him.[157] Instead, the PA requires the agency to publish a notice in the Federal Register that lists the character of the record system and the category of individuals covered by the record system.[158] Despite the seemingly low standard of notice, the record of compliance by the agencies has been low.[159] The Directive seems to be based upon direct notice to the specific data subject, therefore, the PA would have to be modified to meet the adequacy requirements of the E.U.

---

[154] Article 10 details the information to be transmitted to the data subject when the information is collected from the data subject. *See* Directive *supra* note 15, art. 10. Article 11 lists the information to be given to the data subject if the information is collected from a source other than the subject. *See* Directive *supra* note 15, art. 11.

[155] Other information provided to the data subject includes; the recipients of the data, whether replies to the inquiries are obligatory or voluntary, as well as, the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him. *See id.*

[156] *See id.* arts. 10, 11.

[157] The general consensus of Congress was that since the information held by government was most likely collected directly from the individual by the agency in question, the individual was already aware of many of the files concerning them. *See* GREENAWALT, *supra* note 58 at 53.

[158] Privacy Act (PA) of 1974, 5 U.S.C. § 552a(e)(4) (1994). This constitutes general notice to the public. Ostensibly, this provision would allow an individual suspecting he was included within the category of individuals covered by the records to object to the disclosure of data concerning him.

[159] The General Accounting Office(GAO) investigated federal compliance with the public notice requirements and found that almost one-third of the agencies were in violation of the PA. *Big Brotherism Feared: GAO Report Raises New Computer Privacy Concerns*, COMM. DAILY, Aug. 31, 1990, at 6. In addition, the GAO reported that 78% of the computer systems were interconnected. *See id.* This was interpreted to mean that "data collected on individuals without their knowledge and consent [w]as widely available" to both government and commercial users." *Id.*

The CMPPA's position on the individual's right to know of a file's existence is based on the presumptions of the PA. However, if an individual's benefits are in jeopardy by virtue of information discovered pursuant to a match, the CMPPA requires the agency to notify the individual of the findings of the match and advise him of what procedures he should follow to challenge the match's results.[160] The CMPPA also prohibits taking adverse action until the agency verifies the accuracy of the adverse information.[161] As a corollary, if the match does not result in adverse action to the individual, a newly compiled (matched) file would exist concerning the individual and no notice of its existence would be required. One might argue that the most important notice an individual would want is the existence of adverse information in his file. If that is the case, then a failure to inform the individual of a newly compiled but "positive" data file might not be considered a serious deficiency. It is substantially different from the provisions of the Directive and might not be considered affording "adequate protection."

The individual's right to discover the existence of a file under the FCRA is limited. If the report is a consumer report, there is no requirement of "automatic" notice.[162] The only notification requirement attaches when the individual has been denied a benefit by the user of a report.[163] If the report is an investigative consumer report, however, the individual is provided a much more complete right of notification. When an investigative report is requested, the user must inform the consumer of the request and of the consumer's right to request disclosure of the nature and scope of the investigation.[164] With this notice, the consumer has the right to request information concerning the purpose, nature and scope of the investigation, the sources of information, and the identity of any of the report's recipients.[165] This coverage is fairly complete. Its drawback is that these requirements are triggered only when the

---

[160] *See* 5 U.S.C. § 552a(p)(3)(1)(B).

[161] *See* 5 U.S.C. § 552a(p)(1)(A).

[162] The individual has a right to see his file on demand. This is not the same as having a right of notification concerning the existence of a file.

[163] *See* Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681m(a) (1994).

[164] *See* 15 U.S.C. § 1681d(a)(1).

[165] *See* 15 U.S.C. § 1681d(b).

individual's initial eligibility is being considered.[166] If the FCRA were to be amended to provide pre-disclosure notice provisions for both investigative reports and regular consumer reports, it would most likely meet the adequacy requirements of the Directive.

FERPA seems to assume that the student is aware of the file's existence and makes no provision for notice. Its protections focus on access to and limitations on secondary disclosure. Since these protections are reasonably well defined, FERPA's silence on notice provisions should not be fatal to its adequacy under the Directive.

2. *Right of Access to the File*

Article 12 gives the data subject the right to obtain personal information held by others. Included in this right of access is the right to correct information that is found to be incorrect. Article 13 allows for the creation of exemptions from this right of access.

Under the PA, the individual has a right to access his file if he believes he is included within the character of the record and category of individuals in a system of records. The individual must make an inquiry of the agency; the agency is not required to notify the individual of the record.[167] This assumes that the individual would have a reason to think he was included within a category of records about to be disclosed. Such awareness is not likely on the part of either a U.S. citizen or E.U. national. Another limitation on the right of access is that the file can only be viewed at the agency's site.[168] If the agency is located in Washington, D.C., gaining access to the record would be burdensome work for the data subject. This deficiency may render the access provisions of the PA inadequate. Pursuant to the CMPPA, an individual can gain access to matched records only after the match is performed. The agency, which performed the match, informs the individual that due to the adverse informa-

---

166 *See* 15 U.S.C. § 1681d(b).

167 *See* 5 U.S.C. § 552a(f). The agency is only obligated to respond to an individual's inquiry if it is satisfied that the inquiry is a legitimate one.

168 *See* 5 U.S.C. § 552a(d).

tion discovered, the individual's federal benefits are at risk.[169] The individual must be advised of the procedures to follow in contesting the findings of the match.[170] The agency cannot proceed with the adverse action until it verifies the data independently.[171] While some might prefer that the notice to the individual be made before the match, the pre-action notification is probably vital. It protects against the loss of benefits by providing the data subject with the opportunity to correct inaccurate statements. While admittedly not perfect, this CMPPA provision does insure the fairness and accuracy required by the Directive. However, it does not presently meet the Directive's notice requirements.

Access under the FCRA can occur upon the request of the data subject, but free access occurs only when the user of a consumer report denies a benefit.[172] In the absence of such a denial, the individual may be required to pay a fee if he wants to access his credit report.[173] The report may be accessed either in person or by telephone pursuant to written request.[174] The access provisions of the FCRA would seem to meet the adequacy requirements of the Directive.

Each institution subject to FERPA is required to establish procedures for granting access to the student's records.[175] Access must be provided in no more than 45 days after the request has been made. The access has few limitations.[176] There should be no problem with FERPA meeting the Directive's adequacy standards concerning access.

3. *Restrictions on Collection of the Information*

Under the Directive, if the data is processed pursuant to 7(e) or 7(f), the data subject has the right ". . . to object at any

---

[169] *See* 5 U.S.C. § 552a(p)(1)(B). The individual is also notified of what procedures he should follow to contest the accuracy of the data. *See* 5 U.S.C. § 552(a)(p)(1).

[170] *See* 5 U.S.C. § 552a(p)(3).

[171] *See* 5 U.S.C. § 552a(p)(1)(A)(i).

[172] *See* Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C § 1681m (1994).

[173] *See* 15 U.S.C. § 1681g-h.

[174] *See* 15 U.S.C. § 1681g-h.

[175] *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(1)(A).

[176] Exclusions include the financial records of parents, and pre Jan. 1, 1975 letters of recommendation. *See id.* at 20 U.S.C. § 1232(g)(a)(1)(B). The student can waive his access rights to recommendation letters.

time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[177] When there is a "justified objection," the controller is required to "cease the processing."[178] Conversely, under the PA, the agency cannot collect the information unless the data is relevant to the agency's use[179] and it must inform the individual whether collection of the data is mandatory or voluntary. This acts as a virtual non-restriction since there is no central agency which monitors the agency's compliance with the PA. No provision allows the data subject to challenge the agency's right to collect the data. The agency's duties to the data subject are evident only by virtue of the penalties imposed for "willful acts"[180] and actual damages for any "adverse effect"[181] suffered by the data subject.

Before a match can be performed under the CMPPA, a formal agreement must exist between the agency and the requesting party.[182] The matching process is limited to an 18-month period.[183] Unlike the PA procedure, the party requesting a match under the CMPPA must specify the source of its authority to collect the information, the purpose of the match, describe the records that will be searched, and the methods to be used in verifying the accuracy of the information used in the match.[184]

Under the FCRA, the CRA may only collect information relating to determinations of credit worthiness or reputation of a consumer.[185] In the absence of an agreement between an individual and his creditor, the creditor is free to record the information with the CRA. The FCRA requires that adverse information in a report cannot be recorded in a subsequent re-

---

[177] *See id.* art 14. In the 1992 Commission Draft, the data subject had a right to object pursuant to every provision of article 7. *Supra* note 13 art. 15.

[178] *See id.*

[179] Relevance means that the information is "necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order. . . " 5 U.S.C. § 552a(e)(1). As an additional protection to the individual, the PA requires that the agency maintain its records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness. . . " in decisions made about the individual. 52 U.S.C. § (e)(5).

[180] 5 U.S.C. § 552A(G)(4).

[181] 5 U.S.C. § 552a(g)(1)(D).

[182] *See* 5 U.S.C. § 552a(o)(1)(A)-(D).

[183] *See* 5 U.S.C. § 552a(o)(2).

[184] *See* 5 U.S.C. § 552a(o)(1)(A)-(D).

[185] *See* Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681 (1994).

port unless it is verified.[186] The FCRA is based on the presumption that CRA' require no pre-collection consent in accepting consumer information from the data subject's creditors. While consent under Article 7(a) is the preliminary basis for legitimizing data processing, the Directive implies that records can be collected without consent for specified purposes.[187]

The presumption made in FERPA is that data was voluntarily surrendered by the student during the application process and matriculation at the educational institution. Consequently, there is no need to provide restrictions to collection. Due to the other protections provided, the absence of any limitation on the right to collect information does not destroy FERPA's adequacy under the Directive.

4. *Restrictions on Secondary Use*[188]

Article 14(b) of the Directive provides that the opportunity to object to disclosure must have been offered to the data subject before personal data is either disclosed to third parties or the data is used for direct marketing purposes. The PA, on the other hand, requires that information not be used for any purpose other than that for which it was collected.[189] It also provides twelve exemptions to confidentiality,[190] that mirror the principles relating to "the reasons for making data processing legitimate" under Article 7.[191] PA exemptions 1, 4, 7, 9, 10 and 11 could be categorized as falling under the Directive article 7(e) type; PA exemptions 5 and 6 could fall under Directive Arti-

---

[186] *See* 15 U.S.C. § 1681.

[187] Directive, art. 7(b)-(f).

[188] Secondary use refers to the use of the information for a purpose other than that for which the data was collected from the data subject.

[189] *See* 5 U.S.C. § 552a(1).

[190] *See* 5 U.S.C. §§ 552a(b)(1)-(12). The data is exempt from confidentiality if the proposed disclosure is 1) to officers and employees of the agency needing the records for the performance of their duties; 2) required under the FOIA; 3) for routine uses under 5 U.S.C. § 552a(a)(7); 4) to the Census Bureau; 5) for bona fide statistical research using non-identifiable information; 6) to National Archives and Record Administration for a record having historical value; 7) to an instrumentality of government for civil or criminal law enforcement activity; 8) for health, safety or preservation of the individual; 9) to either House of Congress or committee to the extent of matter within its jurisdiction; 10) to the comptroller general in the course of the performance of his duties; 11) pursuant to a court order; or 12) to a consumer reporting agency pursuant to 31 U.S.C. § 3711.

[191] Directive, art. 7(a)-(f). *See* discussion on these provisions *supra* part III. A.

cle 7(f); and PA exemption 8 could be described as a Directive Article 7(d)-type reason.[192] Even if the PA exemptions did not satisfy the adequacy requirements of the Directive, the data transfer could most likely occur under the derogations of Article 26.[193]

Two exemptions are problematic for the PA passing Directive muster. PA exemption (2) allowing for disclosure of data if disclosure is required by FOIA has already been discussed.[194] The other significant limitation of the PA, however, is its exemption (3) allowing for disclosure "for routine uses."[195] Routine use is defined in the PA to mean "use of such record for a purpose which is compatible with the purpose for which it was collected."[196] In theory, the routine use exemption restricted the scope of disclosure and "adequately" protected the privacy of the individual. In practice, however, the agencies used this exemption as a broad grant of disclosure.[197]

This exemption was used to justify a staggering number of data matching activities.[198] This practice combined with two other factors to render the PA's protections illusory.[199] Unlike the Directive, the PA did not require the agency to restrict the use of the information upon its transfer to a third party.[200] In

---

192 *See* 5 U.S.C. § 552a(b)(1)-(12).

193 Directive, art. 26(1). The derogations are substantially similar to the provisions allowing processing under article 7. *See* Directive *supra* note 15, art. 7.

194 *See* discussion *supra* part III. A.

195 5 U.S.C. § 552a(b)(3).

196 5 U.S.C. § 552a(a)(7).

197 This abuse of the exemption was criticized by both the government and by the courts. *See, e.g.,* PRIVACY PROTECTION STUDY COMM'N, THE PRIVACY ACT OF 1974: AN ASSESSMENT 91-93 (1977); HOUSE COMM'N ON GOVERNMENT OPERATIONS, WHO CARES ABOUT PRIVACY, OVERSIGHT OF THE PRIVACY ACT OF 1974, by the Office of Budget and Management and by Congress, H.R. Doc. No, 98-455, 98th Cong. 1st Sess. 41-53(1983); Britt v. Naval Investigative Services, 866 F.2d. 544 (3d Cir. 1989); Swenson v. United States Postal Services, 890 F.2d 1075, 1078 (9th Cir. 1989); Edison v. Dept. of the Army, 672 F.2d 840, 846 (11th Cir. 1982).

198 A survey of a limited number of authorized data matching programs reported that matches involving approximately seven billion records were performed in a five year period. SENATE COMM. ON GOV'T. AFFAIRS, THE COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1987, S. Rep. No. 516, 100th Cong., 2d Sess. 5 (1988). Congress attempted to plug this hole by the enactment of the CMPPA. *See* discussion *infra* part III.

199 *See* DAVID FLAHERTY, PROTECTING PRIVACY in SURVEILLANCE SOCIETIES 323 (1989).

200 Directive, art. 6. "1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit, and legiti-

addition, there was no requirement that a requesting party establish a legitimate need for the information before it was turned over.[201] The "routine use" exemption needed to be substantially tightened if the PA was to meet the adequacy standard of the Directive on secondary disclosure.[202]

In the attempt to eliminate the "data matching" loophole created by the "routine use" exemption, Congress enacted the CMPPA.[203] Its specific purpose was to restrict the government's ability to collect data concerning individuals by "matching" data held by one agency with data held by a different agency or other source.[204] The broad information collection opportunity of data matching had effectively circumvented the PA's consent requirement.

The CMPPA imposed a series of pre-matching requirements to answer the apparent deficiencies. As a prerequisite to performing a match, a requesting agency had to enter into a written agreement with the source. The agreement had to specify the legal authority for the match, the purpose and justification for the match, describe the records that would be searched,

---

mate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide adequate safeguards . . . [i]t shall be for the controller to ensure that paragraph 1 is complied with." *Id.*

201 See discussion *infra* part III. D. 4.

202 Congress did attempt to address the deficiencies of this exemption in a 1991 proposed Bill, which would have amended the PA in two respects: Define routine use to mean a purpose "which is necessary for the purpose for which the record is collected." *See* Privacy Act Amendments of 1991, H.R. Res. 2443, 102nd Cong. (1991). The other proposed amendment would have prohibited the use of the Federal Register as a means of noticing "routine use." *See* 137 CONG. REC. H3451 (daily ed. May 22, 1991) (This measure did not pass.).

203 Until its enactment, the matching of data was considered by many agencies a "routine use." *See* OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC RECORD SYSTEM AND INDIVIDUAL PRIVACY 57 (1986).

204 "[T]he term 'matching program'— (A) means any computerized comparison of— (i) two or more automated systems of records or a system of records with non-Federal records for the purpose of— (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or (II) recouping payments or delinquent debts under such Federal benefit programs . . ." 5 U.S.C. § 552a(a)(8). *See generally* Comment, *The Computer Matching and Privacy Protection Act of 1988: Necessary Relief From the Erosion of the Privacy Act of 1974*, 2 SOFTWARE L.J.391 (1988).

and specify the procedures for verifying the accuracy of the information used in the match.[205] The agency was also required to give notice to the public that a match was going to be done or revised.[206]

Unlike the Directive's Article 14, the CMPPA did not give the individual the power to prevent or object to a proposed match.[207] The propriety of the match was to be determined and monitored internally by the agency's Data Integrity Board.[208] As an ultimate oversight function, the Board reports the agency's matching activities to the Office of Budget and Management once each year.[209]

The CMPPA did, however, create post-match protections for the individual by requiring the agency to do an independent check of information before taking adverse action.[210] The agency was also required to issue "notice . . . containing a statement of its findings and informing the individual of the opportunity to contest such findings."[211] The standard of adequacy should not be construed to require identical protections in a third country. Assuming that the abuse of the "routine use" exemption can be curtailed, pre-match notice to the individual may not be crucial to the protection of the individual's informational privacy. Of more importance would be notice to the individual that adverse information exists and his ability to correct the inaccuracy before it can be used to his detriment. Therefore, the post-match notice and access provisions of the CMPPA should be considered as meeting the requirement of "adequacy."

The FCRA is based upon the secondary use of personal information. Reports are generated from information collected pursuant to activities between the individual and creditors or government. It would be rare if the data subject had direct in-

---

205 5 U.S.C. § 552a(o)(1)(A)-(D)(1996).

206 *See id.* The notice is not given to a specific individual, but rather is a general notice printed in the Federal Register no less than 30 days before the match is conducted.

207 The Data Integrity Board was to conduct a cost-benefit analysis to determine and document "the justification of the program and any anticipated results including a specific estimate of any savings" made because of the performance of the match. 5 U.S.C. § 552a(o)(B)(1996). Directive, art 14(a)(b).

208 5 U.S.C. § 552a(u)(3)(A)(C)(1994).

209 5 U.S.C. § 552a(u)(3)(D)(1994).

210 5 U.S.C. § 552a(o)(1)(E), (p)(1)(A)(I)(1996).

211 5 U.S.C. § 552a(p)(3)(A)(1996).

volvement with the consumer reporting agency. The FCRA does require that use of consumer reports and investigative consumer reports are limited to "legitimate business need."[212] Unfortunately, the term "legitimate business need" is not defined in the statute and there are few checks on the legitimacy of a request. Another failing of FCRA is the post-adverse effect notice provided by the statute.[213]

Under FERPA, express written consent is required before disclosure can be made to a third party.[214] The consent must specify the records to be released and the purpose for the disclosure.[215] Disclosure, without consent, may be made pursuant to a subpoena, but, not without notice to the student in advance of compliance.[216] There are other permissible disclosures pursuant to authority vested in the collector.[217] The consent provisions of FERPA most resemble the consent requirement of the Directive. FERPA's allowance of disclosure without consent mirrors the permissible sans-consent provisions of the Directive. This satisfies the adequacy standard of the Directive.

IV. CONCLUSION

The panoply of U.S. data protection laws is still developing. Despite the variances in protections afforded by the different provisions considered, many will be said to meet the adequacy requirements in some circumstances. As long as the U.S. refuses to consider an omnibus approach to data protection, each statute will have to be amended separately. There may not be a serious blockage in transborder data flows between the U.S. and E.U. nations, however, because of the broad ability for the parties to contract between themselves as to parameters of the data exchange. Despite this, it is clear that the E.U.'s vision of data processing protections for individuals is far more developed than that of the U.S. Recently, the office of the National Information Infrastructure filed a notice and request for comments on draft principles which were to update the Code of Fair

---

212 *See* Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681b (1994).

213 15 U.S.C. § 1681 (1984).

214 *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(5)(A)(B) (1994).

215 *See* 20 U.S.C. § 1232(g).

216 *See* 20 U.S.C. § 1232(g).

217 *See* 20 U.S.C. § 1232g(3)(B).

Information Practices developed in the 1970's.[218] This notice demonstrates a federal awareness that the U.S. may be lagging behind in the full use of the information economy's resource. We can be hopeful that the issues raised by that inquiry will result in substantive changes in federal law.

[218] National Information Infrastructure; Draft Principles for Providing and Using Personal Information and Commentary, 60 Fed. Reg. 4362 (Office of Management and Budget 1995)(notice).