Fordham Law Review

Volume 60 | Issue 6 Article 9

1992

The Privacy Obstacle Course: Hurding Barriers to Transnational Financial Services

Joel R. Reidenberg

The Privacy Obstacle Course: Hurding Barriers to Transnational Financial Services

Cover Page Footnote

Professor Reidenberg prepared this paper for a lecture on Aprul 2, 1992 at the Fordham University School of Law to the Graduate Colloquium on "Transnational Financial Services in the 1990s." He thanks Stewart Dresser and Malcom Norris for their helpful comments. Professor Reidenberg is grateful for the generous support of a Fordham University Faculty Research Grant Award and a grant from the Fordham Law School. Rori Wender, FLS'93, provided able and valuable research assistance for the project.

THE PRIVACY OBSTACLE COURSE: HURDLING BARRIERS TO TRANSNATIONAL FINANCIAL SERVICES

*JOEL R. REIDENBERG**

Professor Reidenberg addresses the challenge to transnational financial services resulting from national regulation of information processing. National laws around the world seek to define fair information practices for the private sector and contain prohibitions on data transfers to foreign destinations that lack sufficient privacy protection. The effect of these laws for the financial services industry is significant because financial services depend on personal information. Professor Reidenberg argues that the international attempts to harmonize information practice standards and the national efforts to regulate information processing encourage divergence of national standards for financial services. He argues that regulatory flexibility and customization is necessary to support financial services and accomodate, without circumventing, divergent national standards of fair information practices. Professor Reidenberg's theme of convergence focuses on bridging national differences, rather than on harmonizing national standards. He concludes by offering a shared rule to manage regulatory differences that enables the use of a set of legal, technological and social techniques. Thus, Professor Reidenberg proposes convergence on a flexible and customized way to bridge national differences.

INTRODUCTION

IN thinking about the next decade, students of financial services tend naturally to focus on the implications that a transnational marketplace has for the regulation of the banking, securities, and insurance industries.[1] As a consequence, recent international trade negotiations seek to

 Associate Professor of Law, Fordham University School of Law. A.B., Dartmouth 1983; J.D., Columbia 1986; D.E.A. dr. int'l éco., Univ. de Paris I (Panthéon-Sorbonne) 1987.

Professor Reidenberg prepared this paper for a lecture on April 2, 1992 at the Fordham University School of Law to the Graduate Colloquium on "Transnational Financial Services in the 1990s." He thanks Stewart Dresner and Malcolm Norris for their helpful comments. Professor Reidenberg is grateful for the generous support of a Fordham University Faculty Research Grant Award and a grant from the Fordham Law School. Rori Wender, FLS '93, provided able and valuable research assistance for the project.

1. *See* Doty, *The Role of the Securities and Exchange Commission in an Internationalized Marketplace*, in Annual Survey of Financial Institutions and Regulation, Transnational Financial Services in the 1990s, 60 Fordham L. Rev. S77 (1992); Felsenfeld, *The Compatibility of the UNICITRAL Model Law on International Credit Transfers with Article 4A of the UCC*, in Annual Survey of Financial Institutions and Regulation, Transnational Financial Services in the 1990s, 60 Fordham L. Rev. S53 (1992); Lichtenstein, *U.S. Restructuring Legislation: Revising the International Banking Act of 1978, For the Worse?*, in Annual Survey of Financial Institutions and Regulation, Transnational Finan-

create a more harmonized regulatory environment for financial services.[2] These initiatives generally seek convergence on liberalization of national laws.

Global electronic networks for financial services blur the boundaries of these traditional regulatory frameworks.[3] As an astute European once observed, "in the final analysis, the financial system is a network of information."[4] In essence, information processing is a basic component of financial services.[5] Financial services depend on personal information and create significant information about individuals.[6] Traditional banking functions such as money transmission and credit extension require sensitive and detailed information about individuals, while the transaction records from these functions create important sources of personal information.[7] These transaction records provide significant information about an individual's life and lifestyle.[8] Similarly, insurance services are

---

cial Services in the 1990s, 60 Fordham L. Rev. S37 (1992); Malloy, *Bumper Cars: Themes of Convergence in International Regulation*, in Annual Survey of Financial Institutions and Regulation, Transnational Financial Services in the 1990s, 60 Fordham L. Rev. S1 (1992); Shirley, *The What, Why and How of Privatization—A World Bank Perspective*, in Annual Survey of Financial Institutions and Regulation, Transnational Financial Services in the 1990s, 60 Fordham L. Rev. S23 (1992); Tekinalp, *Turkey's New Financial Leasing Law and Industry*, in Annual Survey of Financial Institutions and Regulation, Transnational Financial Services in the 1990s, 60 Fordham L. Rev. S117 (1992); Wegen, *Transnational Financial Services—Current Challenges for An Integrated Europe*, in Annual Survey of Financial Institutions and Regulation, Transnational Financial Services in the 1990s, 60 Fordham L. Rev. S91 (1992).

2. During the Uruguay Round negotiations within the General Agreement on Tariffs and Trade, policy-makers have sought to include services in the negotiations. *See General Agreement on Tariffs and Trade: Ministerial Declaration on the Uruguay Round of Multilateral Trade Negotiations*, Sept. 20, 1986, 25 I.L.M. 1623, 1627. Themes of convergence may also be found in the recent Free Trade Agreements and multinational banking policies. *See* Free Trade Area Agreement, Apr. 22, 1985, U.S.-Isr., 24 I.L.M. 653, 679-81; Free Trade Agreement, Jan. 2, 1988, U.S.-Can., 27 I.L.M. 281; B.I.S. Comm. on Banking & Supervisory Practices, *Consultative Paper on International Convergence of Capital Measurement and Capital Standards*, 30 I.L.M. 967, 967 (1991); Malloy, *supra* note 1, at S14-20.

3. *See* R. Bruce, J. Cunard & M. Director, The Telecom Mosaic 265 (1988).

4. C. Goldfinger, La Géofinance 401 (1986).

5. *See* Fascell & Schlundt, *United States International Communications and Information Policy: A Crisis in the Making?*, 5 Nw. J. Int'l L. & Bus. 486, 490-94 (1983) (the authors were the chairman and staff director, respectively, of the Committee on Foreign Affairs, U.S. House of Representatives).

6. *See* Berkvens, *Payment Systems Meet the EC Data Protection Initiative*, Int'l Fin. L. Rev., Aug. 1991, at 33.

7. Opening a deposit account routinely includes the disclosure of a client's social-security number, home address, work address, telephone numbers, and wealth. Obtaining credit requires an individual to disclose among other information, financial and employment histories. *Cf. Citicorp Plan to Sell Credit Card Information Stirs Controversy about Consumer Privacy*, Wall St. J., Aug. 22, 1991, at 22 (transaction records are valuable commercial assets).

8. For example, records from a checking account or credit card reveal a client's commercial relationships and personal habits or preferences. *See* J. Bing, Reflections on a Data Protection Policy for 1992, at 4 (paper presented to conference on "Legal Challenges and Opportunities Created by the Prolific Growth of Electronic Information Serv-

information-intensive. Life and health insurance providers must collect and use detailed information about an insured's medical history. Casualty insurers must collect sensitive information about the value of insured personal assets. Even brokerage services require the processing of personal information and provide details on the lives of individuals.

Financial networks "transnationalize" personal information.[9] The technology creates "global products" and "global services."[10] Banking and payment systems involve significant international flows of personal information such as transaction records.[11] The regulation (or lack of regulation) of information processing has a critical impact on the evolution of transnational financial services.

As the international economy transnationalizes, there has been a failure to achieve a multilateral consensus for the framework necessary to promote global information services.[12] There are competing international instruments for data processing, and each effort to promote uniform international standards for data processing has failed.[13] Many European countries, including France, Denmark, Germany, the Netherlands, and the United Kingdom, have broad data processing statutes that apply information privacy principles to industry, including the financial services sector.[14] These national laws do not adopt identical norms. Among

---

ices," organized jointly by the Council of Europe and the Commission of the European Communities, Luxembourg, March 27-28, 1990) (on file with the *Fordham Law Review*).

9. *See* Goldfinger, *supra* note 4, at 287-91; Eger, *The Global Phenomenon of Teleinformatics: An Introduction*, 14 Cornell J. Int'l L. 203, 205 (1981) [hereinafter *Teleinformatics*]; Fascell & Schlundt, *supra* note 5, at 489-91; Herman & Halvey, *International Flow of Data Is Threatened*, Am. Banker, Sept. 25, 1990, at 12.

10. *See* Gassman, *Vers un cadre juridique internationale pour l'informatique et autres nouvelles techniques de l'information*, in 1985 Annuaire francais de droit international (Centre national de la recherche scientifique) 747.

11. *See* Berkvens, *supra* note 6, at 33; Herman & Halvey, *supra* note 9, at 12.

12. *See* Gassman, *supra* note 10, at 748; Kirby, *Legal Aspects of Transborder Data Flow*, 11 Computer/L.J. 233, 242-43 (1991).

13. *See infra* text accompanying notes 29-162.

14. *See* Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law No. 78-17 of Jan. 6, 1978 concerning data processing, records and freedom], J.O. du 7 janvier et rectificatif au J.O. du 25 janvier [hereinafter French Law]; The Danish Private Registers Act, No. 293, June 8, 1978, *amended by* Act No. 383, June 10, 1987, *translated in* Danish Ministry of Justice, Pub. No. 622 (Oct. 2, 1987) [hereinafter Danish Law]; Wet Persoonsregistraties [Act of Dec. 28, 1988, providing rules for the protection of privacy in connection with personal data files], Stb. 1988, at 665, *translated in* Council of Europe Doc. CJ-PD (89) 4 (Jan. 27, 1989), *reprinted in* A. Nugter, Transborder Flow of Personal Data Within the EC 397-410 (1990) [hereinafter Dutch Law]; Bundesdatenschutzgesetz (BDSG), *translated in Germany: Federal Data Protection Act 1991*, Council of Europe Doc. CJ-PD (91) 30 (12 July 1991) [hereinafter German Law]; U.K. Data Protection Act 1984, *reprinted in* A. Nugter, *supra*, at 365-95 [hereinafter British Law]; *see also* Nugter, *supra* note 14 (analysis of the French, Dutch, British and superseded German laws); Evans, *European Data Protection Laws*, 29 Am. J. Comp. L. 571, 578-80 (1981); *Data Protection Roundup*, Privacy L. & Bus., July 1991, at 2-7 (summarizing the status of data protection legislation in 31 countries). A recent draft directive on data protection issued by the Commission of the European Communities has also increased attention to privacy protection. *See* Proposal for a Council Directive concerning the pro-

other things, these laws permit national authorities to prohibit transfers of personal information such as credit card or insurance data to countries without sufficient privacy protection. In North America and Asia, different approaches are used to deal with privacy issues.[15] Recently, several foreign governments have restricted the transmission of personal information to countries perceived as ignoring computer privacy concerns.[16] For transnational financial services, differences between national information processing regulations and the treatment of data exports creates an obstacle course for transnational service providers that is increasingly hazardous.

Although the financial services industry has noted the importance of information privacy regulation, data processing rules are just beginning to appear on the international trade agenda, though rarely in a prominent position.[17] The recent free trade agreements, for example, do not address these issues, and the Uruguay Round of GATT negotiations has only recently taken tentative steps to include privacy matters.[18] The privacy dimension poses a major challenge for regulatory policy and significant hurdles for the development of transnational financial services.[19]

The thesis of this Article is that the search for international harmonization of national information practice laws has been elusive; that national fair information practices are evolving—particularly in the context of financial services; and, that therefore, the appropriate evolution for

---

tection of individuals in relation to the processing of personal data, Eur. Comm. Doc. COM 314 final—SYN 287 (Sept. 13, 1990) [hereinafter Draft EC Directive].

15. *See infra* text accompanying notes 66-96.

16. Norway, Austria, Germany, and Sweden have each imposed restrictions on international data flows because of privacy concerns. *See Compte rendu de la onzième conférence des commissaires à la protection des données (Berlin, 29-31 aout 1989) in* C.N.I.L., 10e Rapport d'activité 308-09 (1990) [hereinafter *Compte rendu*]. France has restricted the transfer of personal information to Italy, Belgium, Switzerland, and the United States on privacy grounds. *See infra* notes 178-80. The United Kingdom has also blocked a data transfer to the United States. *See infra* note 183.

17. *See, e.g.*, Drake & Nicholaidis, *Ideas, Interests and Institutionalization: "Trade in Services" and the Uruguay Round*, 46 Int'l Org. 37, 47-48, 89 (1992) (data protection appears sporadically on the trade agenda); *Regulation of Financial Services Ten Global Issues*, 18 AMEX Bank Rev, Apr. 3, 1991, at 7 (privacy is mentioned as a peripheral issue).

18. *See* Free Trade Area Agr., Apr. 22, 1985, U.S.-Isr., 24 I.L.M. 653; Free Trade Agr., Jan. 2, 1988, U.S.-Can., 27 I.L.M. 281.

Initially, the Uruguay Round mandate for GATT negotiations on services did not mention data processing or privacy. *See General Agreement on Tariffs and Trade: Ministerial Declaration on the Uruguay Round of Multilateral Trade Negotiations*, Sept. 20, 1986, 25 I.L.M. 1623, 1627. Subsequently, negotiators have debated including a mention of privacy issues in either the telecommunications annex or in a framework agreement. In either case, the treatment of the issues will be rather general.

19. This Article will focus generally on cross-border banking and will use occasional examples from the insurance and securities fields. A detailed treatment of each type of financial service activity and its privacy implications would necessitate an entire series of articles. This Article will also be confined to fair information practices in the private sector and will not address public sector issues such as the controls on government access to and use of personal information related to financial services.

the regulatory obstacles to transborder flows of personal information must allow flexibility and regulatory customization to accommodate divergent protection without circumventing privacy goals. This theme of convergence shifts the debate to shared rules for the management of regulatory differences rather than continuing the "dialogue de sourds" on a shared set of uniform rules.

Part I of this article explores the mechanisms used to regulate information processing. It analyzes how the two international legal instruments reflect a search for fair information practices and invite non-uniform substantive and procedural standards. Part I also demonstrates that these instruments do not provide significant guidance for personal information in the financial services sector. Beyond the international efforts, this Part demonstrates that the national laws similarly reflect attempts to define rules of fair information practices. It shows that the national techniques vary substantially, and are still evolving, in the treatment of personal information. Part II analyzes various data export restrictions. This analysis shows that the requirements for data exports are not consistent and present real obstacles to cross-border financial services. Part III shows that the obstacles posed by these data export restrictions present a regulatory challenge for transnational financial services based on the difficulty and complexity of comparisons among national laws. Finally, Part IV argues that the policy choices for dealing with transborder data flows in a complex, dynamically changing information marketplace requires flexibility and sensitivity toward varying methods of regulation. This flexibility calls for a particularized approach to rules on transnational fair information practices. A flexible and customized approach to regulation of information flows allows regulators to avail themselves of both legal and extra-legal tools. This Article concludes by suggesting a combination of legal, technological and societal techniques that policy-makers may use to achieve privacy satisfaction in the global information economy.

I. INSPECTING THE COURSE: REGULATORY SCHEMES FOR FAIR INFORMATION PRACTICES

For over one hundred years, legal systems have sought to define rules for the protection of information about individuals.[20] Information practices relating to both individuals and corporations are often proscribed by government regulation. In the United States, the rules are cast as a set of rights protecting individual privacy.[21] During the last century, serious attempts to define clearly the privacy right and its underlying basis have

20. These efforts to protect individual rights trace their origins to the legendary article by Samuel Warren and Louis Brandeis. *See* Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

21. The classic American formulation by Warren and Brandeis described privacy as a "right to be let alone." *Id.*

been inconclusive.[22] In the context of computer-processed information, the United States has traditionally sought, in limited ways, to define fair information practices.[23] Great importance is placed on the value of the free flow of information.[24] Essentially, these definitions seek to balance unrestrained information flows with the need to safeguard individuals from various harms that occur as a result of overly free flows of information.

Europeans have similarly sought to identify the sphere of control or protection that individuals may have regarding personal information. Some European countries include information about legal persons within the sphere of protection.[25] Europeans refer to such rights as "data protection" rather than privacy.[26] The European philosophy derives from a strong belief in "information self-determination."[27] As in the American privacy concept, data protection seeks to achieve a set of fair information practices. In general, Europeans emphasize human rights concerns.[28]

---

22. *See, e.g.*, Restatement (Second) of Torts § 652A comment c (1977) (privacy is divided into four categories with none "exclud[ing] the possibility of future developments"); A. Westin, Privacy and Freedom 7 (1967) (arguing for an individual's right to control personal information: "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."); Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 962 (1964) (arguing that privacy protects human dignity and noting that, despite the many cases founded on privacy, confusion persists as to what the right protects); Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 Law & Contemp. Probs. 326, 327-28 (1966) (criticizing the protection of privacy in tort law, in part, because of its open-ended nature); Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 Mich. L. Rev. 1089 (1969) (arguing that privacy means the control of flows of information and that legal notions of privacy are inadequate in dealing with the problems of computerization); Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 393 (1978) (noting the "concept of 'privacy' is ill defined and has an economic foundation). *See generally* Fried, *Privacy*, 77 Yale L.J. 475 (1968) (arguing that privacy is the right to define one's self for others); Prosser, *The Right of Privacy*, 48 Cal. L. Rev. 383 (1960) (attempting to catalog and define interests protected by privacy).

23. *See* U.S. Privacy Protection Study Comm'n, *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission* 10-11 (1977) [hereinafter *Privacy Report*]; U.S. Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Sys., *Records, Computers, and the Rights of Citizens* (1973), *reprinted in Privacy Report*, *supra*, at 15 n.7; Eger, *supra* note 9, at 210-11; Reidenberg, *Privacy in the Information Economy—A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm. L. J. 195 (forthcoming).

24. *See, e.g.*, U.S. Const. amend I ("Congress shall make no law . . . abridging the freedom of speech.").

25. *See Data Protection Roundup*, *supra* note 14, at 2-7 (Austria, Denmark, Iceland, Luxembourg, and Norway protect both natural and legal persons).

26. *See* Walden & Edwards, *Data Protection*, in Computer Law 198, 200-02 (Chris Reed ed. 1990).

27. *See* Judgment of the First Senate (Bverfge, Karlsruhe, Dec. 15, 1983) *translated in* 5 Hum. Rts. L.J. 94 (1984) (landmark census case in the German Federal Constitutional Court ruling that the 1977 German statute on information privacy was unconstitutional because it did not adequately recognize information self-determination).

28. The early European interest in data protection derived from the desire of human rights advocates to adapt the European Human Rights Convention to the computer age.

At the international level, two major attempts tried to define fair information practices on a global basis: the Organization for Economic Cooperation and Development (the "OECD") sought to establish norms, and the Council of Europe created legal standards.[29] The attempts faced the classic challenge of accommodating different national techniques and concepts.[30] While the two efforts approached the transnationalization of information from different perspectives,[31] the underlying tension between human rights concerns and free flows of information framed the harmonization attempts with a similar set of issues for fair information practices. Neither of the international efforts sought specifically to regulate financial services, yet each has a direct effect on the regulation of transnational financial services. Despite the efforts, no international consensus emerged on obligatory standards. National techniques remain critical for fair information practice standards. These techniques, too, have a direct effect on financial services, and the diversity poses a challenge for the development of transnational financial services.

A. *International Objectives*

In 1980, the Organization for Economic Cooperation and Development promulgated voluntary guidelines for the protection of privacy and transborder data flows (the "OECD Guidelines").[32] The following year, the Council of Europe opened for signature a convention on data processing and privacy (the "European Convention").[33] While neither of the documents deals explicitly with financial services, each tries to enun-

---

See, e.g., Walden & Edwards, *supra* note 26, at 199; *Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* ¶ 4, 19 I.L.M. 282, 300 (1980) [hereinafter *Explanatory Report*]. With this history, it is curious that some European countries grant these protections to corporations and not just individuals. *See infra* text accompanying notes 104-06.

29. *See infra* notes 32-60 and accompanying text.

30. *See, e.g.*, D. Tallon, *L'harmonisation des règles du droit privé entre pays de droit civil et de common law*, R.I.D.C. 514 (1990) (explaining difficulties harmonizing common law and civil law rules).

31. *See infra* note 35-36 and accompanying text.

32. *See* Organization for Economic Co-operation & Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981) [hereinafter OECD Guidelines].

33. *See* Council of Eur., Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T.S. No. 108, *reprinted in* 20 I.L.M. 377 (1981) [hereinafter European Convention]. The Council of Europe is an intergovernmental organization that promotes human rights, including civil, political, economic and social rights. *See* Statute of the Council of Eur., May 5, 1949, art. 3, Eur. T.S. No. 1. (1968). Membership consists of twenty-six countries: Austria, Belgium, Cyprus, Czech & Slovak Federal Republic, Denmark, Finland, France, Federal Republic of Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, San Marino, Spain, Sweden, Switzerland, Turkey, and United Kingdom.

ciate standards of fair information practice for the private sector.[34]

Both instruments focus on the conflict between safeguarding privacy and free flows of information, but the drafting organizations emphasize different perspectives. The OECD Guidelines highlight that free flows of information are critical for economic development, while the European Convention stresses the need to protect individuals.[35] These differences should not be surprising; the OECD is designed to foster economic growth among industrialized nations, while the Council of Europe has as its mission the advancement of human rights.[36] In keeping with these differing perspectives, the legal nature of the two instruments varies significantly. The OECD Guidelines posit voluntary adherence and stress the development of self-regulation.[37] Signatories to the European Convention, however, are obligated to enact conforming national legislation,[38] and the treaty implicitly prefers enforcement through an administrative agency with supervisory powers.[39]

Despite the apparent differences in approach, the two instruments identify a similar set of fair information practice issues, though the instruments diverge on precise standards.[40] Each targets the processing of information about identified or identifiable individuals.[41] The European

34. *See* European Convention, *supra* note 33, § 3(1); OECD Guidelines, *supra* note 32, ¶ 2.

35. *See* OECD Guidelines, Preamble, *supra* note 32, at 422; European Convention, Preamble, *supra* note 33, at 422; Bing, *The Council of Europe Convention and the OECD Guidelines on Data Protection*, 1984 Mich. Y.B. Int'l Legal Stud. 271, 272; Cole, *New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws*, 17 N.Y.U. J. Int'l L. & Pol. 893, 901 (1985); Patrick, *Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines*, 21 Jurimetrics J. 405, 409 (1981). The explanatory memorandum issued by the Council of Europe for the European Convention also casts the debate in terms of "information power" and "social responsibility." *Explanatory Report*, *supra* note 28, ¶ 2 at 299.

36. *Compare* Statute of the Council of Eur., May 5, 1949, art. 3, Eur. T.S. No. 1 (1968) (membership in the Council is predicated on acceptance of principles of human rights and fundamental freedoms) *with* Convention on the Organization for Economic Co-operation & Dev., Dec. 14, 1960, 12 U.S.T. 1728, 1730-32 (organization designed to foster economic welfare of members and promote harmonization of national laws).

37. *See* OECD Guidelines, *supra* note 32, ¶ 19.

38. *See* European Convention, *supra* note 33, § 4(1). Ten countries (Austria, Denmark, France, Federal Republic of Germany, Ireland, Luxembourg, Norway, Spain, Sweden, and the United Kingdom) have ratified the European Convention, while eight nations (Belgium, Cyprus, Greece, Iceland, Italy, Netherlands, Portugal, and Turkey) have also signed without ratification. Five members (Finland, Liechtenstein, Malta, San Marino, Switzerland) have not signed the treaty at all. *See* Council of Eur., *Chart of Signatures and Ratifications*, Jan. 8, 1990 (on file with the *Fordham Law Review*); *Data Protection News from Around the World*, Privacy L. & Bus., Aug. 1990, at 2.

39. *See* European Convention, *supra* note 33, § 13(2)(a).

40. *See generally* Bing, *supra* note 8 (describing the differences between the two instruments); Cole, *supra* note 35, at 896-900 (discussing background to both instruments); Eger, *supra* note 9; Patrick, *supra* note 35 (also comparing the OECD Guidelines and the European (draft) convention).

41. *See* OECD Guidelines, *supra* note 32, ¶ 1(b); European Convention, *supra* note 33, § 2a. The European Convention further permits signatories to apply the principles to

Convention is broader in that it expressly allows the application of the principles to legal persons.[42] Financial services are affected by the application of fair information practice regulation to data about corporations as well as individuals.

The OECD Guidelines and the European Convention focus generally on data processing activities, though neither is limited to computer-processed information.[43] Both set forth policies on data collection,[44] use of personal information,[45] storage of personal information,[46] and transmission and dissemination of personal information.[47] Unlike the OECD Guidelines, the substantive rights and obligations in the European Convention represent the minimum level of protection that signatories must

---

legal persons as well as non-computerized record systems. *See* European Convention, *supra* note 33, § 3(2)b-c.

42. *Compare* European Convention, *supra* note 33, § 3(2)(b) (signatories must give notice if the European Convention principles protect legal persons) *with* OECD Guidelines, *supra* note 32, ¶ 1(b) (the guidelines do not prevent the protection of legal persons). *See also* Grossman, *Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations*, 4 Nw. J. Int'l L. & Bus. 1 (1982) (arguing that it is inappropriate to protect legal persons in the same manner as individuals).

43. The European Convention refers to personal data undergoing automatic processing, though signatories may apply the protections to manual record systems. *See* European Convention, *supra* note 33, § 3(2)(c). The OECD Guidelines indicate that principles may also be applied to non-automatic processing of personal data. *See* OECD Guidelines, *supra* note 32, ¶ 2(c). This distinction is of minor significance for transborder financial services.

44. The instruments deal with the manner of data collection. *See* OECD Guidelines, *supra* note 32, ¶ 7 (data must be obtained lawfully and fairly, with consent of the data subject where appropriate); European Convention, *supra* note 33, § 5(a) (personal data shall be obtained and processed fairly and lawfully). Each calls for a right of access to stored information. *See* OECD Guidelines, *supra* note 32, ¶ 13a (individual has right to know of existence of data collection); European Convention, *supra* note 33, § 8a (individuals should receive notice of data collection). Each places a limitation on unnecessary or overly intrusive collections of personal information. *See* OECD Guidelines, *supra* note 32, ¶ 8 (setting forth a relevancy test); European Convention, *supra* note 33, § 5c (setting forth a test of adequacy and relevancy). Both documents emphasize the importance of data accuracy. *See* OECD Guidelines, *supra* note 32, ¶ 8 (data should be "accurate, complete and kept up-to-date); European Convention, *supra* note 33, § 5d (data should be "accurate, and where necessary, kept up-to-date").

45. *See* OECD Guidelines, *supra* note 32, ¶¶ 9-10 (personal data should not be used for purposes other than those specified to the data subject at the time of collection, unless consent has been granted); European Convention, *supra* note 33, § 5b (data may not be used in a way incompatible with specified purposes).

46. *See* European Convention, *supra* note 33, § 5e (limits duration of storage).

47. *See* OECD Guidelines, *supra* note 32, ¶ 10 (personal information should not be disclosed except for legitimately specified purposes); European Convention, *supra* note 33, § 5(a)-(b) (limits disclosures of personal information if not in furtherance of legitimate processing).

Another aspect also covered by both documents is a security requirement to prevent unintended disclosures or unwanted access to personal information. *See* OECD Guidelines, *supra* note 32, ¶ 11 ("[p]ersonal data should be protected by reasonable security safeguards"); European Convention, *supra* note 33, § 7 (appropriate security measures should be taken for personal data). Because these measures relate to third party interference with personal information and not to fair information practices of the data user per se, this Article will not give specific consideration to security issues.

enact into national legislation.[48] Ironically, the convention, thus, invites disharmony of substantive standards that go beyond the minimum level. For example, the European Convention recognizes a need for countries to adopt additional safeguards that protect certain types of data such as race, health, and sexual preferences or activity information.[49] These must be adopted on a national level. As a result, signatories are encouraged to have different levels of protection for sensitive data. In the context of financial services, this particular ambiguity over specific standards of protection can have special significance. For certain insurance services dependent on actuarial data, these restrictions may pose critical problems—namely satisfying different levels of protection on a cross-border basis.

The generality of the rights and obligations in both the OECD Guidelines and European Convention can be troublesome generally for transnational information services and specifically for transnational financial services. In particular, the assumptions underlying these instruments may be anachronistic for complex financial service information processing. For example, any information that relates to an identifiable person is covered under the two instruments. However, often, personal information for financial services is encrypted or coded with account numbers or administrative numbers. In these instances, linking the information to a particular person may be difficult, if not impossible, for various participants processing the data. In addition, each of the international instruments imposes the fair information practice obligations on the "controller" of personal information.[50] This means the ability to determine the content and use of personal information. In the context of sophisticated computer networks and global telecommunications linkages, there may be several entities that simultaneously "control" the personal information, or there may be no single entity that "controls" the personal information.[51] The European Convention is also founded on the notion that information transfers will be discrete transactions.[52] For financial services, distributed databases may mean that personal information is shared and created regardless of borders.

48. *Compare* OECD Guidelines, *supra* note 32, ¶ 19 (OECD member countries "should establish" privacy rules to implement guidelines) *with* European Convention, *supra* note 33, § 4 (signatories "shall take the necessary measures in its domestic law" to implement the principles).

49. *See* European Convention, *supra* note 33, § 6.

50. *See* European Convention, *supra* note 33, § 2(d); OECD Guidelines, *supra* note 32, ¶ 1(a).

51. For example, in the case of a credit card transaction, personal information will be handled by several entities, including the retailer, network processor, card brand processor, and card issuing bank. Each may have some control over the data, but it may only be the card issuer that controls the linkage between the processed numbers and the cardholder's identity. The retailer, though, may have control over certain name-linked information, such as the customer's identity and credit card holdings.

52. *See* European Convention, *supra* note 33, § 12(1) (referring to "transfers" across borders).

The ambiguity of these principles ineluctably leads to asymmetry in implementation for financial services. Although the OECD Guidelines emphasize sectoral codes of conduct, the elaboration of such codes is left to industry without any government or OECD supervision.[53] Industry groups have rarely developed such codes and have incentives to develop minimal standards when fair information practices are addressed. The European Convention provides an interpretive mechanism for specific sectoral applications under the aegis of a consultative committee, rather than representatives from the concerned industries.[54] This promotes limited consideration of the industry perspective and is more likely to result in stricter standards. Because the purpose is to promote consistent national interpretations of the treaty principles, the consultative committee's interpretations are only hortatory and do not bind national authorities who may give greater weight to the industry view.

Following the OECD approach, industry groups in several countries have, nevertheless, sought to develop codes of fair information practices for financial services.[55] Only one recommendation has been issued for financial services through the European Convention process. It covers payment and other related operations.[56] The recommendation takes a very restrictive view of permissible data processing activities for personal information gathered in relation to payment operations such as fund transfers and credit card transactions.[57] The recommendation, for example, severely limits the internal use by a financial institution of client information.[58] The recommendation also limits the external disclosures, use and matching of data collected during the course of payment operations. A financial institution may not, for example, use, or cross-match personal information for marketing purposes, either for its own account or for third parties.[59] Personal information acquired in connection with

53. *See* OECD Guidelines, *supra* note 32, ¶ 19(b).

54. *See* European Convention, *supra* note 33, §§ 18-19. Section 18 establishes a consultative committee and section 19 authorizes it to express opinions on the application of the convention. The consultative committee does have limited industry participation through a representative with observer status from the International Chamber of Commerce.

55. *See infra* notes 86-87 and accompanying text.

56. *See* Council of Eur., Recommendation R(90)19 on the Protection of Personal Data Used for Payment and other Related Operations (Sept. 13, 1990) [hereinafter Recommendation R(90)19].

57. *See* Berkvens, *supra* note 6, at 33. *But see* Bourland, *La Sauvegarde de la vie privée dans les transferts électroniques de fonds* 1991 Droit de l'informatique & des télécoms 17, 25-27.

58. *See* Recommendation R(90)(19), *supra* note 56, app. ¶ 3.4 (restricts the permissible purposes for the collection and storage of personal data to verifying identity and determining the validity and lawfulness of the payment transaction). The Recommendation takes a more flexible view of the data that constitutes "personal information". It does not apply to data that can be associated with an individual only through unreasonable amount of time, cost, and manpower. *See id.* app. ¶ 1.2. This definition differs from the European Convention. *See* European Convention, *supra* note 33, § 2(a).

59. An individual must be notified in writing and must consent prior to the use of transaction information for direct marketing purposes. *See* Recommendation R(90)(19),

payment operations may not be communicated to third parties for marketing or other non-payment purposes without an affirmative consent.[60]

These two instruments, though attempting to harmonize national regulatory standards for fair information practices, encourage differences over the issues of fair information practices in the financial services context.

B. *National Objectives*

While the OECD Guidelines are perceived as making some contribution to international harmonization of fair information practice issues,[61] and the European Convention strives to develop uniform standards, the national treatment of fair information practices continues to diverge rather than converge. Some of the national techniques pre-date the two international efforts,[62] and those more recent national enactments refine the implementation of fair information practice standards in dissimilar ways.[63] Even the European Convention by its terms does not create uniform, self-executing rights or obligations.[64]

Essentially, two approaches have been taken at the national level. Some countries, such as the United States, treat data privacy issues on an ad hoc basis and seek to focus narrowly on particular data processing issues through sectoral laws and industry self-regulation. Others, such as France, the Netherlands, and the United Kingdom, have enacted omnibus legislation consistent with the broad stipulations in the European Convention and thereby try to regulate all data processing activities.[65]

1. The Ad Hoc Approach

Although broad concepts of privacy were first identified in the United States, the American approach to fair information practice represents the paradigm use of ad hoc techniques. There is a complex web of federal and state legislation combined with state common-law rights that seek to protect against targeted privacy abuses; constitutional rights do not address information processing activities wholly within industry.[66]

In the context of financial services, the ad hoc approach rarely addresses each of the principles of fair information identified in the OECD Guidelines and European Convention. For example, existing federal legislation in the United States addresses the treatment of personal informa-

---

supra note 56, app. at ¶¶ 4.2, 4.3. The consent, however, need not be an affirmative declaration. Notification to the individual gives rise to a presumption of consent, unless the individual objects. *See id.*

60. *See* Recommendation R(90)(19), *supra* note 56, app. ¶ 5.1(c).

61. *See* Gassman, *supra* note 10, at 750.

62. *See e.g.* French Law, *supra* note 14 (enacted in 1978).

63. *See* Dutch Law, *supra* note 14; German Law, *supra* note 14; Nugter, *supra* note 14.

64. *See* European Convention, *supra* note 33, § 4(1).

65. *See* Evans, *supra* note 14, at 578.

66. *See* Reidenberg, *supra* note 23, at 208-09.

tion for credit services,[67] debt collections,[68] and electronic fund transfer.[69] These laws do not, however, provide consistent treatment for fair information practice issues. The credit laws do not focus on serious data collection issues such as notice and consent for the collection of personal information and on the collection of unnecessary information.[70] Similarly, the credit laws do not carefully constrain the purposes for collection or use of personal information or the storage of inaccurate and obsolete information.[71] The federal regulation of electronic fund transfers targets data accuracy and does not address the other fair information practice concerns.[72] Other federal legislation does not thoroughly address the treatment of personal information for the remaining areas of financial services such as the securities industry.[73] Interestingly, in Australia, where ad hoc protection generally applies to the private sector, the public sector privacy law was recently amended to apply specifically to credit reporting activities and was not amended to apply to other financial services.[74]

At the state level in the United States, there are additional ad hoc laws governing financial services.[75] Some states include more stringent rules on data collection for credit card or check transactions.[76] State laws may also restrict disclosures of customer information by banks.[77] Insurance services are also regulated at the state level. These laws tend to govern some aspects of the collection, use, and dissemination of personal information by insurance companies, but do not generally address practices

67. *See* Fair Credit Billing Act, 15 U.S.C. § 1666 (1988); Fair Credit Reporting Act, 15 U.S.C. § 1681 (1988); Equal Credit Opportunity Act, 15 U.S.C. § 1691 (1988).

68. *See* Fair Debt Collections Practices Act, 15 U.S.C. § 1692 (1988).

69. *See* Electronic Fund Transfers Act, 15 U.S.C. § 1693 (1988).

70. *See* Reidenberg, *supra* note 23, at 210-215, 219-220

71. *See id.*

72. *See id.* at 215, 219.

73. In the securities field, the use of personal information relates to the management of customer accounts and usually is limited to transaction records. Federal securities laws do address record-keeping practices for the enforcement of the securities trading laws, but not for fair data processing uses. *See, e.g.*, Investment Advisor's Act, 15 U.S.C. § 80b-1, -21. (1988) (requiring registered investment advisers to maintain certain records on client transactions).

74. *See Australia's Privacy Commissioner Rules on Credit and Health Data*, Privacy L. & Bus., Dec. 1991, at 16-17.

75. *See* Reidenberg, *supra* note 23, at 229-31.

76. *See, e.g.*, Cal. Civ. Code § 1747.8 (West Supp. 1991); Md. Com. Law Code Ann. § 13-318 (Supp. 1991); N.Y. Gen. Bus. Law § 520-A (McKinney Supp. 1991); Wash. Rev. Code Ann. § 62A.3-512 (West Supp. 1992). These laws restrict the types of information that may be collected in connection with a credit card or check purchase. They are designed to stem credit card fraud problems. *See* Reidenberg, *supra* note 23, at 230-31.

77. *See, e.g.*, Conn. Gen. Stat. Ann. § 36-9k (West 1987); Ill. Ann. Stat. ch. 17, para. 360(c) (Smith-Hurd 1981 & Supp. 1991). Common law fiduciary obligations may also require that a bank maintain the confidentiality of customer information. *See* L.R. Fischer, The Law of Financial Privacy: A Compliance Guide ¶ 5.04[3] (2d ed. 1991). This obligation addresses the disclosure to third parties of a client's personal information and would not affect the collection, use or storage of personal information.

related to unnecessary information or to the storage of personal information.[78]

The complexity and narrow characteristic of the ad hoc approach may also be reflected by the complementary layer of state common-law rights in the United States. Four well-developed common-law rights of privacy exist: (1) the intrusion upon seclusion; (2) public disclosures of private facts; (3) publicity that places one in a false light; (4) misappropriation of one's name or likeness for a commercial purpose.[79] These rights, however, provide limited application to information processing concerns.[80] Consequently, the rights provide little guidance for fair information practices in the financial services sector.[81] In other countries, courts have similarly established particular rights. For example, the Hungarian Constitutional Court recently ruled that the Hungarian constitution bars the collection and use of the national identity numbers if there is no definite and limited purpose for the collection and use.[82]

As an alternative to sectoral legal rights, the ad hoc approach encourages self-regulation to set fair information practice standards.[83] Often, industry promotes self-regulation as a way to forestall government prescriptions for fair information practices.[84] Rather permissive, and rarely complete, standards of fair information practice result from industry self-regulation. Through this ad hoc technique, two varieties of self-regulation guide financial services activities. Some organizations chose to

78. *See* Reidenberg, *supra* note 23, at 233-34.

79. *See* Restatement (Second) of Torts § 652 (1977); Prosser, *supra* note 22, at 389. These common law rights have been codified in many states. *See* Reidenberg, *supra* note 23, at 222, 228.

80. Intrusion upon seclusion may protect only against unfair or unlawful data collections through surreptitious and intrusive means. Public disclosure of private facts may guard only against shocking disclosures to the general public of intimate personal information. Similarly, false-light publicity may protect only against the wide dissemination of inaccurate personal information. Misappropriation liability may arise from some commercial uses of personal information without consent. *See* Reidenberg, *supra* note 23, at 221-27, 234-35.

81. If a financial services company were to widely disseminate health or financial information, the tort liability might be imposed under the doctrine of public disclosure of private facts. However, the dissemination must be made to the general public and the facts must be shockingly offensive. *See* Restatement (Second) of Torts § 652D (1977). These thresholds are not likely to be met easily.

82. *See Hungary's Constitutional Court Rules Against Arbitrary Use of PINS*, Privacy L. & Bus., Dec. 1991, at 20-21.

83. *See, e.g.*, U.S. Office of Consumer Affairs, Administration Position Statement on Privacy (1991) (policy statement calls for respect by business of five basic privacy principles, but does not recommend any legal rights).

84. Industry representatives testify before congressional committees and government commissions to argue for self-regulation rather than legislative action. *See, e.g., Privacy Report, supra* note 23, at 34; *Hearing on Domestic and International Data Protection Issues: Public and Corporate Reactions to Privacy Before the Subcomm. on Gov't Info., Justice and Agric. of the House Gov't Operations Comm.*, 102nd Cong., 1st Sess. (1991) [hereinafter Hearings]. The same response may be seen in Europe. *See* Dresner, *Publisher's Comment*, Privacy L. & Bus., Aug. 1990, at 1.

adopt specific policies on fair information practices.[85] In other cases, an entire arm of the industry may develop a code of fair information practices. In Canada, for example, the banking industry association and an insurance industry group have each drafted a code of fair information practices.[86]

Self-regulation and sectoral legal rights are not mutually exclusive. In Japan, consumer credit information is protected by edicts from the Ministry of Finance and the Ministry of International Trade and Industry, while the Center for Financial Industry Information Systems ("FISC") elaborated voluntary guidelines for other personal information processed by financial institutions, insurance companies, securities companies, and companies offering credit systems.[87] FISC based its code on the OECD Guidelines.

In some legal cultures, the dividing line between sectoral rights and self-regulatory guidelines may not be clear. Although the FISC guidelines in Japan are designed for voluntary implementation, the Ministry of Finance has strongly encouraged institutional compliance.[88] Consequently, this ad hoc technique may promote the most tailored set of fair information practice standards for financial services. Similarly, the Japanese Ministry of International Trade and Industry recommended that other industries in the private sector comply with a different set of volun-

85. For example, the American Express Company has pledged itself to a set of fair information practices that consist of: (1) collecting only relevant information and disclosing its intended uses; (2) allowing customers to opt-out of inclusion on marketing lists; (3) taking measures to ensure the accuracy of personal information; (4) provide security against unauthorized access to personal information; (5) disclose personal information only with customer consent; (6) encourage business partners to respect customer privacy; (7) train employees to adhere to privacy principles. *See* Am. Express, The American Express Consumer Privacy Principles (1991) (on file with the *Fordham Law Review*). Equifax, a major U.S. credit reporting agency, also has a set of "information policies." *See* Hearings, *supra* note 84, 25-26. This policy is a pseudo-code of fair information practice standards.

In the United States, 180 companies are said to have adopted the OECD Guidelines as a corporate information policy. *See* Gassman, *supra* note 10, at 750. However, recent poll data indicates that less than one-sixth of U.S. insurance, credit, and banking organizations have advisory boards or panels that deal with privacy issues. *See* Louis Harris & Assocs., The Equifax Report on Consumers in the Information Age 98-99 (1990).

86. *See* Canadian Bankers' Ass'n, *Model Privacy Code for Individual Customers* (Dec. 1990); Canadian Life & Health Ins. Ass'n, *Policy Holder Services: Right to Privacy* (1980).

87. *See* FISC, Guidelines on the Protection of Personal Data For Financial Institutions (March 1987); Yamashita, *Protecting Personal Data in the Private Sector*, 78 Japan Computer Q. 30, 31 (1989); Yui, *Protective Measures for Personal Data in the Consumer Credit Industry*, 78 Japan Computer Q. 38, 41-43 (1989). FISC used the OECD Guidelines as the model.

88. FISC is a non-profit corporation supported by the Ministry of Finance. The chiefs of the Banking and Securities Bureaus in the Ministry of Finance issued a statement: "We trust that all financial organizations will use this guideline to deal appropriately with the issue of personal data in the future. The Japanese authorities will be observing future developments with great interest." Yamashita, *supra* note 87, at 32.

tary guidelines developed by JIPDEC in 1986.[89] In Canada, although the bank association code of practice is voluntary, all chartered banks must be members of the association.[90] Also, the Minister of Consumer and Commercial Relations in Ontario, Canada indicated that insurance companies must conform to the privacy guidelines issued by the Canadian Life and Health Insurance Association in order to do business in Ontario.[91]

Since privacy rights are usually targeted narrowly under an ad hoc approach, there is a natural tendency to rely on private enforcement mechanisms. The United States, for example, has no single government supervisory agency to monitor the collection or use of personal information or to enforce existing rights, especially in connection with financial services.[92] For situations dependent on self-regulation, by definition, there is no government supervision. This tendency is also reflected in Hong Kong and Japan where neither country has a government agency designed to supervise industry fair information practices.[93]

In countries using ad hoc techniques, the debate over targeted protections and their evolution is on-going. The United States, for example, has a plethora of proposals that revisit the treatment of personal information by the credit industry.[94] In Hong Kong, where there is a voluntary set of data protection guidelines, the Law Reform Commission is working on broad legislation.[95] In Canada, the provincial governments are re-

89. *See* Yamashita, *supra* note 87, at 32, 35. JIPDEC, the Japan Information Processing Development Center, is a non-profit think tank closely allied to the Ministry of International Trade and Industry. *See id.* at 32.

90. *See Canadian Bankers' Association Strengthens Privacy Code*, Privacy L. & Bus., Winter 1990/91, at 14.

91. *See* Can. Life & Health Ins. Ass'n, *supra* note 86.

92. For example, in addition to private litigation, the Federal Trade Commission is authorized to prosecute violations of the Fair Credit Reporting Act and the Fair Credit Billing Act. *See* 15 U.S.C. § 1681s (1988); 15 U.S.C. § 1607 (1988). The Electronic Funds Transfer Act is enforced by the banking supervisory agencies. *See* 15 U.S.C. § 1693 (1988). Enforcement of the Electronic Communications Privacy Act is by either private litigation or the prosecutor. *See* 18 U.S.C. § 2511 (1988).

93. For financial services, to the extent that the Japanese Ministry of Finance and the Japanese Ministry of International Trade and Industry have promulgated or assisted the development of privacy codes these ministries may have strong persuasive powers. *See supra* notes 87-89 and accompanying text.

94. *See, e.g.*, H.R. 29, 102d Cong., 1st Sess. (1991); H.R. 194, 102d Cong., 1st Sess. (1991); H.R. 421, 102d Cong., 1st Sess. (1991); H.R. 633, 102d Cong., 1st Sess. (1991); H.R. 670, 102d Cong., 1st Sess. (1991); H.R. 1751, 102d Cong., 1st Sess. (1991).

95. *See generally* Dep'ts & Gen. Div. Admin. Servs. & Info. Branch, Gov't of H.K., Data Protection Principles and Guidelines (1988) (existing government-recommended voluntary guidelines); Mortimer, *Hong Kong Plans Data Protection Law*, Privacy L. & Bus., July 1991, at 14-17 (the government set up a "sub-committee of the Hong Kong Law Reform Commission in March 1990 to formulate proposals for Data Protection Legislation"); Memorandum on Privacy Protection of Personal Information, The Law in Hong Kong and Options for Reform from Mark Berthold, Sec'y of the Privacy Subcommittee of the Hong Kong Law Reform Commission to the Law Reform Commission (Feb. 1990) (this paper represented the personal views of the author and does not neces-

examining ad hoc protection.[96]

2. The Omnibus Approach

In contrast to the ad hoc approach, many countries prefer omnibus legislation as the tool to define fair information practices for both the private and public sectors. As with the ad hoc approach, the omnibus laws fail to converge on a uniform set of standards, though unlike the ad hoc approach, all the basic issues of fair information practice found in the European Convention are generally covered. The first generation of omnibus laws, including the French, Swedish, and original German data protection statutes, set forth single, coherent sets of principles that were to be applied in all circumstances.[97] The second generation of laws begin to seek more flexible mechanisms that differentiate among sectors and increase the types of available sanctions as well as self-regulatory mechanisms.[98] This generation includes the Dutch and revised Danish statutes.

In contrast to the ad hoc approach, omnibus legislation often creates powerful administrative agencies with significant enforcement powers.[99] In France, the Commission nationale de l'informatique et des libertés (the "C.N.I.L.") supervises compliance with the data protection statute, prosecutes violations, and has authority, with broad discretion, to conduct on-site searches and seizures.[100] The C.N.I.L. tends to focus on private sector enforcement and has, for example, made a number of inspections of insurance data processing sites.[101] In the United Kingdom, the Data Protection Registrar performs a similar role. The new German statute gives enforcement powers to state supervisory agencies and permits searches of business records.[102] Not surprisingly, the omnibus approach emphasizes penalties for violations of fair information practices. Harmed individuals may recover actual or statutory damage amounts.

---

sarily reflect the views of the Law Reform Commission) (on file with the *Fordham Law Review*).

96. *See* Letter from Paul-André Comeau, President, Commission d'accès à l'informatique du Québec, to Joel R. Reidenberg, Associate Professor of Law, Fordham University (Feb. 20, 1992) (on file with the *Fordham Law Review*).

97. *See* Nugter, *supra* note 14, at 19-20. One should note that Nugter's analysis refers to the first German data protection statute. A more recent law has entered into force in Germany. *See generally* German Law, *supra* note 14 (Germany enacted the Federal Data Protection Act in 1991).

98. *See* Nugter, *supra* note 14, at 19.

99. *See* D. Flaherty, Protecting Privacy in Surveillance Societies 11-16 (1989). The omnibus laws tend to establish data protection authorities. *See, e.g.*, French Law, *supra* note 14, § 6; Dutch Law, *supra* note 14, § 37; Danish Law, *supra* note 14, § 22; British Law, *supra* note 14, §§ 10, 19.

100. *See* French Law, *supra* note 14, §§ 6, 11, 21. The C.N.I.L. may exercise these powers to investigate complaints, improve its knowledge of data practices and enforce its decisions. *See* C.N.I.L., Dix ans d'informatique et libertés 68 (1988) [hereinafter C.N.I.L., Dix ans].

101. *See* A. Lucas, Le droit de l'informatique 173-75 (1987); C.N.I.L., 9e Rapport d'activité 211-15 (1988) [hereinafter C.N.I.L., 9e Rapport].

102. *See* German Law, *supra* note 14, § 38(1)-(4).

In addition, the data protection authorities may seek civil and criminal sanctions against infringing parties.

Although many of the countries with omnibus data protection laws are signatories of the European Convention and proponents of the OECD Guidelines, the omnibus technique has not achieved uniform rules within the scope of national laws. Most of the omnibus laws seek to protect only individuals.[103] Several apply, also, to legal persons.[104] The distinction in connection with information about individuals acting in their capacities as employees or officers of corporations may be blurred for some laws. For example, the French law is limited to information about individuals, but France interprets personal information broadly to include corporate files containing information relating to "officers, stockholders or partners."[105] The British law is interpreted similarly for sole proprietorship companies.[106] Other laws may specifically address financial data.[107] A recent European effort, however, seeks to limit the definitional scope of personal information by excluding information that could be used to identify particular individuals only through extraordinary or unreasonable efforts.[108] This exclusion would be significant for financial services that involve intermediate data processing activities of personal information about identifiable, but not actually identified individuals (such as account number referencing). The new German law makes some special allowances for storage of depersonalized information.[109] In addition, a number of the omnibus laws apply to non-computerized records on individuals.[110]

The national laws seek significant and different fairness requirements for data collection. Most omnibus regimes require careful disclosure to individuals at the time of data acquisition, though the nature of these disclosures varies. France, for example, mandates that an individual must be informed of the obligatory or optional character of providing personal information, the consequences of refusing to provide information, the identity of any persons receiving the information and the existence of the right of access and correction.[111] The British law also

103. *See* Data Protection Roundup, *supra* note 14, at 2-7.

104. The Austrian, Danish, Finnish, Icelandic, Luxembourgeois and Norwegian laws give rights to information about legal persons. *See id.* at 2-7.

105. *See* C.N.I.L., Dix ans, *supra* note 101, at 42; H. Croze & Y. Bismuth, Droit de l'informatique 36 (1986).

106. *See* U.K. Data Protection Registrar, *Guideline 2—The Definitions*, ¶ 4.1 (1989).

107. *See, e.g.*, Danish Law, *supra* note 14, § 1(1).

108. *See* Draft EC Directive, *supra* note 14, § 2(b). This view differs from some of the laws. The British, for example, view depersonalization skeptically. *See* U.K. Data Protection Registrar, *Guideline 2—The Definitions*, ¶ 3.2 (1989).

109. *See* German Law, *supra* note 14, § 30(1).

110. For example, the Dutch, French and German laws apply to manual records. *See* French Law, *supra* note 14, § 5 (applies to manual records used in conjunction with data processing); Dutch Law, *supra* note 14, § 1 (applies if data is systematically disposed); German Law, *supra* note 14, § 3(2) (applies to non-automated structured personal information).

111. *See* French Law, *supra* note 14, § 26 (forbids unfair and illegal data collections),

stipulates that personal information shall be obtained fairly; this means that the collector of personal information must notify the individual of the data collection, of the reasons for the collection, whether disclosures of the information will be made to others, and must refrain from collecting excessive information.[112] Similar requirements exist in the new German statute.[113] Thus, the standards of individual consent to data collection are similar, but not identical. For financial services, these differences may be important; the collection requirements for credit information, card transaction information, and insurance underwriting information may require onerously detailed disclosure in some countries to satisfy the general purpose fairness requirements. Collections may also need to comply with several differing requirements.

In addition, many of the laws place prohibitions on the collection and processing of "sensitive data" that may be dangerous for individuals if misused. The European Convention specifically recognizes this need, yet not all European laws define "sensitive data" in the same way; the concept draws from different European experiences with discrimination, hatred, and genocide. Information identifying racial origin, opinions (political, religious, or philosophical), union membership, and criminal convictions is usually targeted.[114] Nevertheless, the differences may be important. For example, the French law does not include health or sexual preference information, while the British, Danish, and Dutch laws do.[115] In the context of financial services, some of these restrictions may be problematic for insurers developing actuarial tables and verifying health payments, as well as for banks or credit institutions seeking to protect against fraud through reference to criminal records. In some

§ 27 (lists the notice obligations for data collection); *see also* C.N.I.L., Dix ans, *supra* note 101, at 16.

112. *See* British Law, *supra* note 14, Sched. 1, Pt. 1, § 1-7; Office of U.K. Data Protection Registrar, Fifth Annual Report 8 (1989) [hereinafter Fifth Report].

113. *See* German Law, *supra* note 14, §§ 4(2), 33.

114. *See* European Convention, *supra* note 33, § 6 (listing information related to "racial origin, political opinions or religious or other beliefs . . . health or sexual life . . . [and] criminal convictions"); C.N.I.L., Dix ans, *supra* note 101, at 42-43.

115. *Compare* French Law, *supra* note 14, § 31 (setting forth sensitive data as information reflecting: racial origin, political, philosophic or religious opinions, or trade union affiliation) *with* British Law, *supra* note 14, § 2(3) (supplemental protections may apply to information relating to: racial origin, political opinions or religious or other beliefs, physical or mental health or sexual life, or criminal convictions) *and* Danish Law, *supra* note 14, § 3(2)(limits processing of data on: race, religious belief or color of skin, political, sexual or criminal matters and on health, social problems or excessive use of intoxicants) *and* Dutch Law, *supra* note 14, § 7(1) (requires regulatory guidance for the use of information relating to: "religious beliefs or philosophy of life, race, political persuasion, sexuality or intimate private life and medical, psychological, criminal or disciplinary" information). The German Law proscribes communication of information concerning health, criminal and administrative offenses, religious or political views, and information divulged to an employer under the labor law. *See* German Law, *supra* note 14, § 28(2)1b. The European Convention covers data relating to race, political opinions, religious or other beliefs, health and sex life, and criminal convictions; it does not mention union membership or any other categories. *See* European Convention, *supra* note 33, § 6.

cases, however, additional restraints on sensitive data may never actually be implemented.[116]

As in the European Convention, national laws seek to impose strict purpose limitations on the use of personal information. In the new German law, personal information may generally be used by private entities only "in accordance with the purposes of a contract or quasi-contractual fiduciary relationship . . . [unless] the data can be taken from generally accessible sources."[117] The personal information must still be obtained fairly. France views the purpose limitation as one of the most critical components of data protection policy.[118] Both the British and the French laws require the data collection purposes to be specifically registered with the data protection authority.[119] Under the Dutch law, personal information cannot generally be communicated to third parties unless the communication satisfies a specified purpose or the individual has given express, written consent.[120] For financial services, purpose limitations may pose difficulties for constantly evolving, multi-layered networks of service providers.

Omnibus legislation also seeks to assure the quality of available personal information. National laws grant individuals similar rights of access to stored personal information and impose obligations to ensure the correction of erroneous information.[121] Some special exemptions from the access requirements may be granted for financial institutions performing statutorily defined duties. These exemptions are not uniform.[122] The quality norm also leads to variable rules on the duration of data storage. The Danish law, for example, generally limits storage to a five-year period.[123] Other laws have different durational limits.[124] In the case of credit information, French regulations limit storage to three years for settled accounts and five years for defaulted accounts.[125]

116. *See* Dutch Law, *supra* note 14, § 7. No implementation guidance has been issued by the Registration Chamber.

117. German Law, *supra* note 14, § 28(1).

118. *See* C.N.I.L., Dix ans, *supra* note 101, at 38 (secondary uses of personal information are a major risk to individual rights).

119. *See* British Law, *supra* note 14, § 4(3)(b) & Sched. 1, II(2); French Law, *supra* note 14, § 19.

120. *See* Dutch Law, *supra* note 14, §§ 11(1), 12(1).

121. *See* British Law, *supra* note 14, §§ 21, 22, 24; French Law, *supra* note 14, §§ 34-37; Dutch Law, *supra* note 14, §§ 29, 31; German Law, *supra* note 14, §§ 34, 35; Danish Law, *supra* note 14, § 7(a).

122. *See, e.g.*, French Law, *supra* note 14, § 40 (access to health information kept by an insurer may be indirect through the individual's physician); German, *supra* note 14, § 34(4) (access not required if statutory authority exempts collection from notice requirements under section 33(2)(3)); Isle of Man Data Protection Act 1986 § 29 (access not required if it would interfere with the discharge of a statutory function).

123. *See* Danish Law, *supra* note 14, § 4(2).

124. *See, e.g.*, French Law, *supra* note 14, § 28 (duration limited to registered period); German Law, *supra* note 14, § 35(2) (erasure required as soon as no longer needed).

125. *See* Délibération No. 88-83 du 5 juillet 1988, *reprinted in* C.N.I.L., 9e Rapport, *supra* note 102, at 381-83; *see also* C.N.I.L., 9e Rapport, *supra* note 102, at 202.

The omnibus approach stresses transparency of private data processing activities.[126] The public should be able to discover data processing activities that involve personal information. To this end, the laws oblige data processing activities to be either disclosed to a government data protection authority or licensed by the national authority.[127] Generally, the data processing purposes, types of personal information being stored, contact information for individuals to seek access to and correction of data, and destinations of personal information must be filed with the authority.[128] These registration systems tend to be rather cumbersome. The U.K. Data Protection Registrar has recently concluded that simplification is an important goal.[129]

The more nuanced, second-generation approach to omnibus regulation recognizes the difficulties inherent in applying general principles to all industries in a rapidly changing technological environment.[130] These laws allow diverging interpretive mechanisms to evolve. The revised Danish law, for example, includes specific provisions for credit reporting,[131] direct marketing,[132] and third party electronic data processing.[133] The Dutch law uses a novel technique of elaborating fair information practice rules, and permits sectoral groups to develop codes of practice for approval by the Registration Chamber.[134] Only proposals for precisely defined sectors, drafted by representative groups that have consulted with interested organizations, are considered.[135] The Dutch approval process includes a period of public comment.[136] The financial services sector has initiated some of the first sectoral codes. The Association of Dutch Bankers and the Association of Insurance Companies are each drafting codes of practice to implement the data protection principles, though neither code has been released yet for public comment.[137] If these codes are approved, the process offers a persuasive safe-harbor attesting to compliance with the statutory obligations even though the

126. *See* C.N.I.L., Dix ans, *supra* note 101, at 17.

127. *See, e.g.*, French Law, *supra* note 14, §§ 16, 17 (licensing for private sector data processing, automatic licensing for non-risk, common practices); British Law, *supra* note 14, §§ 4, 7(6) (licensing of data users and computer bureaux, though applications have provisional validity upon filing); Dutch Law, *supra* note 14, § 24 (licensing requirement for private sector data processing); German Law, *supra* note 14, § 32 (notification requirement for private sector).

128. *See, e.g.*, French Law, *supra* note 14, § 19; British Law, *supra* note 14, § 4(3).

129. *See* Fifth Report, *supra* note 112, at 73-79.

130. *See id.* at 67-72.

131. *See* Danish Law, *supra* note 14, §§ 8-16.

132. *See id.* §§ 17-19.

133. *See id.* § 20.

134. *See* Dutch Law, *supra* note 14, § 15(1).

135. Facsimile from the Hon. Peter J. Hustinx, President, Registration Chamber, to Joel R. Reidenberg, Associate Professor of Law, Fordham University 1 (March 6, 1992) (on file with the *Fordham Law Review*).

136. *See id.* at 2.

137. *See id.* at 1-2.

codes will still not be binding on Dutch courts.[138] The legal character is more powerful and persuasive than a purely industry-drafted, sanctionless self-regulatory scheme.[139] Hong Kong is considering a similar device in its plans for an omnibus law.[140]

The omnibus approach has not led to a uniform view of extraterritoriality.[141] The rights and obligations of data protection acts apply to foreign data processing activities in different manners. The French law, for example, applies only to processing operations in France.[142] The British law applies only to persons in the United Kingdom who control the content and use of personal information, whether or not the processing occurs within the United Kingdom.[143] And, the Dutch law applies to data files located within the Netherlands and to data processing outside the Netherlands if the user is within the Netherlands and the data pertains to a Dutch resident.[144] For multinational financial services, the concurrent application of varying standards of fair information practice can be a detrimental influence on service development.

The varying rules contained in omnibus laws may also dictate non-uniform corporate organization requirements. Some omnibus laws require that a data protection officer be employed by companies processing personal information.[145] Others merely require that a division be responsible for data protection policy.[146] These structural issues can have a significant impact on global financial service companies. In some cases, the fair information practice rules may even require the formation of new legal entities, such as the incorporation of a trade association in order for financial institutions to share information on delinquent debtors.[147]

Financial services have benefitted from some national guidance on the implementation of fair information practice principles. In the United Kingdom, banking issues have recently been addressed.[148] In addition,

---

138. *See* Dutch Law, *supra* note 14, § 15(6).

139. *See* Nugter, *supra* note 14, at 167 (if these self-regulatory sectoral codes are not adopted in a manner satisfactory to the Registration Chamber, mandatory sectoral regulations may be issued).

140. *See* Mortimer, *supra* note 95, at 16.

141. *See* Nugter, *supra* note 14, 182-94.

142. *See, e.g.*, French Law, *supra* note 14, § 47.

143. *See* British Law, *supra* note 14, § 39.

144. *See* Dutch Law, *supra* note 14, § 47.

145. *See, e.g.*, German Law, *supra* note 14, § 36.

146. The French law, for example, requires that the application for the registration of data processing activities specify the corporate division responsible for data protection policy and the contact for individuals to exercise the right of access. *See* French Law, *supra* note 14, § 19.

147. France required the formation of a "groupement d'intérêt économique" in order for credit establishments to share data on delinquent consumer debtors. *See* C.N.I.L., 9e Rapport, *supra* note 102, at 203-04.

148. *See* Fifth Report, *supra* note 112, at 4-5. In 1989, the British Review Committee on Banking Services Law (known as the Jack Committee) recommended a variety of measures to improve the banker's duty of confidentiality and establish standards of "best practice" for customer consent to disclosures of information. *Id.* at 32-33. The banking

the information practices of credit reporting agencies have been scrutinized. The U.K. Data Protection Registrar has challenged the use of third-party information by credit reporting agencies in reports on credit applicants.[149] These guidance issues revolve around the fairness of data collection (notice to individuals and legitimacy of collected information) and processing purposes. The U.K. Data Protection Registrar has also focused on the ambiguity of the principles for electronic point-of-sale transactions (EFTPOS) and is seeking to develop particular guidance.[150]

The French data protection authorities have also historically been concerned by the application of the law's principles to financial services. The C.N.I.L. has developed simplified registration procedures for data processing relating to client accounts,[151] retail lending,[152] and insurance.[153] To satisfy these regulations, the C.N.I.L. specifically limits the types of personal information that may be collected, the uses of and access to such personal information, as well as the duration of storage. Sensitive data protection issues have been raised in France in connection with the development of private databases for lost and stolen checks.[154] The C.N.I.L. has sought to establish that the personal information used by any such databases be relevant for the narrow objectives of preventing payment on lost and stolen checks.[155] The C.N.I.L. required that individuals provide written consent before the information may be disseminated.

The C.N.I.L. raised similar concerns for databases related to defaulted consumer loans and provided comparable guidance.[156] Even credit scoring is prohibited by the French law, though the C.N.I.L. does not interpret this strictly.[157] The C.N.I.L. has also been sensitive to computerized

industry responded and adopted a code of practice that mentions data protection. *See generally* British Bankers Ass'n, Good Banking (1992).

149. *See* Fifth Report, *supra* note 112, at 6-7; Equifax Eur. Ltd. v. Data Protection Registrar, U.K. Data Protection Tribunal Appeal Decision, 5-6 (June 28, 1991); Infolink Ltd. v. Data Protection Registrar, U.K. Data Protection Tribunal Appeal Decision, 5-6, 18-19 (May 31, 1991); CCN Sys. Ltd. v. Data Protection Registrar, U.K. Data Protection Tribunal Appeal Decision 4-5 (undated opinion) [collectively hereinafter Data Tribunal Cases].

150. *See* Fifth Report, *supra* note 112, at 8-9.

151. *See Norme Simplifiée No. 12: Délibération No. 80-22 du 8 juillet 1980, reprinted in* C.N.I.L., *Informatique et Libertés No. 1473* 165-68 (1991).

152. *See Norme Simplifiée No. 13: Délibération No. 80-23 du 8 juillet 1980, reprinted in* C.N.I.L., *Informatique et Libertés No. 1473* 169-72 (1991) [hereinafter NS 13].

153. *See Norme Simplifiée No. 16: Délibération No. 81-04 du 20 janvier 1981, reprinted in* C.N.I.L., *Informatique et Libertés No. 1473* 181-84 (1991).

154. *See* C.N.I.L., 11e Rapport d'activité 131-42 (1991) [hereinafter 11e Rapport]. Databases have been proposed in the public sector through the Banque de France as well as the private sector through regional groups such as organizations of retailers.

155. *See* C.N.I.L., 11e Rapport, *supra* note 154, at 132.

156. *See id.* at 142-53. The proposed database was initiated through the Banque de France rather than a private institution.

157. *See, e.g.*, French Law, *supra* note 14, § 2 (no private sector decision on character may be based solely on a computer generated profile); NS 13, *supra* note 152, at 181-84 (simplified registration unavailable if credit scoring is used). The C.N.I.L., however, is

profiling in the insurance sector and has issued rules for such practices.[158] Risk calculations are limited to the use of certain parameters, including the insured's age, marital status, and health situation.[159] In response to concerns about the use of medical records, the C.N.I.L. also investigated the practices of life insurance companies and required a trade association to terminate its database on "high-risk" individuals.[160] In contrast, the reinsurance industry has been permitted to use the national identification number in order to price high-risk policies.[161] The C.N.I.L. has similarly delimited fair information practices in connection with health insurance payments. Health care providers may electronically access insurance data.[162] The personal information is restricted to identity, address, insurance number, and insurance status.

II. THE STARTING BLOCK: EXPORT OBSTACLES FOR FINANCIAL SERVICES INFORMATION

Because of the transnationalization of personal information processing, fair information practice rules often consider the international implications of differing standards.[163] Transborder data flows raise legitimate concerns for national authorities of the sufficiency of foreign fair information practice rules. Problems may arise in several contexts: the differing levels of fair information practice standards; the uncertainty of applicable law; and, the practical problems of implementation.[164] The French fear of "data havens," for example, is reasonable when information processing for French companies may be structured off-shore to avoid fair information practice rules in France.[165] Nevertheless, a country's interest in off-shore data processing standards for financial transactions that may take place between a foreign national and a foreign financial institution suggests that the application of national fair informa-

---

said not to object to credit scoring when credit is granted; the practice is seen as objectionable only when credit is denied. *See* C.N.I.L., 9e Rapport d'activité, *supra* note 101, at 200 (1989) (a financial institution need not explain the denial of credit to an applicant, but the C.N.I.L. emphasizes that a credit score may not be the sole reason for denial).

158. *See* C.N.I.L., Dix ans, *supra* note 100, at 102.

159. *See id.*

160. *See* C.N.I.L., 11e Rapport, *supra* note 154, at 153-55; *Délibération No. 90-95 du 11 septembre 1990, reprinted in* C.N.I.L., 11e Rapport, *supra* note 154, at 155-57.

161. *See Délibération No. 90-43 du 3 avril 1990, reprinted in* C.N.I.L., 11e Rapport, *supra* note 154, at 159-60.

162. *See Délibération No. 88-06 du 6 janvier 1988, reprinted in* C.N.I.L., 9e Rapport, *supra* note 101, at 363.

163. *See, e.g., Teleinformatics, supra* note 9, at 208-17; Fishman, *Introduction to Transborder Data Flows*, 16 Stan. J. Int'l L. 1, 7, 11-12 (1980) [hereinafter *Transborder Data Flows*]; Kirby *Transborder Data Flows and the "Basic Rules" of Data Privacy*, 16 Stan. J. Int'l L. 27, 28 (1980); Turn, *Privacy Protection and Security in Transnational Data Processing Systems*, 16 Stan. J. Int'l L. 67, 74 (1980).

164. *See* Hondius, *Data Law in Europe*, 16 Stan. J. Int'l L. 87, 102-04 (1980).

165. The French conceived of this problem, in part, through the fear that dating services would send personal information off-shore. *See* Lucas, *supra* note 101, at 67.

tion practice rules would be inappropriate.[166]

The international instruments address the data export issue, but offer contradictory standards. Because these instruments conflict and restrain only some national regulation of transborder data flows, it is critical to examine how various omnibus laws treat data exports.[167] Although the omnibus laws do not separately identify exports of information related to financial services, the transborder data flow provisions apply to the information flows associated with these services. Data flow regulation may affect several levels of financial service activities such as intra-corporate information processing (from corporate record keeping practices for world-wide operations or business management of global services to the more routine electronic mail communications across borders), inter-corporate processing (such as payments), and external flows (such as the marketing of information services).[168]

A. *International Mechanisms*

1. The Permissive OECD Guidelines

The OECD Guidelines reflect a positive view of international data flows. The guidelines stipulate that countries should refrain from restricting transborder flows of personal data unless the destination "does not yet substantially observe these Guidelines" or fails to provide specific protection to certain categories of sensitive information such as race, religion, or political beliefs that are subject to specific protection in the sending country.[169] In addition, the OECD Guidelines obligate countries to take "all reasonable and appropriate steps to ensure that transborder flows of personal data . . . are uninterrupted"[170] and to avoid developing laws or policies that create obstacles to transborder data flows.[171]

2. The Restrictive European Convention

In contrast, the European Convention assumes that international data flows may be a greater threat and warrant greater control. The convention permits restrictions on data flows to other signatories only if the destination does not have "equivalent" specific legislation regulating certain categories of sensitive personal information or if data is to be "transshipped" from a signatory to a non-signatory.[172] The meaning of equivalent is not defined in the European Convention, and the treaty is

166. For example, if a U.S. citizen on vacation in Paris transfers funds between U.S. accounts using a U.S. issued credit card, there is no significant basis for France to care about what happens to the personal information in the United States.

167. Countries that do not use the omnibus approach to fair information practice regulation tend not to distinguish between domestic and international data processing.

168. *See* Grossman, *supra* note 42, at 9-12; Nugter, *supra* note 14, at 8-10.

169. OECD Guidelines, *supra* note 32, ¶ 17.

170. *Id.* ¶ 16.

171. *See id.* ¶ 18.

172. European Convention, *supra* note 33, § 12(2).

surprisingly silent on direct transborder data flows to non-signatory countries.[173] By allowing restrictions on trans-shipment of data to non-signatory countries, the treaty implicitly allows restrictions on all direct transborder data flows to non-signatory countries. National laws address this problem directly. In addition, the failure of the European Convention to define equivalent protection for sensitive data flows to signatory countries opens the door to restrictions that may hamper credit and health insurance services.

In the financial services context, the Council of Europe's specific guidance on payment operations goes further than the European Convention and presumes that data transfers to non-signatory countries should be prohibited. The text of the recommendation notes that "respect for the principles contained in this recommendation . . . shall be regarded by the competent authorities in the Contracting Parties as a strong justification for allowing personal data to be transferred."[174] Data transfers among signatory countries are to be free of obstacles provided that "equivalent" protection is guaranteed.[175] The notion of equivalence, while still undefined, goes beyond the treatment of sensitive data and applies to all payment related information.

B. *National Restrictions*

National Laws in Europe tend to allow or encourage the prohibition of data exports. In France, data processing activities involving the export of personal information must be registered with the C.N.I.L. and the C.N.I.L. has a discretionary power to prohibit transfers abroad of personal information.[176] Ever since the French realized that dating service records might be sent overseas, the French have been particularly obsessed with fears that personal information would be exported from France to "data havens" for processing.[177]

Among the Europeans, France appears the least hesitant to restrict international data flows. The first published case involved the centralization of personnel records for a multinational company. The C.N.I.L. prohibited the transfer of data from the French subsidiary to the Italian parent company because Italy did not have an omnibus data protection law.[178] For the same reason, the C.N.I.L. is also reported to have restricted the transfer of health information from France to Belgium[179] and

173. *See id.* § 12.

174. Recommendation R(90)19, *supra* note 56, app. § 10.2.

175. *Id.* app. § 10.1.

176. Article 19 of the French Law requires specific mention in the registration application: "if the data processing is designed to export personal information between French territories and foreign locations." French Law, *supra* note 14, § 19. Article 24 provides that the C.N.I.L. "can prohibit" transborder data flows. *Id.* § 24.

177. *See* Lucas, *supra* note 102, at 67.

178. *See Délibération No. 89-78 du 11 juillet 1989 reprinted in* C.N.I.L., 10e Rapport 32-34 (1989).

179. *See Délibération No. 89-98 du 26 sept. 1989, reprinted in* C.N.I.L., 10e Rapport

other personal information from France to Switzerland and France to the United States.[180]

Similarly, the U.K. Data Protection Registrar has begun to prohibit international data flows. Under the British law, personal information can only be transferred abroad when the transfer is designated on the registration filed with the Data Protection Registrar.[181] The Data Protection Registrar may issue a transfer prohibition notice interdicting the transmission of personal information abroad when the transmission may lead to the contradiction of the statutory principles.[182] The first prohibition was issued in 1990 against the transfer of a mailing list from the United Kingdom to the United States.[183] This first case involved an American direct mail organization that allegedly sought to defraud British consumers. The precedent is noteworthy and further cases are expected.

In the Isle of Man, a jurisdiction with a sizeable presence of multinational insurance companies, the data protection statute also permits the local authority, the Data Protection Registrar, to restrict the export of personal information.[184] The Data Protection Registrar has even noted the impropriety of prohibiting data flows to some countries while ignoring problems with privacy protection in the United States.[185]

Other European laws contain similar affirmative restrictions on transborder data flows. Danish law prohibits the collection of sensitive data for storage outside of Denmark including information on health, skin color, political beliefs, philosophical or religious opinions, and union affiliations.[186] The collection of other data for use outside of Denmark

---

d'activité 35-37 (1990) (health data could only be transferred in anonymous form under agreement providing for French protections in Belgium); *see also Délibération No. 85-07 du 17 fév. 1985, reprinted in* C.N.I.L., *Informatique et Libertés No. 1473*, 281-83 (1990) (patient records for medical research may only be transferred aborad in anonymous form). Where omnibus laws exist, the C.N.I.L. permits the transfer of health data. *See Délibération No. 90-114 du 6 nov. 1990, reprinted in* C.N.I.L., 11e Rapport d'activité 234-35.

180. Interview with Ariane Mole, Attachée Relations internationales, Direction juridique de la Commission nationale de l'informatique et des libertés, in Paris, France (June 6, 1991).

181. *See* British Law, *supra* note 14, § 4(3)(e).

182. Section 12(2) allows the Data Protection Registrar to prohibit data exports if the transfer is likely to contravene or lead to the contravention of the British data protection principles, provided that the destination is not bound by the European Convention. Section 12(3) allows for restrictions to destinations bound by the European Convention if certain conditions are met. *See* British Law, *supra* note 14, § 12.

183. *See* Office of the Data Protection Registrar, Seventh Annual Report 33-34 (1990); *First UK Ban on Data Exports is to Named Companies in the USA*, Privacy L. & Bus., Winter, 1990/91, at 5.

184. Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information § 12 (July 16, 1986).

185. *See* Office of the Isle of Man Data Protection Registrar, First Annual Report 11 (Oct. 1989).

186. *See* Danish Law, *supra* note 14, § 21(1); Briat, *Personal Data and the Free Flow of Information* in Freedom of Data Flows and EEC Law 50 (1987).

must be licensed if a license would be required to process the information in Denmark.[187] The new Dutch law allows the national authority, the Registration Chamber, to prohibit data exports for processing in destinations where the protections of the Dutch law are not applicable.[188] The Dutch law, however, has a broad extra-territorial sweep. Databases containing personal information relating to Dutch residents, even though located outside of the Netherlands, will be subject to the protections of the Dutch law if the database is under the control of a Dutch resident.[189] The Registration Chamber may exempt such foreign databases if the local law provides "equivalent protection for the privacy of the data subjects."[190] In contrast, foreign data subjects may benefit from data protection in jurisdictions where personal information is used.[191] Luxembourg, for example, applies the protections of its law to foreign databases if they are electronically accessible in Luxembourg.[192]

A draft proposal for a European directive on data protection contains a strikingly restrictive transborder data flow provision. Although the specific terms of the proposal have been rather controversial, there is little disagreement over the need to address transborder data flow issues.[193] The first version of the proposal prohibits data flows to non-EC countries that do not provide a guarantee of "adequate" data protection.[194] Observers believe that the final text will adopt a higher "equivalent" standard of comparison for non-EC countries.[195] In any event, the original proposal would establish a consultative committee to draw up a list of countries with unsatisfactory protection.[196] Transfers to these countries would only be permitted after a case-by-case review that allows members to object.[197]

Elsewhere narrow rules may apply to financial services activities. In Canada, for example, the Banking Act prohibits Canadian banks from

187. *See* Danish Law, *supra* note 14, § 21(1).

188. Article 49(2) of the Dutch Law provides: "data shall not be supplied from the Netherlands to, or obtained in the Netherlands from, any data file in another country to which this Act does not apply where it has been declared by General Administrative Order that such a transfer of data would have a serious adverse effect on the privacy of the persons concerned." Dutch Law, *supra* note 14, § 49(2).

189. *See id.* § 47(1).

190. *Id.* § 47(2).

191. *See* Nugter, *supra* note 14, at 216-24.

192. *See* Briat, *supra* note 186, at 51.

193. *See* Commission on Legal Affairs & Citizen's Rights, Draft Report, Eur. Parl. Doc. (COM(90)314 final—SYN 287, 288), Explanatory Statement ¶¶ 1, 8 (1991).

194. *See* Draft EC Directive, *supra* note 14, § 24.

195. Remarks by Malcolm Norris, Data Protection Registrar, Office of the Isle of Man Data Protection Registrar, to Electronic Democracy Conference, Washington, D.C., Sept. 5, 1991; Remarks by Ulla Ihnen, Directorate Gen. for Internal Market and Indus. Aff., Comm'n of the Eur. Communities, to 4th Annual Privacy Laws & Business Conference, Cambridge University, July 3, 1991. In March, 1992, however, the European Parliament voted on proposed revisions and did not modify the "adequacy" standard. The Commission may, nevertheless, incorporate the change in the next draft.

196. *See* Draft EC Directive, *supra* note 14, §§ 24(2), 27, 28(1)b.

197. *See* Draft EC Directive, *supra* note 14, § 25.

processing client information abroad.[198]

III. THE FIRST LAP: A REGULATORY CHALLENGE

The international and national sanctions for data flow controls pose a significant regulatory challenge. Conflict over international data flows may arise at both the process and privacy substance levels; different approaches to regulation may cause friction and varying substantive rights may also cause tension. The continued existence of varying approaches to fair information practices[199] and the failure to achieve harmonized substantive rules suggest that international efforts to achieve a broad consensus on privacy or data protection policy will not resolve transborder data flow conflicts.

A. *The Intra-European Challenge*[200]

Within the European Community, important problems arise due to the data export prohibitions contained in national laws. A significant number of the members of the European Community have not ratified the European Convention.[201] Consequently, the stipulation that signatories refrain from restricting data exports to other signatories does not apply to all intra-European data flows. As a result, differences among national laws can result in the exercise of export control mechanisms among members of the European Community.[202]

Because the omnibus approach to fair information practice standards is common in Europe, a comparison of European data protection laws generally reveals a consistent lack of symmetry on the substantive rights, rather than on the procedural approach.[203] The scope of the laws varies significantly on the definition of personal information—specifically on whether legal persons are included with individuals. These scope differences are compounded by asymmetry in the national laws on the applicability to manual records as well as to computer files. The definition of sensitive data varies. These differences may be particularly troublesome for insurance services. Generally speaking, the interpretation of national

198. Bank Act, R.S.C., ch. B-1, § 157 (1985) (Can.).

199. The voluntary OECD approach contrasts with the Council of Europe treaty approach and the omnibus technique opposes the ad hoc technique for national rules.

200. *See generally* Nugter, *supra* note 14; *The TEDIS-EDI Legal Workshop*, Eur. Comm. Doc. AT/dd(89)1814 (1989) [hereinafter *The TEDIS-EDI Legal Workshop*].

201. The twelve member states of the European Economic Community have each signed the European Convention, but only Denmark, France, Germany, Ireland, Luxembourg, and the United Kingdom have ratified with the enactment of conforming laws. Portugal and the Netherlands have each enacted legislation, but have not yet ratified the European Convention. Spain has ratified the convention, but never enacted data protection legislation. Belgium, Greece, and Italy have not succeeded in adopting legislation. *See Data Protection Roundup*, *supra* note 14, at 2-7.

202. *See supra* notes 176-90 and accompanying text.

203. *See* Nugter, *supra* note 14; Hondius, *supra* note 164; *The TEDIS-EDI Legal Workshop*, *supra* note 200, at 12-34.

laws may not result in the same guidance for the collection and use of personal information by financial institutions.

The obligations on users of personal information may also vary considerably. In particular, the extent to which a financial institution must notify and obtain consent from an individual for the processing of personal information is not uniform. The French law, for instance, requires that an individual be informed of the data collection, informed of the consequences if information is not provided, and informed of the third parties to whom the information may be communicated.[204] Other statutes may only require that an individual be properly informed of the purposes of data collections. Financial institutions may be exonerated from specific obligations. The British law contains an exception to subject access for the prevention of financial services fraud.[205] In contrast, the French law does not contain such a distinction.[206] Similarly, some laws may require notification and consent even if personal information is not obtained directly from the concerned individual, while other laws may not.[207]

Beyond the scope and nature of the data protection rights, the supervisory rules are not uniform. Some of the laws require government approval or registration prior to the commencement of data processing activities.[208] Others may only require a declaration.[209]

While scholars have also argued that the Treaty of Rome might limit restrictions on intra-European data flows,[210] the Commission of the European Community has recognized the lack of uniform fair information practice standards as a major obstacle to the development of a single European market.[211] The Commission has proposed a directive that seeks to elaborate minimum standards of data protection and to prohibit limitations on intra-European transfers of information. These standards combine a number of features from many of the existing national laws and do not follow any single existing law. If approved, the directive will require member states to enact conforming national laws. Even though member states may continue to develop separate interpretations and more stringent standards of fair information practice, the directive would effectively define "equivalence" for purposes of intra-European data exports; the mandate on unrestrained information flows within Europe re-

204. *See* French Law, *supra* note 14, § 27.

205. *See* British Law, *supra* note 14, § 29.

206. *But see* French Law, *supra* note 14, § 30 (exemption for insurance providers from certain processing limitations).

207. *See, e.g.*, Danish Law, *supra* note 14, § 10(1) (credit reporting agency must notify individuals within four weeks of data collection from sources other than certain public records); Dutch Law, *supra* note 14, § 5(1) (data must only be obtained legitimately).

208. *See, e.g.*, French Law, *supra* note 14, § 16.

209. *See, e.g.*, German Law, *supra* note 14, § 32(1).

210. *See, e.g.*, Briat, *supra* note 186, at 48 (discussion of Treaty of Rome and information flows); Cole, *supra* note 35, 928-41 (same).

211. *See* Draft EC Directive, *supra* note 14, Preamble; *The TEDIS-EDI Legal Workshop*, *supra* note 200.

quires that differences in national standards be ignored—the directive will, in effect, set forth a "minimum equivalent level of protection."

B. *The United States Challenge*

Between the European countries with data export rules and the United States, conflicts have been predicted for over a decade.[212] Recent experience suggests that the predictions of transfer obstacles are becoming a reality for international data flows.[213] The proposed European directive on data processing puts the comparison issue clearly on the international agenda for financial services.

In comparing United States privacy protection to European rules of fair information practice, the obvious starting point is the process: the United States lacks an omnibus law. In the financial services field, however, some of the sectoral laws do cover many of the substantive aspects embodied in the European laws.[214] Nevertheless, in contrast to the thoroughness of omnibus legislation, the ad hoc techniques used in the United States leave significant gaps in comparable coverage for fair information practice standards.[215]

Some of the basic omnibus protection principles for data collection correspond to existing United States rights. Obtaining data fairly and lawfully corresponds to the state privacy right against intrusion upon seclusion.[216] However, the seclusion right only protects against shocking data collections,[217] unlike the lower standard inherent in European notions of "fairness".[218] A few of the financial services laws have similar rights.[219] Significantly, the federal credit reporting law does not address issues of notice and consent.[220] Even with some guidance for fair and legitimate data collection practices in the financial services field, limitations on the collection of sensitive data are rare under United States law in contrast to the European regulation.[221]

---

212. *See, e.g.*, Cole, *supra* note 35, at 918-26; *Teleinformatics*, *supra* note 163, at 214-15; *Transborder Data Flows*, *supra* note 163, at 8-11.

213. *See supra* notes 178-80, 183, 185; *see also* Draft EC Directive, *supra* note 14, § 24 (proposing a mechanism to blacklist countries with unsatisfactory privacy protection for international data flows).

214. *See* Reidenberg, *supra* note 23, at 219-20.

215. *See id.* at 219-20, 234-36.

216. *See supra* note 79 and accompanying text.

217. The right protects against improper conduct in the acquisition of personal information and will not apply to voluntarily disclosed information. *See* Reidenberg, *supra* note 23, at 222-23.

218. *See, e.g.*, Fifth Report, *supra* note 112, at 102-03 (setting forth the Data Protection Principles and their interpretation).

219. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681q (1988) (prohibits obtaining credit reports under false pretenses).

220. *See* Reidenberg, *supra* note 23, at 211. An exception exists for investigative reports of information collected personally from third parties. *See* 15 U.S.C. § 1681(d)(a)(1) (1988).

221. Some state regulations restrict the storage of sensitive data for credit reporting activities. *See, e.g.*, Me. Rev. Stat. Ann. tit. 10, § 1321 (West 1980 & Supp. 1990) prohib-

The limitations on purpose found in omnibus legislation are occasionally seen in United States law. Electronic fund transfer statutes at the state level sometimes restrict the use of collected data[222] and the federal Equal Credit Opportunity Act prohibits the use of certain types of data for discriminatory purposes in the granting of credit.[223] The permissible purposes for which credit reference data may be used can differ.[224] Like the United Kingdom, the use of third-party information for credit decisions would be prohibited in the United States.[225] Unlike France, United States law prohibits the use of data relating to age, sex, nationality and marital status for the purposes of determining credit.[226] In contrast to European laws, United States law allows private sector credit reporting agencies to store and use information about criminal convictions.[227] Personal information gathered by a credit reporting agency in the United States is only supposed to be disclosed for a statutorily enumerated purpose.[228] However, the statute allows disclosures for "any legitimate business need" and does not restrict the secondary use that a legitimate recipient may make of disseminated information. In limited circumstances, the state right against misappropriation of an individual's name may also provide protection.[229] Generally, however, there is no analogous right for the opt-out view of payment-related information.[230]

Few rights exist in the United States that are comparable to the European ban on the collection and storage of unnecessary personal informa-

---

iting the preparation of a report containing sensitive information such as race, religion, sexual preference, political affiliation or belief); N.Y. Gen. Bus. Law § 380j (McKinney 1984 & Supp. 1991) (setting forth information prohibited in consumer reports including data or race, religion, ancestry, or ethnic origin).

222. *See* Reidenberg, *supra* note 23, at 230. *Cf.* Fair Debt Collection Practices Act, 15 U.S.C. § 1692 (1988) (limits use of information regarding debtor's financial situation).

223. *See* 15 U.S.C. 1691(a)(1) (1988).

224. *Compare infra* note 228 and accompanying text (U.S. law allows secondary uses provided that a statutorily authorized purpose has been satisfied) *with supra* note 119 and accompanying text (French and British law restrict narrowly the purposes for which such data may be used.)

225. *Compare* Miller v. American Express Co., 688 F.2d 1235 (9th Cir. 1982) (credit decisions based on third-party characteristics are banned in the United States) *with* Data Tribunal Cases, *supra* note 149.

226. *Compare* 15 U.S.C. § 1691(a)(1) (1988) (limitation on the use of personal information for discrimination in the extension of credit) *with* NS 13, *supra* note 152 (permission to use age, sex, marital status and nationality for credit decisions provided that no decisions are automatic on the basis of credit scoring).

227. *Compare* 15 U.S.C. § 1681c (1988) (allows storage of criminal records) *with* French Law, *supra* note 14, § 30 (limits data processing of criminal records to government authorities or quasi-public enterprises and insurance companies) *and* Dutch Law, *supra* note 14, § 7(1) (allows special limits to be set for the use of criminal records).

228. Those purposes essentially are establishing the individual's eligibility for: (1) credit; (2) employment; (3) insurance; (4) professional licensure; and (5) any other legitimate business need. *See* 15 U.S.C. §§ 1681, 1681b (1988).

229. *See supra* notes 79-80 and accompanying text. This right may protect an individual against the commercial use of one's name without consent if the use "appropriates" characteristics of the individual's personality. *See* Reidenberg, *supra* note 23, at 225-27.

230. *See supra* note 56 and accompanying text.

tion. Some American states ban the collection of extraneous information for purchases made by credit card or check.[231] However, the federal legislation for credit reporting actually sanctions the collection of overbroad, unnecessary information.[232]

Accuracy concerns are seen in United States financial services laws. The Fair Credit Reporting Act and the Fair Credit Billing Act each obligate reporting parties to grant rights of access and objection to consumers.[233] The Electronic Fund Transfer Act provides similar access rights to transaction records.[234] The personal data withheld in a recent British case—ATM transaction records[235]—would be subject to automatic disclosure under United States law.[236] In these situations, the United States result may provide stronger access protections than seen in some European countries. State insurance statutes are also concerned with accuracy.[237] Additionally, at the state level, the right against false light publicity may provide some protection.[238] This right will only protect against disclosures to a broad segment of the public that portray the individual in a false light or misleading way such as the broad dissemination of inaccurate personal information. Sufficiently broad publication of personal information, however, would be rare for the financial services sector.

Unlike the European counterparts, the duration of storage is generally ignored by United States law. Although the credit reporting legislation purports to limit the dissemination of certain types of potentially sensitive obsolete personal information, such as paid tax liens, arrest and conviction records, suits and judgment history, the law allows disclosures beyond the statutory period of seven years (and consequently storage beyond seven years) if requested in connection with specified transactions.[239] These transactions will cover a substantial number of cases. In

231. *See, e.g.*, Cal. Civ. Code § 1747.8 (West Supp. 1992); Del. Code Ann. tit. 11, §§ 914, 915 (Supp. 1991); Fla. Stat. Ann. § 832.075 (West Supp. 1992); Md. Com. Law II Ann. Code § 13-318 (Supp. 1991); N.Y. Gen. Bus. Law § 520-a (McKinney Supp. 1991); Va. Code Ann. § 11-33.1 (Michie Supp. 1991); Wash. Rev. Code Ann. § 62A.3-512 (West Supp. 1992).

232. *See* 15 U.S.C. § 1681a(d) (1988); Reidenberg, *supra* note 23, at 211.

233. *See* 15 U.S.C. § 1666 (1988); 15 U.S.C. §§ 1681e(g), 1681i (1988).

234. *See* 15 U.S.C. § 1693d (1988).

235. *See Halifax Building Society Acquitted in 1st U.K. Data Protection Crown Court Case*, Privacy L. & Bus., Winter 1990/91, at 16-19 (case focused on whether Halifax held the data in conformity to registered purposes and did not challenge the denial of cardholder access). A subsequent Data Protection Tribunal case did address access and only required disclosure to the individual if the person concerned stated good reasons for desiring access. *See* Halifax Building Society v. The Data Protection Registrar, U.K. Data Protection Tribunal Appeal Decision, Jan. 25, 1992.

236. *See* 15 U.S.C. § 1693d (1988).

237. *See* Reidenberg, *supra* note 23, at 233-34.

238. *See* Reidenberg, *supra* note 23, at 224-25; *supra* notes 79-80 and accompanying text.

239. *See* 15 U.S.C. § 1681c (1988).

any event, the European laws may prohibit the storage and disclosure beyond shorter periods of time.

Another critical difference between the United States and omnibus approaches is the supervision mechanism. Existing fair information practice rights in the United States emphasize private litigation as the mechanism for enforcement, rather than administrative action. Consistent with this policy, the United States has no filing or licensing requirement for data processing activities.

Even in financial services contexts that are covered by both the ad hoc United States rights and the European data protection statutes, the interpretation of substantive rights can still be problematic. For example, in France, reporting on individual credit repayment histories is made to the Banque de France. The Banque de France may not maintain adverse information longer than three years.[240] In the United States, such records are maintained by private credit reporting agencies and restrictions may also apply to data storage, but none are as short as three years.[241]

C. *The Asian Challenge*

In a situation similar to the United States, the Asian reliance on ad hoc techniques for the regulation of fair information practice invites tension with the European laws over both procedural and substantive issues.[242] While the European regulators have curiously avoided significant discussion of Asian standards of fair information practice, several Asian jurisdictions have focused on the comparisons. In Japan, international pressures stimulated work on the financial services code of practice.[243] In Hong Kong, the international perspective has been an important factor in the Law Reform Commission's work to shift from the ad hoc technique to a broader legislative approach.[244]

As for the substantive standards, the voluntary guidelines in Hong Kong and the FISC guidelines in Japan each follow the more permissive OECD approach. The FISC policy, for example, does not draw narrow limitations on data collection and permissible uses like the European laws. If a financial institution is authorized to engage in business activity, then any personal information may be collected to further that activ-

240. *See Délibération No. 90-72 du 29 mai 1990, reprinted in* C.N.I.L., 11e Rapport, *supra* note 154, at 150-53.

241. *See* 15 U.S.C. § 1681c (1988).

242. *See, e.g.*, M. Horibe, *Privacy in Japan: The Development of Policy on Personal Data Protection*, 78 Japan Computer Q. 3 (1989) (tracing the development of local and national regulations leading to the present state of Japan's personal data protection); Yamashita, *supra* note 87 (discussing Japan's attempt to formulate guidelines for protecting personal data in the private sector); Mortimer, *supra* note 95 (recommendations of the Privacy Subcommittee of the Hong Kong Law Reform Commission); Berthold, *supra* note 95, at 13-21 (same).

243. *See* FISC, *supra* note 87, at 1.

244. *See* Mortimer, *supra* note 95; Berthold, *supra* note 95, at 13-21.

ity[245] and the use for any data processing purposes in furtherance of authorized activities is permitted.[246] Disclosure of personal information to third parties is expressly permitted, even without the knowledge or consent of the data subject, if such disclosures further authorized business activities of a financial institution and the data subject has no "justifiable" interest worthy of protection.[247] The limitation for justifiable interests seems rather meek. Similar to the European laws, the FISC guidelines recommend rights of access and correction[248] and require limitations on data storage, though, unlike the European laws, the guidelines do allow storage beyond the time required to fulfill legitimate purposes.[249]

Unlike the European laws, the Japanese and Hong Kong guidelines do not recommend supervision or enforcement mechanisms. Additionally, no remedies are suggested for non-compliance with these voluntary standards, though government persuasion may exist and provide some form of sanction.[250] As a result, the substantive rights do not appear to have quite the same legal character as the European laws.

IV. THE FINISH LINE: CONCEPTUAL CHOICES FOR THE REGULATORY CHALLENGE

Whether a regulatory decision to restrict data exports will be based on "equivalency" or "adequacy" of data protection in the destination country, the underlying policy concern for the exporting country is the sufficiency of foreign fair information practice standards. In the realm of transnational financial services, the search for sufficiency will necessarily be complex. Personal information may transit a multitude of countries and be processed in several jurisdictions. As a result, a series of data export rules may apply and a series of complicated comparisons of fair information practice laws may be involved.[251]

The international failures to achieve convergence on the approach and content of fair information practice standards suggests an important conceptual choice for transborder data flows. Whether European regulators take a rigid, superficial view of different sets of regulation or whether they use a more subtle, nuanced assessment will be a critical issue. Rigid

245. *See* FISC, *supra* note 87, § II.1(1) & cmt. B.
246. *Id.* § II.2.(1) & cmt. B.
247. *Id.* § II.2(2) & cmt. C.
248. *Id.* § II.4
249. *Id.* § II.3(1) & cmt. C.
250. *See supra* notes 88-91 and accompanying text.
251. The discussion in this Article assumes that the exporting country has a legitimate interest in regulating fair information practices. Choice of law issues for the applicable national law might otherwise be raised. For example, if a transaction in the United States between U.S. citizens is processed abroad, conflict of law analysis may dictate that U.S. fair information practice regulation should apply exclusively. Similarly, a conflict of law analysis may be able to narrow the comparisons. However, such analyses are beyond the scope of this Article.

comparisons of foreign standards for fair information practice are likely to encourage needless controversy for transnational financial services. The alternative is for government regulators to accept a degree of flexibility and tailor regulatory applications to particular information transfer contexts. A shared vision of flexibility and regulatory customization broadens the possibilities for data exports and allows new legal and extra-legal policy instruments to satisfy fair information practice standards.

A. *Standards of Comparison*

Although various standards of comparison are defined in the international instruments and in national laws to determine the permissibility of data exports, significant ambiguity remains. The OECD Guidelines frame the issue in terms of substantial compliance with the data protection principles;[252] the European Convention gives no guidance for non-signatories and uses an "equivalency" standard for restrictions among signatories;[253] national laws may set no particular standard or may require "equivalency" of protection;[254] and, the proposed harmonization rule for the European Community is likely to adopt an "equivalency" standard.[255] The conventional wisdom suggests that "equivalence" may impose a higher standard for the sufficiency of foreign laws. However, under any of these standards, several interpretations are possible: the satisfactory nature of foreign standards may depend on the similarity of approach to fair information practices, the comparability of substantive rights, or some combination of each.

If the data protection authority of an exporting country chooses to examine only the process side of foreign fair information practices, the foreign regulatory approach then becomes the only relevant criteria. France seems to favor this line of inquiry.[256] Paradoxically, in cases where omnibus legislation exists in the foreign destination, the failure of existing omnibus laws to converge on identical standards suggests that the process inquiry has limited utility. Actual comparability will still depend on the substantive rights under any given omnibus law.

For financial services, a superficial comparison of regulatory schemes would be devastating. Neither the United States nor Asian countries would be able to satisfy such a threshold and information flows would be seriously encumbered for global services. Nevertheless, when the foreign destination does not have omnibus legislation, a comparison of fair information approaches does not presumptively require data flow restrictions. National regulatory schemes that follow the ad hoc method may for a

252. *See supra* note 169 and accompanying text.
253. *See supra* notes 172-75 and accompanying text.
254. *See supra* notes 176-98 and accompanying text.
255. *See supra* notes 193-197 and accompanying text.
256. *See supra* notes 178-80 and accompanying text. The C.N.I.L. decisions were based on the lack of a foreign omnibus law. The reports do not indicate that any inquiry into foreign substantive rights took place.

particular sector have an equivalent "sectoral/omnibus" law. In these cases, a process inquiry must choose between broad and narrow comparisons. A broad comparison favors data flow restrictions, while the narrow view satisfies concerns over foreign fair information practice standards without burdening transnational flows of information. The proposed European directive seems to favor the narrow view; although the basic rule on transborder data flows looks generally at the destination country's fair information practice standards, the derogation procedure contemplates a narrower analysis of data transfers. In the case of the United States, even a narrow view of sectoral comparisons may not sufficiently help financial services.[257]

The process inquiry also leads to a comparison of enforcement and supervision mechanisms. Different approaches to fair information practice regulation tend toward divergent enforcement and supervision mechanisms.[258] Any comparison of these differences is likely to favor data flow restrictions where the European country has a powerful data protection authority and the foreign destination does not. Ironically, the wisdom of encouraging the creation of government supervisory agencies with broad search and seizure powers can be questionable in some societies, such as those with totalitarian histories or unstable governments.

Attempts to define broad standards for comparison are incongruous with the complex character of the information marketplace. In particular, the financial services sector represents global networks with many players. The flow of personal information over financial networks includes data needed for infrastructure purposes as well as data inherent in financial service products. Because the comparison of approaches suggests the desirability of a sectoral interpretation, the context of particular information transmissions is important.

An alternative to the process comparison is a search for parallel substantive standards. This choice of a comparison standard for data export regulation emphasizes a context-based evaluation.[259] Any comparative analysis of substantive rights would necessarily focus on the type of data transfer and the available sectoral rights in the destination. The choice of this comparison raises administrative costs. Case-by-case analysis would be required for foreign data transfers.[260] However, generic solutions

257. *See supra* text accompanying notes 212-41.

258. *See supra* notes 92-93, 99-102 and accompanying text.

259. *See* Reidenberg, *A Commentary on Data Protection, Privacy and Regulatory Conflicts between the European Community and the United States*, Access Reports, May 1991, at 8-9.

260. *See* U.K. Data Protection Registrar, Home Office Consultation CEC COM 314 final—SYN 287, 288, ¶ 4.2.9 (Dec. 3, 1990) (criticizing both the complete black-listing of countries and the alternative case-by-case vetting procedure in the Draft EC Directive, particularly with respect to financial services and travel). *But see* Remarks by Malcolm Norris, Data Protection Registrar, Office of the Isle of Man Data Protection Registrar, to the Electronic Democracy Conference, Washington, D.C., Sept. 5, 1991 (indicating that under a future EC data protection directive, case-by-case decisions will likely be needed as the short-term route for EC-USA data flows); Remarks by Ulla Ihnen, Directorate

would not work well with the complex information processing arrangements that are common in the financial services sector. Furthermore, as computer technology itself develops, the difficulties of case-by-case analysis can be reduced with techniques such as computerized decision support systems.[261]

Each of these regulatory choices points toward a need for flexibility in dealing with fair information practices. Both the process and substantive choices for comparisons of fair information standards suggests a focus on narrow contexts.

B. *Reconciling Diversity*[262]

Flexibility suggests that a variety of techniques, in addition to the legal comparisons, will be necessary for fair information practice rules to keep pace with a rapidly changing technological and business environment. As financial services networks evolve, the nature of the information flows will change and the national treatment of fair information practices will evolve. If history is a guide, the evolution of national fair information practice regulation is not likely to result in uniform, international standards. Instead, international convergence on a set of techniques to manage persistent differences can provide a means for reconciling the diversity of fair information practice standards around the world; convergence on the tools to manage national differences offers a bridge across divergent national standards.

This view of a shared international regulatory analysis attempts to create a customized set of fair information practice standards for fair information flows. The tailored "customized regulation" may include combinations of the functional legal comparisons, contractual devices, technological solutions, information network configurations, and societal

---

Gen. for Internal Market & Indus. Aff., Comm'n of the Eur. Communities, to the 4th Annual Privacy Laws & Business Data Protection Conference, Cambridge University, July 3, 1991, at 12 (commenting that category reviews will be likely under any final EC data protection directive).

Various procedural issues are also directly related to the choice of an appropriate standard of comparison. Transborder data flow restrictions necessitate that regulatory authorities make judgments about foreign law. The procedures and sources of information for agency findings have significant consequence. If, for example, the foreign jurisdiction has no corresponding government authority, as is presently the case with the United States, a decision based on arguments by interested private parties may not reflect accurately on nuances and varying interpretations of the state of the law in the foreign jurisdiction. Problems will clearly arise for countries where the law on fair information practices is evolving and no single, definitive interpretation exists.

261. *See* G. Greenleaf & A. Mowbray, The Privacy Workstation (Paper presented at 4th Annual Privacy Laws & Business Data Protection Conference, Cambridge University, July 4, 1991).

262. This theory of managing regulatory differences derives from a presentation made by the author to a meeting on "Networld Order Scenarios" in Paris, June 7, 1991. *See* Reidenberg, *Personal Information and Global Interconnection: The Challenge of Regulatory Convergence*, Project Promethee Perspectives, Dec. 1991, at 27-36.

constraints.[263]

The starting point for a shared vision of diversity management is the comparison of substantive rights on a functional basis. If similar standards exist for the particular information being transferred in the context of specific uses, then there is no need for any bridge. The treatment of transaction data, for example, from credit card purchases may be protected similarly in different jurisdictions through various combinations of legal rights. However, the differences among national laws suggest that no true uniformity of fair information standards will exist even for these narrow sectoral uses of information. As a result, gaps will need to be covered.

The contractual solution is one method to resolve conflicting levels of privacy protection.[264] Data transfers may be permitted if contract rights are granted to supplement the existing fair information practice laws of the destination.[265] The contractual approach, however, assumes that data transfers are rather discrete transactions between two entities. Financial services organizations tend not to follow this model.[266] Financial services networks are often comprised of numerous parties sharing and creating information in symbiotic ways. As a result, a simple contract between the exporter and recipient of personal information may not be appropriate for the circumstances.[267] The success of contractual devices also depends on the legal enforceability of these private contracts. In some jurisdictions, this may be troublesome because individuals are usually third-party beneficiaries to a transborder data flow contract between the data exporter and recipient. Some countries do not allow the enforcement of third party beneficiary rights.[268] Consequently, additional techniques need to be available for increased flexibility.

Beyond the functional legal protections and contractual rights, the technology itself may be used to satisfy fair information practice standards. In some cases, the choice of technology can be used to minimize conflicts. For example, the increasing use of smart cards in the financial

263. *Id.* at 34-35.

264. *See* Note, *Contracts for Transnational Information Services: Securing Equivalency of Data Protection*, 22 Harv. Int'l L.J. 157, 171-75 (1981); Brian Napier, Contractual Solutions to the Problem of Equivalent Data Protection in Transborder Data Flows (paper presented at conference on "Legal Challenges and Opportunities Created by the Prolific Growth of Electronic Information Services," organized jointly by the Council of Europe and the Commission of the European Communities, Luxembourg, March 27-28, 1990) (on file with the *Fordham Law Review*); Model Contract Designed to Ensure Equivalent Data Protection for TBDF, Privacy L. & Bus., Oct. 1991, at 6-7.

265. This solution was used by the C.N.I.L. in the Fiat decision. *See supra* note 178. Austria has taken the same approach. *See* Compte rendu, *supra* note 16, at 308.

266. *See* Brandon & Halvey, *The Outsourcing Decision: Avoiding Pitfalls*, Am. Banker, Jan. 15, 1992, at 4-5 (describing outsourcing practices).

267. *See* Reidenberg, *An American Solution to TBDF Contractual Problems*, Privacy L. & Bus., Dec. 1991, at 12-14.

268. *See* Napier, *supra* note 264.

services community offers the means to erase data and thus minimize the significance of any discrepancies in laws on the duration of data storage.

In a similar way, the configuration of financial services networks can be useful to accommodate asymmetrical national standards of fair information practices. If the network configuration limits the duration of storage of personal information through data purging, then differences in national standards for data storage become irrelevant. Similarly, if the network prevents secondary uses of personal information such as marketing activities through blocking, then differences in national standards are unimportant. In many instances, financial services use personal information on a global basis in innocuous ways for administrative purposes.[269] For these cases, the network may also be structured so that information is coded and barriers to access and use are established in order to preclude practices that might be inconsistent with fair information standards. By preventing certain information collections or uses without legal intervention, actual conflicts over fair information regulation become irrelevant.

These legal and technical solutions may also be supplemented by societal pressures. In seeking to retain a positive public image, companies have an incentive to adopt a certain degree of fair information practice standards.[270] Similarly, in some countries, such as Japan, the government involvement in private sector codes may provide sufficient quasi-legal pressure for companies to comply with fair information practice.[271] Although social pressure cannot be asserted as a panacea, it may be helpful and powerful in conjunction with the other tools. In many instances, though, fair information practices may be challenged by "transparent" companies, or those buried deep in the infrastructure of data processing. But, for these hidden companies, there is only a small public image issue and the social pressure would be weak.

CONCLUSION

National and international regulation of fair information practices directly affect the provision of transnational financial services. Standards of fairness for data processing are evolving both at the national and international levels. Different approaches to regulation and varying substantive rights exist at both levels.

Although some efforts have been made by the OECD and the Council of Europe, the harmonization of national information processing laws has not been successful. The approach and substantive rights continue to differ in countries around the world. The recent proposals from the Eu-

269. *See* Berkvens, *supra* note 6 (administrative acts in connection with payment operations defy relevancy of general data protection principles.)

270. *See, e.g.*, Am. Express, *supra* note 85 (describing the company's policy not to disclose any customer information without prior consent from the customer).

271. *See supra* notes 88-91 and accompanying text.

ropean Commission are similarly not likely to result in identical standards across Europe.

As part of the regulation of fair information practices, the international instruments and national laws establish mechanisms to prohibit data exports to countries without satisfactory standards of fair information practice. The mechanisms rely on comparisons of national laws. In light of the global community's failure to achieve convergence on standards of fair information practice, these comparisons are likely to encourage export prohibitions. For financial services, such restrictions would be crippling.

The standards for comparing national fair information practice regulation suggests a number of choices. These choices favor examinations based on the particular context for information flows. The comparisons also suggest that regulatory flexibility is desirable to bridge inconsequential national differences.

Regulatory flexibility can be enhanced by the use of legal, technological, and societal techniques. A shared vision of the appropriate techniques can be quite useful to reconcile otherwise conflicting regulatory schemes. This notion of convergence establishes a mechanism to customize fair information practice standards for specific contexts. As a result, the irreconcilable differences between the debates in the national and international contexts can be avoided.