Fordham International Law Journal

Volume 21, *Issue* 3 1997 *Article* 10

The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?

Patrick J. Murray*

*

The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?

Patrick J. Murray

Abstract

This Comment addresses how the US protection of personal data will fare when judged against the adequacy standard of the Directive. Part I explains what data protection is and traces the development of data protection law in Europe and the United States. It then analyzes the current approaches to data protection in both the Community and the United States. Part II discusses different approaches to assessing adequacy. It proposes that the Article 29 Working Party presents the only clear explanation of how to assess when a third country ensures adequate protection of personal data. Part II then describes the Working Party's approach to assessing what constitutes adequate protection. Part III argues that under the Working Party's approach, the United States ensures an adequate level of protection in the public sector and in some areas in the private sector. It asserts that the level of protection in much of the private sector will not be considered adequate under the Directive. This Comment concludes that under the Working Party's suggested approach, Member States should find that US data protection is not adequate overall, but does ensure adequate protection in the public sector and a few areas of the private sector.

COMMENTS

THE ADEQUACY STANDARD UNDER DIRECTIVE 95/46/EC: DOES U.S. DATA PROTECTION MEET THIS STANDARD?

*Patrick J. Murray**

INTRODUCTION

Recent developments in information technology,[1] particularly in computers and networks,[2] threaten informational privacy.[3] These technologies permit data controllers[4] ("control-

* J.D. Candidate, May 1999, Fordham University School of Law.

1. *See* COLIN J. BENNETT, REGULATING PRIVACY 16 (1992) (defining informational technology as "hardware and software associated with all features of automatic digital data processing and communication"). Information technology includes the people using the technology, their equipment, and the techniques that they use. *Id.*

2. *See* Susan H. Borgos, *Computer Networks for Lawyers*, 24 COLO. LAW. 1557, 1557-58 (1995) (discussing types of networks and practical network components); Henry H. Perritt, Jr., *What Lawyers Need to Know About the Internet: Basic Technological Terms and Concepts*, 443 PRACTICE L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 23, 26-29 (June 5, 1996) (describing structural features of networks). A network is a group of computers connected together so that the people using them can communicate with one another, transfer files, and share resources. Borgos, *supra*, at 1557. Networks may be local area networks or wide area networks. Perritt, *supra*, at 26-27. While local area networks serve a limited number of computers in reasonable proximity to each other, wide area networks often span larger areas. *Id.*; *see also* Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 111-12 (1995) (discussing how networks that replaced mainframe computers decentralized information processing and facilitated surveillance).

3. *See* ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD 49 (1997) (explaining that powerful computers and high-speed networks make monitoring people's activities easy); *see* BENNETT, *supra* note 1, at 22-37 (discussing three aspects of informational technology problem). Informational privacy is an individual's claim to control the terms under which personal information is acquired, disclosed, and used. NATIONAL TELECOMM. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995) [hereinafter NTIA REPORT]; *see* PRISCILLA M. REGAN, LEGISLATING PRIVACY 5 (1995) (defining informational privacy as "involving questions about the use of personal information collected by organizations such as credit card companies, banks, the federal government, educational institutions, and video stores."). Europeans frequently refer to informational privacy as data protection. *See* BENNETT, *supra* note 1, at 12-14 (mentioning data protection as more accurate term for policies designed to regulate collection, storage, use, and transfer of personal information).

4. Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Indi-

lers") to collect, store, use, and disseminate personal data[5] outside of an individual's control.[6] Although this new technology has many advantages,[7] data controllers also can misuse technological advances to violate an individual's informational privacy.[8]

In response to increased threats to informational privacy, countries began to regulate the processing of personal data[9] dur-

---

viduals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(c), O.J. L 281/31, at 38 (1995) [hereinafter Directive]. Controller means "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." *Id.*

5. Directive, *supra* note 4, art. 2(a), O.J. L 281/31, at 38 (1995). Personal data is any information relating to an identified or identifiable natural person. *Id.*

6. BENNETT, *supra* note 1, at vii.

7. *See* CAVOUKIAN & TAPSCOTT, *supra* note 3, at 65 (discussing advantages of developments in information technology); BENNETT, *supra* note 1, at 20 (noting universal recognition of advantages derived from use of information technology). Information technology can relieve workers of tedious tasks, increase speed and efficiency of production, and enhance analytic capabilities of a company. *See* BENNETT, *supra* note 1, at 20 (relating advantages derived from information technology for government). Consumers can purchase goods with debit cards that withdraw money directly from their accounts. *See* INFORMATION POLICY COMM., NATIONAL INFO. INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE 6 (1997) [hereinafter IITF OPTIONS] (describing how information technology has facilitated collection of personal information by private sector). An individual can order a pay-per-view movie to watch at home without leaving the house. *See id.* (noting that new information technology allows consumers to buy new information services). One person can send messages by e-mail to another next door, across the country, or around the world almost instantaneously. *See id.* (stating that developments in information technology have increased the volume of electronic transactions such as e-mail). Doctors using tele-medicine can diagnose distant patients. *See* PRESIDENT WILLIAM J. CLINTON & VICE PRESIDENT ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 2 (1997) [hereinafter FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE] (describing Internet's effect upon Global Information Infrastructure).

8. IITF OPTIONS, *supra* note 7, at 6; *see* BENNETT, *supra* note 1, at 35 (describing increased dangers caused by information technology). For example, a store offering a discount card might request that customers provide personal information unrelated to the card's purpose. *See* CAVOUKIAN & TAPSCOTT, *supra* note 3, at 31-32 (explaining that store's request violates collection limitation principle because store should collect only necessary information). Hospitals may even sell patients' sensitive health records to defer costs. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 14 (1996) (stating purpose limitation principle that proscribes using personal data for purposes incompatible with original purpose). The U.S. Federal Bureau of Investigation might store criminal records indefinitely on government databases. *See id.* (explaining that excessive storage of personal information is improper because information loses accuracy and relevancy with time).

9. Directive, *supra* note 4, art. 2(b), O.J. L 281/31, at 38 (1995). The processing of personal data, or data processing, includes "any operation or set of operations which is performed upon data, whether or not by automatic means." *Id.*

ing the 1970s.[10] The German state of Hesse[11] enacted the first comprehensive data protection[12] law in 1970.[13] Since then, many European countries have adopted omnibus[14] data protection laws[15] based upon certain fundamental data protection principles.[16] These national laws occasionally prohibited data

10. *See* BENNETT, *supra* note 1, at 57 tbl.1 (listing years that countries enacted data protection legislation). Early political action on data protection can be attributed to the confluence of four factors in the late 1960s. *Id.* at 46-55. Plans for centralized databanks, proposals for personal identification numbers, upcoming censuses, and alarmist literature motivated political action on privacy. *Id.*

11. Joachim Schrey & Joachim Felges, *Germany, in* DATA TRANSMISSION AND PRIVACY 213, 213 (Dennis Campbell & Joy Fischer eds., 1994). Germany is a federation of states, called Länder. *Id.* The German Länd, Hesse, is one of these states. *See* Helge Seip, *Data Protection, Privacy and National Borders, in* 25 YEARS ANNIVERSARY ANTHOLOGY IN COMPUTERS AND LAW 67, 68 (Jon Bing & Olav Torvand eds., 1995) (noting that Hesse established world's first data protection law).

12. *See* BENNETT, *supra* note 1, at 14 (noting that data protection is analogous to informational privacy).

13. Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 447 (1995); *see* BENNETT, *supra* note 1, at 124-25 (explaining effect of Hessian statute on subsequent data protection legislation in Germany).

14. *See* A.C.M. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC 18-19 (1990) (distinguishing between omnibus data protection legislation adopted by European countries and sectoral data protection measures adopted by United States). Omnibus data protection laws apply to both the government and the private sector, not just to specific sectors. *See id.* at 19 (noting other differences between European legislation and U.S. model); *see also* Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level?: Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 130 (1996) (explaining that most countries have adopted comprehensive data protection laws); BENNETT, *supra* note 1, at 113-14 (noting that most countries besides United States, Canada, and Australia apply data protection principles to both private and public sector).

15. *See* BENNETT, *supra* note 1, at 57 tbl.1 (listing European data protection laws and date of passage). For example, Sweden, Germany, France, Spain, the United Kingdom, and the Netherlands have adopted omnibus data protection laws. Datalagen, Svensk Forfeittuings Samling (SFS) 1973: 289 (amended version SFS 1982: 446) (Swe.); Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz), v. 27.1.77 (BGBl. I S.201) (Gr.); Loi No. 78-17 du janvier 1978 relative à l'informatique, aux fichers et aux libertés, Loi. No. 78-17 of January 1978, 1978 Journal Officiel de la Republique Francaise [O.J.] 227, 1978 Bulletin legislatif Dalloz [B.L.D.] 77 (Fr.); Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la Intimidad personal y familiar y a la propia Imagen (BOE 115 & 129, of 14 May 1982 and 30 May 1985) (Sp.); Data Protection Act of 1984, c. 35. 1984 (U.K.); Wet Persoonsregistraties, Act of 28 December 1988, Stbl. 665, amended by the Act of October 1989, Stbl. 480 (Neth.).

16. *See* BENNETT, *supra* note 1, at 95-115 (discussing convergence of data protection policies). Countries have formulated data protection policies in different ways, but these formulations reflect similar fundamental principles. *See id.* at 96-101 (relating national variations of data protection principles). One scholar condenses the various na-

controllers from transferring personal data to countries without equivalent data protection.[17] As each country adopted its own data protection measures, disparities arose between the national laws.[18] These national laws created potential obstacles to the free flow of information[19] because controllers could not transfer personal data to countries that did not have sufficient protection.[20]

The European Community[21] ("EC" or "Community") en-

---

tional policies into six fundamental data protection principles. *Id.* at 101. These six principles are the principle of openness, the principle of individual access and correction, the principle of collection limitation, the principle of use limitation, the disclosure limitation principle, and the security principle. *See id.* at 101-11 (discussing presence of data protection principles in policies of United States, Great Britain, Germany, and Sweden); *see also* SCHWARTZ & REIDENBERG, *supra* note 8, at 12-17 (explaining European fair information practices).

17. *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 481 (1995) [hereinafter Schwartz, *Restrictions on International Data Flows*] (discussing principles in context of European national data protection laws). For instance, the French government prohibited Fiat S.p.A. from transferring employee information from a French subsidiary to its Italian headquarters because the French government considered Italian data protection to be insufficient. Amy Fleischmann, Note, *Personal Data Security: Divergent Standards in the European Union and the United States*, 19 FORDHAM INT'L L.J. 143, 150 (1995). In addition, Norway, Austria, Germany, Sweden, and the United Kingdom have imposed restrictions on international data transfers. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COM. L.J. 195, 199 n.16 (1992) [hereinafter Reidenberg, *Fortress or Frontier*].

18. *See* Organization for Economic Co-operation & Dev., Explanatory Memorandum to Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, O.E.C.D. Doc. C(80)58 final, Sept. 23, 1980, *reprinted in* 20 I.L.M. 422, 427 [hereinafter OECD Guidelines Explanatory Memorandum] (explaining that data protection laws that OECD member states adopted assumed different forms).

19. *See* NUTGER, *supra* note 14, at 225-26 (describing free flow of information as one of two competing interests of data protection). Article 10(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") protects the free flow of information:

> Everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 10(1), 213 U.N.T.S. 221, 230 [hereinafter ECHR].

20. *See* OECD Guidelines Explanatory Memorandum, *supra* note 18, at 427 (noting that disparities in legislation created obstacles to free flow of information); Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 472 (discussing regulation of international data flows).

21. Treaty Establishing the European Community, Feb. 7, 1992, [1992] 1 C.M.L.R. 573 [hereinafter EC Treaty], *incorporating changes made by* Treaty on European Union, Feb. 7, 1992, O.J. C 224/1 (1992), [1992] 1 C.M.L.R. 719, 31 I.L.M. 247 [hereinafter TEU]. The TEU, *supra*, amended the Treaty Establishing the European Economic

acted legislation to overcome these obstacles to the free flow of information while still protecting personal data.[22] The EC's Council of the European Union[23] ("Council") and the European Parliament[24] ("Parliament") adopted Directive 95/46/EC[25] ("Di-

---

Community, Mar. 25, 1957, 298 U.N.T.S. 11 [hereinafter EEC Treaty], *as amended by* Single European Act, O.J. L 169/1 (1987), [1987] 2 C.M.L.R. 741 [hereinafter SEA], *in* TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES (EC Off'l Pub. Off. 1987). The Treaty on European Union ("TEU") represents a stage in the process of creating an "ever closer union among the peoples of Europe." TEU, *supra*, art. A, ¶ 2, O.J. C 224/1, at 5 (1992), [1992] 1 C.M.L.R. at 727. The TEU established the European Union ("EU" or "Union") comprised of the three elements (or "pillars"). P.S.R.F. MATHIJSEN, A GUIDE TO EUROPEAN UNION LAW 4 (6th ed. 1995); *see* TEU, *supra*, art. A, ¶ 3, O.J. C 224/1, at 5 (1992), [1992] 1 C.M.L.R. at 727 (stating that "[t]he Union shall be founded on the European Communities, supplemented by the policies and forms of co-operation established by the Treaty."). The three pillars that the Europe Union is founded upon are the European Communities, a Common Foreign and Security Policy, and Co-operation in the Field of Justice and Home Affairs, respectively. MATHIJSEN, *supra*, at 4. The European Communities, the first pillar of the Union, refers to three European communities already in existence; the European Coal and Steel Community ("ECSC"), the European Atomic Energy Community ("Euratom"), and the European Economic Community ("EEC"). *Id.* As of the signing of the TEU, the term European Community ("EC" or "Community") replaces the term European Economic Community. TEU, *supra*, art. G, O.J. C 224/1, at 6 (1992), [1992] 1 C.M.L.R. at 728; MATHIJSEN, *supra*, at 4. Because the European Community conducts almost all aspects of the European Communities, the prevalent term referring to the Communities is the "Community". MATHIJSEN, *supra*, at 4.

The 12 Member States that signed the TEU were Belgium, Denmark, Germany, Greece, Spain, France, Ireland, Italy, Luxembourg, the Netherlands, Portugal, and the United Kingdom. TEU, *supra*, pmbl., O.J. C 224/1, at 2 (1992), [1992] 1 C.M.L.R. at 725-26. On January 1, 1995, Austria, Finland, and Sweden increased the EU membership to fifteen states. EC Treaty, *supra*, art. 148(2), at 680, [1992] 1 C.M.L.R. 573 *as amended by* Act Concerning the Conditions of Accession of the Kingdom of Norway, the Republic of Austria, the Republic of Finland, and the Kingdom of Sweden and the Adjustments to the Treaties on Which the European Union is Founded, art. 15, O.J. C 241/21, at 24 (1994) *as amended by* Council Decision of 1 January 1995, art. 8, O.J. L 1/1, at 3 (1995).

22. Directive, *supra* note 4, recitals para. 8, O.J. L 281/31, at 32 (1995).

23. *See* EC Treaty, *supra* note 21, arts. 145-154, [1992] 1 C.M.L.R. at 679-82 (setting forth powers of Council of Ministers). The Council of Ministers ("Council") consists of ministers representing each Member State. GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 51 (1993) [hereinafter BERMANN ET AL.]. The Council functions as the collective head of state of the European Community by conducting external relations. *Id.* The Council shares legislative power with the Parliament, and in some areas, exercises exclusive power. *See* MATHIJSEN, *supra* note 21, at 57-59 (describing powers of Council).

24. EC Treaty, *supra* note 21, art. 137, [1992] 1 C.M.L.R. at 676. The role of the European Parliament ("Parliament"), originally called the Assembly, is to express the political sentiments of the Member State populations. BERMANN ET AL., *supra* note 23, at 63. Parliament is composed of 626 members selected by direct election. *Id.* at 64; GEORGE A. BERMANN ET AL., 1998 SUPPLEMENT TO CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 32 (1998) [hereinafter BERMANN ET AL., 1998 SUPPLEMENT]. Besides

rective") to harmonize[26] the national data protection laws of EC Member States.[27] The drafters recognized that if the Directive harmonized the Members States' laws,[28] then Member States could transfer data to other Member States while still safeguarding the fundamental rights and freedoms[29] of their citizens.[30] If controllers in a Member State transferred data to a third country[31] that failed to protect personal data, however, then the Members State's protection of personal data would be effectively lost once the Member State transferred the data to the third country.[32] Consequently, the Directive includes provisions on

---

serving as a forum for discussing topics of interest to the peoples of the Member States, the Parliament shares limited legislative power with the Commission and the Council. *Id.* at 66-67. This legislative power has been increased through the various amendments to the original EEC Treaty. *Id.* at 66-68. *See generally*, EC Treaty, *supra* note 21, arts. 137-144, [1992] 1 C.M.L.R. at 676-79 (governing powers of Parliament).

25. Directive, *supra* note 4, O.J. L 281/31 (1995); *see* Rosario Imperiali d'Afflitto, *European Union Directive on Personal Privacy Rights and Computerized Information*, 41 VILL. L. REV. 305 (1996) (analyzing articles of Directive 95/46/EC (the "Directive")).

26. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 481 (defining harmonization). Harmonization is a term of EC law that refers to legally binding measures that require the Member States to enact substantially similar legal rules. *Id.* The translations of the Treaty Establishing the European Economic Community ("EEC Treaty") used the term approximation, not harmonization, but the later term better conveys the meaning used in the EEC Treaty languages. *See* BERMANN ET AL., *supra* note 23, at 430 (explaining concept of harmonization under Article 100 of EEC Treaty). The Directive refers to the original translation of this principle of harmonization where it mentions the need for "Community action to approximate" data protection laws of Member States. Directive, *supra* note 4, recitals para. 8, O.J. L 281/31, at 32 (1995).

27. *See* Directive, *supra* note 4, recitals para. 8, O.J. L 281/31, at 32 (1995) (stating that "[c]ommunity action to approximate [data protection] laws is therefore needed").

28. *See* TEU, *supra* note 21, pmbl., O.J. C 224/1, at 2 (1992), [1992] 1 C.M.L.R. at 725 (listing 12 Member States as of 1992); BERMANN ET AL., 1998 SUPPLEMENT, *supra* note 24, at 4 (noting accession of Austria, Finland, and Sweden in 1995). The 15 current Member States of the European Union are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom. BUTTERWORTH'S EXPERT GUIDE TO THE EUROPEAN UNION 136 (Jörg Monar et al. eds., 1996); *see* BERMANN ET AL., 1998 SUPPLEMENT, *supra* note 24, at 26, 31 (listing new allocation of votes and Parliamentary seats for each of 15 Member States).

29. Directive, *supra* note 4, recitals para. 1(1), O.J. L 281/31, at 38 (1995). The Directive refers to the fundamental rights recognized in Member State constitutions and in the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Id.* recitals para. 1, O.J. L 281/31, at 31 (1995); ECHR, *supra* note 19.

30. Directive, *supra* note 4, recitals paras. 9-10, O.J. L 281/31, at 32 (1995).

31. *Id.* art. 25(1), O.J. L 281/31, at 45 (1995). The Directive does not define "third country", but uses the term to refer to non-Member States of the European Community. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 41 (1997) (referring to third countries under Article 25(1) as "nonmember states").

32. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 472 (dis-

preventing data from being sent to countries without sufficient data protection.[33]

Article 25 of the Directive prohibits Member States from transferring data to a third country unless the third country ensures an adequate level of protection.[34] While Article 26 of the Directive[35] ("Article 26") provides exceptions to the requirement of adequate protection in third countries,[36] the Article 25 requirement that a third country have adequate protection could lead to a data or information embargo.[37] For instance, if the laws of a third country, perhaps the United States, do not provide adequate protection of personal data, then a controller in a Member State could not transfer personal data to the United States unless an exception applied.[38]

This information embargo could have serious consequences in both the Member States and the United States.[39] For example, a Member State government might not be able to send in-

---

cussing need for data protection laws to ensure data transfers beyond borders of Europe).

33. Directive, *supra* note 4, arts. 25-26, O.J. L 281/31, at 45-46 (1995); *see* Explanatory Memorandum of Amended Commission Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 Final-SYN 287, at 34 (Oct. 15, 1992) [hereinafter Explanatory Memorandum of Amended Proposal] (stating that "[w]ithout such a provision the Community's efforts to guarantee a high level of protection for individuals could be nullified by transfers to other countries in which the protection provided is inadequate.").

34. *See* Directive, *supra* note 4, art. 25(1), O.J. L 281/31, at 45 (1995) (stating that "the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection.").

35. *Id.* art. 26, O.J. L 281/31, at 46 (1995).

36. *See id.* art. 26, O.J. L 281/31, at 46 (1995) (setting forth exceptions from Article 25 of Directive).

37. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 472 (referring to data embargo order as orders that block or limit foreign transfers of data).

38. *See* Directive, *supra* note 4, arts. 25-26, O.J. L 281/31, at 45-46 (1995) (setting forth requirement that third country have adequate level of protection, but providing certain exceptions to this requirement).

39. *See* Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 438 (1995) (discussing consequences to U.S. businesses); Robert G. Boehmer & Todd S. Palmer, *The 1992 EC Data Protection Proposal: An Examination of its Implications for U.S. Businesses and U.S. Privacy Law*, 31 AM. BUS. L.J. 265, 308-11 (1993) (explaining Directive's implication for information systems management, human resource management, strategic management, and U.S. data protection law); Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 331-33 (1995) [hereinafter Schwartz, *Health Care Reform*] (discussing consequences of Directive regarding medical data).

formation to the United States about individuals in the third country.[40] A Member State might prevent a private bank in the Member State from transmitting information about its customers to U.S. financial institutions.[41] Likewise, a Member State might prohibit a European employer from sending information about its employees to U.S. subsidiaries.[42]

Whether Member States prohibit data transfers to a third country depends upon whether the third country has adequate protection.[43] Although experts have written about the Directive extensively,[44] they have not reached a consensus as to what will qualify as adequate protection of personal data.[45] In part, this lack of agreement results from the Directive's ambiguity.[46] Recently, however, the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data[47] ("Working

40. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 475-76, 489 (describing German, British, and Dutch data protection laws that permit data protection authorities to prevent international transfers by government).

41. *See Data Protection: Draft EEC Directive Strongly Criticized by Banking Sector*, EUR. INFO. SERVICE, TECH EUR., June 1, 1991 *available in* LEXIS, Intlaw Library, ECNews File (discussing possibility that Directive will prevent electronics transfers of funds to countries without adequate protection).

42. *See* Laura B. Pincus & Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Worker*, 33 AM. BUS. L.J. 51, 83 (1995) (stating that U.S. business with offices in EC Member States will have problems transferring even employee rosters to offices in United States).

43. Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45 (1995).

44. *See, e.g.*, Simitis, *supra* note 13 (discussing compromises reached to enact Directive); Cate, *supra* note 39 (outlining provisions of Directive and potential problems that Article 25 may have upon international data transfers); Schwartz, *Restrictions on International Data Flows*, *supra* note 17 (comparing restrictions on international data flows of both European data protection laws and EC Directive); Gellman, *supra* note 14, at 129 (analyzing need for international data protection regulation).

45. *See* CATE, *supra* note 31, at 98 (noting that Europe and United States share many, but not all, data protection principles); Gellman, *supra* note 14, at 157 (noting uncertainty of how provisions on adequate protection will be interpreted and applied).

46. *See* Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45 (1995) (requiring data transfers to third countries only if third country has adequate level of protection, but not exploring meaning of adequate protection). The Directive does not explicitly set forth a standard for adequate protection. *Id.*

47. *Id.* arts. 29-30, O.J. L 281/31, at 48-49 (1995). Article 29 of the Directive establishes the Working Party "on the Protection of Individuals with Regard to the Processing of Personal Data ("Working Party")." to examine the application of national data protection measures and make recommendations to the European Commission ("Commission") to improve implementation of the Directive. *Id.*

The Commission, the executive organ of the European Community, oversees and implements the requirements of EC foundational treaties. *See* BERMANN ET AL., *supra*

Party") adopted a paper discussing possible ways to assess adequacy.[48] That paper provides insight into how Community institutions and the Member States might assess adequacy.[49]

This Comment addresses how the U.S. protection of personal data will fare when judged against the adequacy standard of the Directive. Part I explains what data protection is and traces the development of data protection law in Europe and the United States. It then analyzes the current approaches to data protection in both the Community and the United States. Part II discusses different approaches to assessing adequacy. It proposes that the Article 29[50] Working Party presents the only clear explanation of how to assess when a third country ensures adequate protection of personal data. Part II then describes the Working Party's approach to assessing what constitutes adequate protection. Part III argues that under the Working Party's approach, the United States ensures an adequate level of protection in the public sector and in some areas in the private sector. It asserts that the level of protection in much of the private sector will not be considered adequate under the Directive. This Comment concludes that under the Working Party's suggested approach, Member States should find that U.S. data protection is not adequate overall, but does ensure adequate protection in the public sector and a few areas of the private sector.

---

note 23, at 57 (listing executive tasks of Commission); MARTIN WESTLAKE, THE COUNCIL OF THE EUROPEAN UNION 339 tbl.XIV.2.1 (1995) (enumerating Commission powers and duties, including advisory, management, regulatory, and safeguarding measures). The Commission has 20 members, two from each of France, Germany, Italy, Spain, and the United Kingdom, and one from each of the other Member States. *See* BERMANN ET AL., *supra* note 23, at 58 (noting that smaller Member States nominate one member of Commission while larger Member States nominate two); BERMANN ET AL., 1998 SUPPLEMENT, *supra* note 24, at 28 (explaining that Commission has 20 members because three new Member States will nominate only one member each). The Commission exercises its broad legislative and administrative powers with independence from the Member States. *See id.* at 57-60 (discussing composition, operation, and development of Commission). *See generally* EC Treaty, *supra* note 21, arts. 155-163, [1992] 1 C.M.L.R. at 682-84 (governing powers of Commission).

48. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy, XV D/5020/97-EN Final, adopted on June 26, 1997 [hereinafter First Orientations].

49. *See id.* (suggesting approach to assess whether third country provides adequate level of protection).

50. Directive, *supra* note 4, art. 29, O.J. L 281/31, at 48 (1995).

I. *DATA PROTECTION IN THE UNITED STATES AND THE EUROPEAN COMMUNITY*

For the past three decades, both the United States and European countries have addressed privacy concerns and developed measures to protect personal data.[51] In 1995, the Community adopted the Directive as an omnibus data protection measure to harmonize Member State data protection laws.[52] In contrast, the United States continues to pursue its ad hoc, sectoral approach[53] to data protection.[54]

A. *Background of Data Protection*

The modern concept of privacy emerged in the United States at the end of the nineteenth century.[55] Data protection, or informational privacy, however, did not become an issue in

---

51. *See* BENNETT, *supra* note 1, at 3 (noting that data protection developed in late 1960s).

52. *See* Directive, *supra* note 4, art. 1(1), O.J. L 281/31, at 38 (1995) (noting Directive's objective to protect processing of personal data).

53. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995) [hereinafter Reidenberg, *Setting Standards*] (providing background on U.S. ad hoc, targeted approach to data protection); Reidenberg, *Fortress or Frontier*, *supra* note 17, at 209-20 (analyzing U.S. data protection by sector); NUGTER, *supra* note 14, at 18-19 (comparing U.S. sectoral approach to omnibus data protection law of most European countries); CATE, *supra* note 31, at 49-100 (examining U.S. privacy regulation in public and private sectors). The United States has approached data protection by adopting ad hoc, sectoral measures. *See* Reidenberg, *Fortress or Frontier*, *supra* note 17, at 209-10 (explaining U.S. ad hoc industry-specific approach). The U.S. model is sectoral in the sense that U.S. data protection laws normally govern either the public or private spheres. SCHWARTZ & REIDENBERG, *supra* note 8, at 7-8. Further, laws governing the private sector address specific industries or economic sectors. CATE, *supra* note 31, at 80; Reidenberg, *Fortress or Frontier*, *supra* note 17, at 210; *see* Gellman, *supra* note 14, at 130-31 (describing U.S. approach to data protection as "'sectoral', with separate and uncoordinated laws applying to some personal records, and no laws applying to others."). The U.S. model is ad hoc in the sense that U.S. legislatures enact data protection measures in reaction to particular problems. Reidenberg, *Setting Standards*, *supra*, at 506. The Video Privacy Protection Act exemplifies this ad hoc, sectoral approach for Congress enacted this industry-specific statute in reaction to public examination of the video rental records of Robert Bork, a nominee of the U.S. Supreme Court. *Id.* at 506 n.48; The Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1994).

54. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 500-01 (explaining U.S. resistance to omnibus or comprehensive data protection rules); Gellman, *supra* note 14, at 130 (noting that under U.S. sectoral approach, while separate and uncoordinated laws apply to some personal information, no laws apply to other personal information).

55. Gellman, *supra* note 14, at 132.

either the United States or Europe until the 1960s.[56] As information technology developed rapidly, both the United States and European countries addressed problems related to the processing of personal data.[57]

1. Data Protection

Data protection, a European term related to informational privacy, refers to measures taken to protect personal data.[58] The protection of personal data developed from earlier traditions that protected privacy.[59] Data protection became necessary because rapid advances in information technologies have dramatically increased the availability of personal information.[60]

a. Definition of Data Protection

Data protection refers to policies designed to regulate the collection, storage, use, or dissemination of personal information.[61] The term, data protection, is a translation of the German *Datenschultz*.[62] Although data protection may connote information contained on computers, the term can cover both automated and manual personal records.[63] The Directive uses data protection to include the protection of both automatic and manual records.[64]

b. Early History of Data Protection

The modern notion of privacy emerged in the United States before the processing of personal data became an issue.[65] In the United States, the concept of the right to privacy first emerged

---

56. BENNETT, *supra* note 1, at 2.

57. *See id.* at 2-3 (noting that many countries have enacted data protection legislation to protect personal data).

58. *Id.* at 13.

59. *See* Gellman, *supra* note 14, at 132 (describing early U.S. tradition of privacy).

60. CATE, *supra* note 31, at 1; *see* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 1-4 (1989) (discussing threats of increased surveillance to individuals posed by technological innovations).

61. BENNETT, *supra* note 1, at 12-14; SCHWARTZ & REIDENBERG, *supra* note 8, at 5.

62. BENNETT, *supra* note 1, at 13.

63. *See id.* at 13-14 (noting that some data protection laws cover both automated and manual files).

64. *See* Directive, *supra* note 4, art. 2(b), O.J. L 281/31, at 38 (1995) (stating that under Directive processing includes operations "performed upon personal data, whether or not by automatic means.").

65. *See* Michael D. Scott, *United States*, *in* DATA TRANSMISSION AND PRIVACY 487, 487

in an 1890 law review article.[66] In this article Louis Brandeis and Samuel Warren proposed that individuals have a common law[67] right to privacy against publication.[68] For many years the right to privacy did not extend beyond common law torts.[69] The scope of the right to privacy, however, eventually expanded beyond torts to include a constitutional freedom from unjustified government regulation of marital and familial relationships.[70] Many European countries expressed a similar commitment to the protection of privacy in the European Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950 ("ECHR").[71] The ECHR sets forth a right to pri-

---

(Dennis Campbell & Joy Fischer eds., 1994) (noting that privacy rights existed in U.S. common law).

66. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see* Gellman, *supra* note 14, at 132-34 (explaining emergence of new conception of privacy). An earlier American legal tradition protected privacy under the Fourth Amendment's requirement of a warrant for searches and seizures and the Fifth Amendment's ban on self-incrimination. C. Herman Pritchett, *Foreward* to DAVID O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY at vii (1979).

67. *See* BLACK'S LAW DICTIONARY 276 (6th ed. 1990) (defining common law as "a body of law that develops and derives through judicial decisions, as distinguished from legislative enactments"); *see also* Monique Olivier, Comment, *The UNIDROIT Convention: Attempting to Regulate the International Trade and Traffic of Cultural Property*, 26 GOLDEN STATE U. L. REV. 627, 637 (1996) (discussing difference between common and civil law countries).

68. *See* Warren & Brandeis, *supra* note 66, at 198-200 (discussing right against publication distinct from statutory right of copyright). Reacting to the abuses of photographic developments, Warren and Brandeis argued for enforcement of a general right of the individual to be let alone. *Id.* at 205. Samuel Warren and Louis Brandeis proposed that individuals enforce this right through tort remedies. *Id.* at 219. One scholar stated that the privacy case law that developed from Warren and Brandeis' theory was incoherent and directionless. BENNETT, *supra* note 1, at 66. Seventy years later after Warren and Brandeis had published their article, William Prosser categorized this right against unwanted publication into four distinct torts: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light in the public eye, and (4) appropriation of name or likeness for commercial purposes. William Prosser, *The Right to Privacy*, 48 CAL. L. REV. 383, 389 (1960); *see* Reidenberg, *Setting Standards*, *supra* note 53, at 504-05 (discussing Prosser's categorization of privacy torts).

69. *See* Scott, *supra* note 65, at 487 (noting privacy protection did not expand until 1960s).

70. *See* RAYMOND WACKS, PRIVACY: VOLUME II at xviii-xiv (1993) (discussing development of U.S. Constitutional right to privacy); *see, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (recognizing right to privacy over marital decisions such as decision to use contraceptives); Roe v. Wade, 410 U.S. 113 (1973) (recognizing right of privacy for women to decide to terminate pregnancy).

71. ECHR, *supra* note 19; *see* OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 11, at 431 (noting that ECHR deals with protection of privacy and free dissemination of information in more general way). The International Covenant on Civil

vacy for individuals.[72]

While some early U.S. privacy case law and a few international agreements had dealt with privacy, concern with data protection did not emerge until the 1960s.[73] Early computers were cumbersome machines that performed limited functions.[74] Advances in informational technologies improved society's ability to collect, manipulate, store, and transmit personal information.[75] These improvements, however, posed threats to personal privacy because they increased the amount of personal information available and expanded the use of this information.[76] As a result of this increased threat to personal information, governments and businesses in the United States and Europe began to recognize the need to embrace data protection.

2. Development of Data Protection

After the emergence of concern with data protection during the 1960s,[77] the United States and European countries enacted legislation during the 1970s and 1980s to address this concern.[78] The United States passed targeted data privacy laws in reaction

---

and Political Rights ("ICCPR") is another international agreement that deals with the protection of privacy and the free dissemination of information. International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171, 6 I.L.M. 368 (1967) [hereinafter ICCPR]; OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 11 at 431.

72. ECHR, *supra* note 19, art. 8, 213 U.N.T.S. at 230. "Everyone has the right to respect for his private and family life, his home and his correspondence." *Id.* The ECHR also established a right to free flow of information. *Id.* art. 10(1), 213 U.N.T.S. at 231. "Everyone has the right to freedom of expression. This right shall include freedom to . . . impart information and ideas without interference." *Id.*

73. BENNETT, *supra* note 1, at 2; *see* REGAN, *supra* note 3, at 26 (explaining that concern for technological changes threatening privacy began in 1960s).

74. BENNETT, *supra* note 1, at 21.

75. FLAHERTY, *supra* note 60, at 11.

76. CATE, *supra* note 31, at 5. One scholar attributes political action promoting data protection to four factors related to advances in informational technology. BENNETT, *supra* note 1. These factors include the specific plans to create centralized government data banks in various countries, proposals to introduce personal identification numbers for every citizen, the occurrence of detailed censuses, and a spate of literature calling attention to privacy problems. *See id.* at 46-55 (discussing four factors of political action on data protection).

77. *See* BENNETT, *supra* note 1, at 2 (describing development of data protection as new policy problem appropriate for comparative analysis).

78. *See* REGAN, *supra* note 3, at 5-8 (relating development of U.S. data protection laws enacted during 1970s and 1980s and their legislative history); BENNETT, *supra* note 1, at 56-58 (discussing European national data protection measures adopted during 1970s and 1980s).

to specific informational privacy concerns.[79] In contrast, many European countries have adopted omnibus data protection measures on a national level and reached joint international agreements.[80]

a. Development of Data Protection in the United States

While the United States has passed various data privacy laws,[81] it has adopted an ad hoc, sectoral approach to protecting personal data.[82] During the 1960s, U.S. interest in privacy and data protection arose contemporaneously with the proliferation of computers.[83] After the executive branch of the U.S. government proposed a computerized federal data center in 1965, the U.S. Congress held hearings to explore different aspects of privacy.[84] During the 1960s, in addition to holding these hearings, Congress enacted the Freedom of Information Act[85] ("FOIA") in 1966, providing individuals with access to federal agency docu-

79. CATE, *supra* note 31, at 80; Reidenberg, *Setting Standards*, *supra* note 53, at 500.

80. *See* Gellman, *supra* note 14, at 135 (describing adoption of comprehensive data protection laws by European counties); NUGTER, *supra* note 14, at 22-28 (describing international data protection agreements adopted by European countries).

81. *See, e.g.*, The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o)-(r), (u) (1994 & Supp. II 1996) (regulating data matching by federal government); The Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996) (regulating federal agencies' treatment of personal information); The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998) (regulating collection, use, and disclosure of credit information); The Electronic Communications Protection Act, 18 U.S.C. §§ 2510-2511, 2701-2709 (1994), *amended by* 18 U.S.C.A. §§ 2510-2511, 2701-2709 (West Supp. 1997) (regulating government access to toll billing records); The Telecommunications Act of 1996, 47 U.S.C.A. § 222 (West Supp. 1997) (regulating telecommunication carriers' use of transactional information).

82. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 500 (describing U.S. ad hoc, targeted approach to data protection); NUGTER, *supra* note 14, at 18-19 (comparing U.S. sectoral approach to European omnibus approach).

83. *See* Gellman, *supra* note 14, at 133 (discussing revival of interest in privacy during 1960s). "By the mid-1960s, concerns about privacy and technology were reflected in a 'literature of alarm' that was instrumental in placing information privacy . . . on the policy agenda." REGAN, *supra* note 3, at 13.

84. REGAN, *supra* note 3, at 7-8. Between 1965 and 1974, nearly fifty Congressional hearings and reports investigated various privacy issues. *Id.* at 7. Further, between 1965 and 1972, legislators introduced over 260 privacy bills. *See id.* at 71-86 (discussing history of early legislation and congressional hearings concerning U.S. data protection). After holding these hearing for nine years, the U.S. Congress eventually passed the Privacy Act of 1974. Pub. L. No. 93-579, 88 Stat. 1897 (codified in 5 U.S.C. § 552a (1994 & Supp. II 1996)).

85. The Freedom of Information Act, 5 U.S.C. § 552 (1994 & Supp. II 1996).

ments.[86] The FOIA protects privacy by exempting personal information from the material that government must disclose under FOIA's provisions.[87]

During the 1970s, the United States improved its data protection.[88] In 1970, the U.S. Congress enacted the Fair Credit Reporting Act[89] ("FCRA") to regulate the use and disclosure of credit information.[90] Congress also passed the Privacy Act of 1974[91] ("Privacy Act") to regulate how the federal agencies[92]

---

86. DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 206-07 (1979).

87. 5 U.S.C. § 552(7)(C). The Freedom of Information Act ("FOIA") provides for disclosures which "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *Id.*

88. *See* Gellman, *supra* note 14, at 135 (describing United States as early leader in privacy, but noting that United States lost this leadership to Europe during mid-1970s). The U.S. Senate Judiciary Committee's Subcommittee on Constitutional Rights, chaired by U.S. Senator Sam J. Ervin, Jr., investigated problems with the federal data banks between 1970 and 1974 and recommended statutory regulation of these data banks. BENNETT, *supra* note 1, at 69. In 1972, the U.S. Secretary of the Department of Health, Education, and Welfare, Eliot Richardson, appointed the U.S. Advisory Committee on Automated Personal Data Systems ("Advisory Committee") to analyze and make recommendations about the danger of computerized information systems. *Id.* at 70; REGAN, *supra* note 3, at 74-75. In 1972, the Advisory Committee presented a report containing a code of fair information practices that became the basis for various U.S. privacy laws. *Id.* at 70-71. Further, scholarly analysis of privacy problems complemented these government investigations. BENNETT, *supra* note 1, at 70; REGAN, *supra* note 3, at 75.

89. The Fair Credit Reporting Act, Pub. L. No. 90-508, 84 Stat. 1128, (codified in 15 U.S.C. §§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998)). Two years earlier, U.S. Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968 ("Crime Control Act"). *See* 18 U.S.C. §§ 2510-2520 (1994), *amended by* 18 U.S.C.A. §§ 2510-2520 (West Supp. 1997) (limiting use of wiretaps). Although U.S. Congress passed the Crime Control Act two years before the FCRA, this law addresses communication privacy more than information privacy. *See* REGAN, *supra* note 3, at 123 (discussing Omnibus Crime Control Act in section on communication privacy rather than information privacy).

90. 15 U.S.C. §§ 1681-18681t.

91. *See* The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified in 5 U.S.C. § 552a (1994 & Supp. II 1996)) (providing safeguards for individuals against invasions of personal privacy by enabling individuals to obtain personal records that federal agencies maintain and by requiring that those agencies only retain information relevant to specific and legal purpose). The U.S. Congress passed the Privacy Act largely as a result of the revelation of government misuses of information that occurred during the Watergate Scandal. REGAN, *supra* note 3, at 8; *see* BENNETT, *supra* note 1, at 71-72 (discussing Watergate crisis as opening policy window for privacy legislation). *See generally* REGAN, *supra* note 3, at 71-90 (discussing legislative history of Privacy Act).

92. *See* The Freedom of Information Act, 5 U.S.C. § 552(f) (1994 & Supp. II 1996) (defining federal agencies as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government . . . or any independent regulatory agency.").

treat personal information.[93] The Privacy Act and the FCRA exemplify the ad hoc, sectoral approach because Congress enacted these statutes in response to concern over data protection and both these statutes regulate specific areas.[94] In 1974, the Privacy Act established the Privacy Protection Study Commission[95] ("PPSC") as a temporary organization to review and report on the treatment of personal information within both the public and private sectors.[96] Among the PPSC's many suggestions to improve the protection of privacy, it recommended that the United States establish an independent Federal Privacy Board to regulate the treatment of personal data in the private sector.[97] Congress never acted upon this recommendation.[98]

During the 1980s, the United States continued to adopt ad hoc, sectoral legislative measures.[99] For example, in response to increased use of data matching[100] during the late 1970s and the early 1980s, the U.S. Congress passed the Computer Matching and Privacy Protection Act of 1988[101] to establish procedural limitations on the federal government's data matching.[102] Similarly,

---

93. The Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996); *see* Scott, *supra* note 65, at 491-96 (discussing protections of Privacy Act). U.S. Constitutional principles permit the government to regulate its own actions, but discourage regulation of relationships between individuals. SCHWARTZ & REIDENBERG, *supra* note 8, at 9.

94. SCHWARTZ & REIDENBERG, *supra* note 8, at 20; *see* NUGTER, *supra* note 14, at 18-19 (classifying U.S. laws specifically targeting credit or government records as sectoral); Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137, S149 (1992) [hereinafter Reidenberg, *Obstacle Course*] (citing FCRA as example of ad hoc legislation in financial services).

95. *See* REGAN, *supra* note 3, at 81-82 (explaining that Congress established Privacy Protection Study Commission as part of compromise between U.S. House of Representatives and U.S. Senate bills on Privacy Act).

96. Gellman, *supra* note 14, at 134; The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified as amended at 5 U.S.C. § 552a (1994 & Supp. II 1996)).

97. *See* REGAN, *supra* note 3, at 84-85.

98. *See id.* at 85 (noting that "no legislation resulted directly from the recommendations of the Privacy Protection Study Commission.").

99. *See* NUGTER, *supra* note 14, at 18-19 (suggesting that U.S. sectoral approach had continued until 1990).

100. SCHWARTZ & REIDENBERG, *supra* note 8, at 100-01. Data matching involves electronic comparison of computerized files with other computerized files to find individuals included on more than one file. *Id.*; REGAN, *supra* note 3, at 86.

101. *See* The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o)-(r), (u) (1994 & Supp. II 1996) (regulating data matching by federal government).

102. *See* REGAN, *supra* note 3, at 92-99 (discussing legislative history of Computer Matching and Privacy Protection Act).

the adoption of the Video Privacy Protection Act[103] exemplifies this U.S. ad hoc, sectoral approach.[104] Reacting to a perceived crisis with video rentals, Congress enacted the Video Privacy Protection Act to address the treatment of video rental and sale records.[105] Other data protection measures that the United States adopted during the 1980s also represent the ad hoc, sectoral approach to data protection.[106]

b. Development of Data Protection in Europe

Although many European countries and the United States began to address data protection during the 1960s, European countries adopted more comprehensive data protection measures than the United States.[107] In 1968, the Council of Europe's[108] ("COE") Parliamentary Assembly[109] asked its Committee of Ministers[110] to determine whether the ECHR and the domestic law of COE member states covered the processing of personal data.[111] The Committee of Ministers ascertained that

---

103. The Video Privacy Protection Act, 18 U.S.C. §§ 2701-11 (1994).

104. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 10 (explaining how Congress enacted Video Privacy Protection Act in reaction to data privacy problem and how act is narrowly targeted).

105. *Id.* The perceived crisis involved the publication of a list of Robert Bork's video rentals during his nomination to the U.S. Supreme Court. *Id.* at 10-11.

106. *See, e.g.*, The Cable Communications Policy Act, 47 U.S.C. § 551 (1994) (regulating treatment of cable television subscriber information); The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2511, 2701-2709 (1994), *amended by* 18 U.S.C.A. §§ 2510-2511, 2701-2709 (West Supp. 1997) (extending protection of communications to new forms of communications such as cellular phones and electronic mail).

107. *See* CATE, *supra* note 31, at 32 (noting Europe as source for most comprehensive data protection legislation).

108. D. LASOK & J.W. BRIDGE, LAW AND INSTITUTIONS OF THE EUROPEAN COMMUNITIES 9 (4th ed. 1987); *see* BERMANN ET AL., *supra* note 23, at 3-4 (describing origin and achievements of Council of Europe); WESTLAKE, *supra* note 47, at 5 (distinguishing Council of Europe from EC Council). The Council of Europe ("COE") consists of a Committee of Ministers, a Secretariat, and a Parliamentary (formerly Consultative) Assembly comprised of national parliamentary representatives from each of the COE Member States. LASOK & BRIDGE, *supra*, at 9; BENNETT, *supra* note 1, at 133. Established in 1949, the COE seeks to promote collaboration in the area of law and human rights among the democratic states of Europe. BENNETT, *supra* note 1, at 133.

109. *See* LASOK & BRIDGE, *supra* note 108, at 9 (explaining that Parliamentary Assembly is component of COE and consists of parliamentary delegates of Member States).

110. BENNETT, *supra* note 1, at 133. The Committee of Ministers is the COE's intergovernmental ruling body. *Id.*

111. Council of Euro., Draft Explanatory Report on the Draft Convention for the

the then current law[112] dealt with privacy issues in a general way, but not with regard to data processing.[113] Motivated by these findings, the Committee of Ministers adopted two resolutions in 1973 and 1974, recommending that the governments of COE member states implement data protection measures.[114]

European countries took various data protection initiatives during the 1970s.[115] Responding in part to the Committee of Ministers' two resolutions recommending that COE member states implement data protection measures,[116] several European countries enacted comprehensive data protection laws.[117] Be-

---

Protection of Individuals with Regard to Automatic Processing of Personal Data, CJ-CD (80) 1, Addendum (Jan. 1980), *reprinted in* 19 I.L.M. 299, 300 ¶ 4 [hereinafter COE Convention Draft Explanatory Report]; Council of Europe, Consultative Assembly, Recommendation No. 509 (1968).

112. *See* OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 11, at 431 (explaining that ECHR and ICCPR did not deal with privacy vis-à-vis processing of personal data); ECHR, *supra* note 19; ICCPR, *supra* note 71.

113. COE Convention Draft Explanatory Report, *supra* note 111, ¶ 4, at 300; NUGTER, *supra* note 14, at 24.

114. COE Convention Draft Explanatory Report, *supra* note 111, ¶ 4, at 300; OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 13, at 431 (explaining that 1973 and 1974 resolutions took steps to give effect to number of basic data protection principles, regarding private and public sectors, respectively); Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, Res. (73)22, Council of Europe, Comm. of Ministers, 224th mtg. (1973) [hereinafter 1973 COE Resolution]; Resolution on the Protection of Individuals vis-à-vis Electronic Data Banks in the Public Sector, Res. (74)29, Council of Europe, Comm. of Ministers, 224th mtg. (1974) [hereinafter 1974 COE Resolution]. The Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector and the Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector set forth basic rules for storage of personal data in electronic data banks, but gave the member states of the COE discretion on how to give effect to these rules. COE Convention Draft Explanatory Report, *supra* note 111, ¶ 5, at 300. In 1972, the committee of experts that prepared these resolutions emphasized that after member states enacted national legislation based on the resolutions, an international agreement should be pursued to reinforce these national laws. *Id.* ¶ 12, at 302.

115. *See* Gellman, *supra* note 14, at 135 (describing European advances in data protection that began in 1970s). These European omnibus laws governed both public and private sector and established formal data protection authorities to oversee data processing and to enforce the law. *Id.*

116. 1973 COE Resolution, *supra* note 114; 1974 COE Resolution, *supra* note 114.

117. COE Convention Draft Explanatory Report, *supra* note 111, ¶ 5, at 300; *see* BENNETT, *supra* note 1, at 57 tbl.1 (listing Organization for Economic Co-operation and Development ("OECD") countries with data protection laws and dates of passage). Between 1973 and 1979, Austria, Denmark, France, West Germany, Luxembourg, Norway, and Sweden adopted such laws. COE Convention Draft Explanatory Report, *supra* note 111, ¶ 5, at 300. Portugal and Spain incorporated data protection as a fundamental

cause these national laws were diverse,[118] however, the resulting different privacy standards became potential obstacles to transfers of personal data between various European countries.[119]

During the late 1970s, three international organizations began to take measures to harmonize these national laws.[120] In 1976, the Council of Europe began to prepare an international convention to establish some basic principles of data protection.[121] The Organization for Economic Co-operation and Development[122] ("OECD") sought to harmonize data protection

---

right in their Constitutions. *Id.*; Constituicao [Constitution] art. 35 (Port.); Constitucion [Constitution] [C.E.] art. XVIII, para.1 (Spain).

In April 1973, Sweden enacted its *Datalagen* (or "Data Act"), the first omnibus, national data protection law. *See* BENNETT, *supra* note 1, at 64-65, 161 (noting Data Act applies to both public and private organizations). The Federal Republic of Germany's *Bundesdatenschutzgesetz*, in force since February 1, 1977, regulates the processing of personal data at the public sector and the private sector. NUGTER, *supra* note 14, at 43-44. France's *Loi relative à l'informatique, aux fichers et aux libertés*, in force since January 6, 1978, covers processing within both the public and private sector. *See id.* at 100 (noting that French supervisory authority establish rules for particular categories of processing in both sectors).

118. *See* OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶¶ 5-6, at 430 (explaining that although various national approaches to privacy protection possessed many common features, these approaches had many disparities, such as scope of legislation, categorization of sensitive data, and method of enforcement). For example, some national data protection laws deal only with computers, while other national laws deal with all privacy issues irrespective of technology. *Id.* ¶ 1, at 428.

119. OECD Guidelines Explanatory Memorandum, *supra* note 18, at 427; *see* Fleischmann, *supra* note 17, at 150 & n.48 (citing Council press release); *see also* d'Afflitto, *supra* note 25, at 307 (explaining that "divergences [that] still exist[ ] among the various national laws may . . . prevent transborder data flow").

120. *See* BENNETT, *supra* note 1, at 131-40 (discussing efforts of COE and OECD to harmonize national data protection laws); NUGTER, *supra* note 14, at 20-33 (explaining harmonization efforts undertaken by OECD, COE, and EC during 1970s).

121. *See* COE Convention Draft Explanatory Report, *supra* note 111, ¶ 13, at 303 (describing COE's efforts to prepare international convention on data protection); OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 14, at 431-32 (noting that COE intended Convention to be completed by June 30, 1980). In 1976, the COE Committee of Ministers instructed a committee of experts on data protection to prepare a convention. COE Convention Draft Explanatory Report, *supra* note 111, ¶ 13, at 303. After holding four meetings from November 1976 to May 1979, the committee of experts produced the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. *Id.* ¶ 17, at 303-04; Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* January 28, 1981, Europ. T.S. No. 108, *reprinted in* 20 I.L.M. 317 (1981) [hereinafter COE Convention]; BENNETT, *supra* note 1, at 135.

122. BERMANN ET AL., *supra* note 23, at 4. The Organization for Economic Cooperation and Development, originally named the Organization for European Economic Co-operation ("OEEC"), is dedicated to the economic development of its member countries. BENNETT, *supra* note 1, at 136. In 1948, the Marshall Plan's recipient nations

laws by drafting a set of international guidelines for OECD member states.[123] Finally, the European Community studied harmonization of national data protection laws, especially in relation to transborder data flows.[124] In May 1979, the Parliament adopted a resolution on personal privacy and data processing, recommending that the Commission of the European Communities[125] ("Commission") propose a directive to harmonize data protection laws.[126]

As a result of the efforts of many European countries during

---

created the OEEC to facilitate administration of the Marshall Plan. BERMANN ET AL., *supra* note 23, at 4. In 1960, the OEEC renamed itself the OECD when Canada and the United States joined. *Id.* While the OECD lacks formal lawmaking power, its recommendations have significantly influenced national economic policies. *Id.*

123. OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 18, at 432-33. In 1968, the OECD Group on Computer Utilization began to study computers and telecommunications. BENNETT, *supra* note 1, at 136. In 1974, the OECD established another group of experts, the Data Bank Panel, to study privacy issues including transborder data flows. *Id.* The Data Bank Panel's study ended in 1977 with a symposium in Vienna. OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 16, at 432. In 1978, the OECD established a Group of Experts on Transborder Data Barriers and Privacy Protection to develop guidelines on basic rules governing transborder data flows and the protection of personal data and privacy. *Id.* ¶ 18, at 432-33; *see* BENNETT, *supra* note 1, at 137 (noting that Group of Experts worked closely with COE).

124. OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 15, at 432. Prior to the EC studies regarding the harmonization of European data protection legislation, EC involvement with data protection began in 1973 when the Commission issued a Communication to the Council, promoting the development of the European data processing industry to combat dependency upon U.S. technology. Community Policy on Data Processing, SEC (73) 4300 Final (1973); *see* NUGTER, *supra* note 14, at 29 (contrasting Commission's and Council's concern for promoting data processing industry with Parliament's concern for data protection).

125. *See* EC Treaty, *supra* note 21, arts. 155-163, [1992] 1 C.M.L.R. at 682-84 (describing role of Commission).

126. 1979 Resolution on the protection of the rights of the individual in the face of technical developments in data processing, O.J. C 140/34 (1979) [hereinafter 1979 Parliament Resolution]; OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 15, at 432. After holding a public hearing on data privacy in early 1978, a sub-committee of the European Parliament reported to the Parliament in spring 1979. OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶ 15, at 432. The report contained a resolution recommending that the Commission propose a directive to harmonize data protection laws. 1979 Parliament Resolution, *supra*, art. 4, O.J. C 140/34, at 35 (1979). The Parliament adopted this resolution in May 1979. NUGTER, *supra* note 14, at 29. The Commission did not propose such a directive at that time because the Commission determined that a measure was not necessary in addition to the Convention. *See* Commission Recommendation, O.J. L 246/31, at 31 (1981) (encouraging EC Member States to sign and ratify the Convention by 1983); NUGTER, *supra* note 14, at 30 (discussing Commission's 1981 recommendation). The Parliament adopted another resolution in 1982, recommending a harmonization directive if the COE Convention proved inadequate. 1982 Resolution on the protection of the rights of the individual in the face of

the 1970s, European countries reached two international agreements to harmonize their data protection laws.[127] On September 23, 1980, the OECD adopted a document titled Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[128] ("Guidelines") that outlines eight basic principles[129] for balancing privacy and the free flow of information to facilitate harmonization.[130] These Guidelines recommend that OECD member states[131] adopt national data protection meas-

---

technological developments in data processing, O.J. C 87/39, at 39 (1982); *see* NUGTER, *supra* note 14, at 30-31 (discussing Parliament's 1982 Resolution).

127. Organization for Economic Co-operation and Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, O.E.C.D. Doc. C(80)58 Final, *reprinted in* 20 I.L.M. 422 (1981) [hereinafter OECD Guidelines]; COE Convention, *supra* note 121.

128. OECD Guidelines, *supra* note 127. OECD's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Guidelines") are not binding upon OECD member nations because the OECD has no formal lawmaking powers. BERMANN ET AL., *supra* note 23, at 4.

129. OECD Guidelines, *supra* note 127, pt. 2, arts. 7-14, at 424-25; *see* OECD Guidelines Explanatory Memorandum, *supra* note 18, ¶¶ 50-62, at 442-46 (explaining basic principles). These eight data protection principles address: limitations on collection, data quality, specification of purpose, limitations of use, security safeguards, openness, individual participation, and accountability. OECD Guidelines, *supra* note 127, pt. 2, arts. 7-14, at 424-25.

130. *See* OECD Guidelines, *supra* note 127, pmbl., at 422 (noting that OECD "[m]ember countries have a common interest . . . in reconciling fundamental but competing values such as privacy and the free flow of information"); *see also* Jennifer M. Myers, Note, *Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States*, 29 CASE W. RES. J. INT'L L. 109, 117 (1997) (discussing harmonization efforts of OCED Guidelines). This balance of competing values is an essential element of data protection because the measures that a country takes to protect information depend upon the balance between privacy and the free flow of information that the country reaches. Jane Zimmerman, *Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism*, 4 J. INT'L L. BUS. 601, 603-04 (1982) (explaining that understanding interplay between privacy and free flow of information is necessary to understand protection laws). For instance, although the United States values informational privacy, it places greater emphasis on the free flow of ideas. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 503-06 (explaining U.S. constitutional emphasis on restraining government). Thus, the United States has adopted an ad hoc, sectoral approach that favors the free flow of information. *Id.* at 506.

131. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEV., CODE OF LIBERALISATION OF CURRENT INVISIBLE OPERATIONS 2 (1997) [hereinafter OECD CODE]. The original OECD member countries are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Convention of the Organization for Economic Co-operation and Development, Dec. 14, 1960, 888 U.N.T.S. 179. Japan joined the OECD in 1964, Finland in 1969, Australia in

ures to implement these principles.[132] The Guidelines, however, have no legal force[133] and permit broad variation in national implementation.[134] Consequently, although the Guidelines provide guidance to OECD member states, they do not create uniform protection laws.[135]

On January 28, 1981, the Council of Europe opened for signature the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention").[136] The Convention sets forth basic data protection principles similar to those outlined in the OECD Guidelines[137] and requires signatory countries of the COE Convention to enact conforming legislation.[138] Nonetheless, while many European data protection laws embodied the principles from the Convention and the OECD Guidelines, these two agreements failed to

---

1971, New Zealand in 1973, Mexico in 1994, the Czech Republic in 1995, and Hungary, Poland, and the Republic of Korea in 1996. OECD CODE, *supra*, at 2.

132. *See* OECD Guidelines, *supra* note 127, pmbl., at 422-23 (stating that "[t]he Council . . . recommends [t]hat Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines").

133. *See* BENNETT, *supra* note 1, at 138 (noting that Guidelines are voluntary in nature).

134. OECD Guidelines Explanatory Memorandum, *supra* note 18, at 428; Cate, *supra* note 39, at 431.

135. *See* Myers, *supra* note 130, at 117 (discussing effect of OECD Guidelines).

136. COE Convention, *supra* note 121, at 323. The COE Convention for the Protection of Individuals with Regard to Automatic Data Processing of Personal Data ("Convention") entered into force on October 1, 1985 when the Convention received its five requisite ratifications. Herald D.J. Jongen & Gerrit A. Vriezen, *The Council of Europe and the European Community*, *in* DATA TRANSMISSION AND PRIVACY 139 (Dennis Campbell & Joy Fischer eds., 1994); BENNETT, *supra* note 1, at 133. Nineteen countries have acceded the Convention. Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 473.

137. *Compare* COE Convention, *supra* note 121, arts. 5-9, at 319-20 (listing and explaining Convention principles) *with* OECD Guidelines, *supra* note 127, pts. 2-3, arts. 7-18, at 424-26 (outlining basic principles). The basic principles from the Convention involved data quality, data security, special categories of data, and rights to access and correct data. COE Convention, *supra* note 121, arts. 5-9, at 319-20. The Convention principles apply only to automated data processing. *Id.* art. 3(1), at 318.

138. *See* COE Convention, *supra* note 121, art. 4(1), at 319 (stating that "[e]ach Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter."); *see also* NUGTER, *supra* note 14, at 26 (explaining legal effect of COE Convention). While the Convention imposes on signatory countries the duty to implement domestic data protection laws, it does not have direct effect. *See* NUGTER, *supra* note 14, at 26 (stating that "[i]ndividuals may not invoke the Convention before their national court.").

harmonize national data protection laws.[139]

B. *Current EC Protection of Personal Data: Directive 95/46/EC*

In 1995, the Community adopted the Directive to harmonize Member State data protection after a long and complex legislative process.[140] With the aim of harmonizing Member State data protection laws, the Directive balances the right to privacy against the need for the free flow of information by setting forth a framework for Member State data protection laws.[141] The Directive also regulates data transfers to non-EC countries.[142] Article 29 of the Directive establishes a Working Party to provide advice upon the application of the Directive.[143]

1. Legislative History of the Directive

Under the co-decision procedure[144] ("co-decision"), the

139. *See* Cate, *supra* note 39, at 432 (noting uneven application of European data protection laws even after OECD Guidelines and COE Convention); Boehmer & Palmer, *supra* note 39, at 279-80 (describing inconsistencies between European data protection laws). This failure to harmonize European data protection laws has been attributed to the agreements' allowance for broad variations in national implementation just like the OECD Guidelines. Cate, *supra* note 39, at 432. Also, some signatories of the Convention have not ratified the document. *Id.* at 432.

140. *See* Cate, *supra* note 39, at 432-33 (describing adoption of Directive); d'Afflitto, *supra* note 25, at 308-09 & n.13 (discussing Directive's legislative history).

141. Directive, *supra* note 4, O.J. L 281/31 (1995).

142. *Id.* art. 25, O.J. L 281/31, at 45-46 (1995).

143. *Id.* arts. 29-30, O.J. L 281/31, at 48-49 (1995).

144. EC Treaty, *supra* note 21, art. 189b, [1992] 1 C.M.L.R. at 694-95; *see* BERMANN ET AL., *supra* note 23, at 79-90 (discussing parliamentary co-decision procedure under Article 189b); GEORGE A. BERMANN ET AL., 1995 SUPPLEMENT TO CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 33-34 (1995) (noting recent developments of co-decision procedure). The TEU created a new legislative procedure under the Article 189b of the EC Treaty, commonly called the co-decision procedure ("co-decision"). BERMANN ET AL., *supra* note 23, at 89. Co-decision applies to harmonization directives that are adopted to establish the internal market under Articles 100a and b. *Id.* Because the Council and Parliament adopted the Directive pursuant to Article 100a, co-decision under Article 189b applies. *See* Directive, *supra* note 4, pmbl., O.J. L 281/31, at 31 (1995) (stating commitment of Council and Parliament to act in accordance with Article 189b having regard to Article 100a). Co-decision essentially gives Parliament veto power. *See* BERMANN ET AL., *supra* note 23, at 89 (noting that Council still has upper hand).

Under co-decision, the Commission submits a proposal to Parliament and the Council. EC Treaty, *supra* note 21, art. 189b(2), [1992] 1 C.M.L.R. at 694. In Parliament's first reading, Parliament may suggest amendments to the Commission. *See id.* art. 189b(2), ¶ 2, [1992] 1 C.M.L.R. at 694 (noting that Council may act "after obtaining the opinion" from Parliament); BERMANN ET AL., *supra* note 23, at 84, 89 (explaining that first phase of co-decision is like consultation and cooperation proce-

Council and Parliament adopted the Directive.[145] In 1990, the

dures). The Commission may amend its proposal and publish a revised version. BERMANN ET AL., *supra* note 23, at 84. Then the Council conducts its first reading and adopts a common position. EC Treaty, *supra* note 21, art. 189b(2), ¶ 2, [1992] 1 C.M.L.R. at 694; BERMANN ET AL., *supra* note 23, at 84. After the Council communicates its common position and reasoning to Parliament, Parliament conducts its second reading. EC Treaty, *supra* note 21, art. 189b(2), ¶ 2, [1992] 1 C.M.L.R. at 694.

Parliament then has three options. *See* BERMANN ET AL., *supra* note 23, at 89-90 (noting Parliament can approve, reject, or amend common position). First, if Parliament either approves the Council's common position or takes no action for three months, then the Council adopts the common position. EC Treaty, *supra* note 21, art. 189b(2), ¶ 3(a)-(b), [1992] 1 C.M.L.R. at 694.

As Parliament's second option, Parliament can propose amendments to the common position by absolute majority. *Id.* art. 189b(2), ¶ 3(d), [1992] 1 C.M.L.R. at 694. The Council then has three months to review Parliament's proposed amendments. *Id.* 189b(3), [1992] 1 C.M.L.R. at 695. If the Council adopts Parliament's proposed amendments by qualified majority (or unanimously if the Commission opposed Parliament's amendments), then the Council shall adopt the amended common position. *Id.* If the Council opposes Parliament's amendments, however, then the Council convenes the Conciliation Committee. *Id.* The Conciliation Committee has six weeks to approve a compromise text, otherwise the draft measure lapses. *Id.* art. 189b(5)-(6), [1992] 1 C.M.L.R. at 695. Prior to the Treaty of Amsterdam, if the Conciliation Committee failed to reach a compromise, the Council could adopt its common position by qualified majority, and Parliament could only reject it by absolute majority. *Id.* art. 189b(6), [1992] 1 C.M.L.R. at 695; *see* BERMANN ET AL., *supra* note 23, at 90 (noting that co-decision gives Parliament legislative veto, but Council has practical and psychological advantage). If ratified, the Treaty of Amsterdam will eliminate this last stage, so if the Conciliation Committee fails to compromise, the Council cannot adopt the measure. *Compare* Consolidated Version of The Treaty Establishing the European Community, art. 251(6), O.J. C 340/03, at 280 (1997), *incorporating changes made by* Treaty of Amsterdam, art. 189b(6), O.J. C 340/01, at 46 (1997), *with* TEU, *supra* note 21, art. 189b(6), [1992] 1 C.M.L.R. at 695; BERMANN ET AL., 1998 SUPPLEMENT, *supra* note 24, at 64.

For Parliament's third option, Parliament may, by absolute majority, notify the Council that it intends to reject the common position. EC Treaty, *supra* note 21, art. 189b(2), ¶ 3(c), [1992] 1 C.M.L.R. at 694. The Council may then convene a Conciliation Committee to explain the Council's views to Parliament. *Id.* After the Conciliation Committee meets, Parliament may confirm its rejection, propose amendments, or do neither. *Id.* If Parliament confirms its rejection of the common position by absolute majority, then the proposal cannot be adopted. *Id.* If Parliament proposes amendments to the common position, then the proposed amendments are treated as proposed amendments to the common position under the second option. *Id.* If Parliament neither rejects nor proposes to amend the common position, then the Council measure will pass whether the Parliament approves the common position or merely does nothing. BERMANN ET AL., *supra* note 23, at 90.

145. Directive, *supra* note 4, pmbl., O.J. L 281/31, at 31. When the Commission issued both its proposal and its amended proposal, the Commission provided for adoption of the Directive under the cooperation procedure ("cooperation") because the TEU had not yet introduced co-decision. *See* Commission Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, pmbl. O.J. C 277/03, at 3 (1990), COM (90) 314 Final-SYN 287 (July 27, 1990) [hereinafter Original Proposal] (noting that Council would act in cooperation with

Commission issued a comprehensive proposal, the Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data[146] ("Original Proposal"), for a directive to harmonize the national data protection laws of EC Member States.[147] The Economic and Social Committee[148] submitted its opinion on the Original Proposal on April 24, 1991.[149] Parliament conducted its first reading[150] of the Original Proposal.[151] Parliament reviewed the report of the

---

Parliament); Amended Commission Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, pmbl., O.J. C 311/04, at 30 (1992), COM (92) 422 Final-SYN 287 (Oct. 15, 1992) [hereinafter Amended Proposal] (noting that Council would act in cooperation with Parliament); EC Treaty, *supra* note 21, art. 189b, [1992] 1 C.M.L.R. at 694-95 (introducing co-decision); BERMANN ET AL., *supra* note 23, at 89 (explaining that TEU created co-decision procedure). When the Council adopted its common position on the Directive and when the Council and Parliament adopted the Directive, however, the Council and Parliament followed co-decision in accordance with Article 189b of the EC Treaty. Council Common Position Adopted by the Council with a view to adopting directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data EC No. 1/95, pmbl., O.J. C 93/1 (1995) [hereinafter Common Position]; Directive, *supra* note 4, pmbl., O.J. L 281/31, at 31 (1995). Although the proposal and the amended proposal provided for adoption under cooperation while the common position and the Directive used co-decision, this difference is not significant because the cooperation and co-decision procedures resemble one another at this early stage. BERMANN ET AL., *supra* note 23, at 89.

146. Original Proposal, *supra* note 145.

147. *See id.* recitals para. 6, O.J. C 277/03, at 3 (1990), COM (90) 314 Final-SYN 287, at 46 (1990) (proposing "to approximate" Member State laws to remove obstacles).

148. EC Treaty, *supra* note 21, art. 193, [1992] 1 C.M.L.R. at 698. The Economic and Social Committee is an advisory body to the Council and the Commission, consisting representatives of the Member States. *Id.* These Economic and Social Committee members also represent particular areas of economic and social activity. *Id.* The EC Treaty provides some circumstances when the Council or Commission must consult the Economic and Social Committee, but the Council or Commission may consult the Economic and Social Committee whenever they chose. *Id.* art. 198, [1992] 1 C.M.L.R. at 699; *see* BERMANN ET AL., *supra* note 23, at 83 (describing Economic and Social Committee).

149. Economic and Social Committee Opinion on the Proposal for Council Directive concerning the protection of individuals in relation to the processing of personal data, O.J. C 159/14, at 38 (1991).

150. EC Treaty, *supra* note 21, art. 189b(2), ¶ 2, [1992] 1 C.M.L.R. at 694; *see* BERMANN ET AL., *supra* note 23, at 84-86 (describing cooperation and co-decision procedures). Under co-decision and the cooperation procedures of Article 189c, the process by which the Council obtains initial suggestions from Parliament is Parliament's "first reading." *Id.* The process by which Parliament reviews a proposal for the second time is Parliament's "second reading." *Id.*

151. Explanatory Memorandum of Amended Proposal, *supra* note 33, COM (92) 422 Final-SYN 287, at 2 (1992).

Committee on Legal Affairs and Citizens' Rights[152] on February 10, 1992.[153] Next, Parliament approved the Original Proposal subject to various amendments on March 11, 1992.[154] Taking into account these suggestions, on October 15, 1992, the Commission presented the Amended Proposal for a Council Directive on the Protection of individuals with regard to the processing of personal data and on the free movement of such data[155] ("Amended Proposal").[156] On February 20, 1995, the Council unanimously adopted a common position ("Common Position"),[157] which it then sent back to Parliament for approval.[158]

---

152. WAYNE MADESON, HANDBOOK OF PERSONAL DATA PROTECTION 27 (1992). The Committee of Legal Affairs and Citizens' Rights is a committee of the Parliament. *Id.* When Parliament reviews proposals from the Commission, the proposals are first reviewed at committee level. BERMANN ET AL., *supra* note 23, at 80. Then Parliament expresses its opinion and suggests any amendments to the Commission. *See id.* (explaining that Commission frequently accepts Parliament's suggestions).

153. Explanatory Memorandum of Amended Proposal, *supra* note 33, COM (92) 422 Final-SYN 287, at 2 (1992).

154. O.J. C 94/173 (1992). Parliament approved the Commission proposal subject to 95 amendments. *See id.* (listing Parliament's suggested amendments next to text of Original Proposal).

155. Amended Proposal, *supra* note 145, pmbl., O.J. C 311/04, at 30 (1992), COM (92) 422 Final-SYN 287 (1992). In the Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("Amended Proposal"), the Commission accepted two of Parliament's major suggestions. Explanatory Memorandum of Amended Proposal, *supra* note 33, COM (92) 422 Final-SYN 287, at 2 (1992). The Amended Proposal dropped the distinction between the public and private sector made in the Original Proposal. *Id.* Further, the Amended Proposal expanded the provisions on notification of the supervisory authority and on codes of conduct. *Id.*

In response to Parliament's suggestions, the Amended Proposal also made other changes to the Original Proposal. *Id.* at 3-4. With the Amended Proposal, the Commission changed the Amended Proposal to address processing of personal data instead of files, to define third party, to apply to non-profit organizations, to make a mandatory exception for journalism, and to clarify the articles on transfers to third countries. *Id.*

156. Explanatory Memorandum of Amended Proposal, *supra* note 33, COM (92) 422 Final-SYN 287, at 2 (1992); *see* Hilary Pearson, *Data Protection in Europe: Recent Developments*, 12 COMPUTER LAW. 21, 21 (1995) (noting that Commission addressed some, but not all, of Parliament's amendments).

157. Common Position, *supra* note 145; *Council Adopts Common Position of Data Protection*, EUR. REP., Feb. 22, 1995 *available in* LEXIS, Intlaw Library, ECNews File [hereinafter Council Adopts Common Position]; Simitis, *supra* note 13, at 445.

158. Pearson, *supra* note 156, at 21; Council Adopts Common Position, *supra* note 157; *Protection of Personal Data – Council Signals Agreement*, RAPID, Dec. 9, 1994 *available in* LEXIS, Intlaw Library, Rapid File (noting Parliament would conduct second reading under co-decision after Council adopted Common Position); *see* EC Treaty, *supra* note 21, art. 189b(2), ¶ 2, [1992] 1 C.M.L.R. at 694 (setting forth requirement that Council send adopted common position to Parliament for Parliament's second reading).

In June 1995, during Parliament's second reading,[159] Parliament presented seven suggested amendments that the Commission later accepted.[160] On July 24, 1995, the Council unanimously adopted Parliament's suggested amendments to the Common Position.[161] Completing this co-decision procedure, both the President of the Council and the President of Parliament signed the Directive on October 24, 1995.[162] Because EC Member States have three years to comply with the legislation, they must conform their national legal systems with the Directive by October 23, 1998.[163]

2. Explanation and Scope of the Directive

The Directive sets forth the framework of data protection principles upon which Member States must harmonize their national laws.[164] The Directive seeks to advance the establishment and functioning of an internal market[165] which ensures the free

159. EC Treaty, *supra* note 21, art. 189b(2), ¶ 2, [1992] 1 C.M.L.R. at 694; BERMANN ET AL., *supra* note 23, at 80.

160. Parliament Decision on the common position established by the Council with a view to the adoption of a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. C 166/105 (1995); *see* d'Afflitto, *supra* note 25, at 308 n.13 (noting that amendments were accepted later).

161. *EU: Council Adopts Directive on Protection of Personal Data*, REUTER TEXTLINE, AGENCE EUROPE, July 26, 1995 *available in* LEXIS, Intlaw Library, Txtec File. Although adoption was unanimous, the United Kingdom abstained. *Id.* By accepting the modifications and adopting the Directive on July 24, 1995, the Council avoided the co-decision procedure that would require the Council to convene the Conciliation Committee under EC Treaty Article 189b. EC Treaty, *supra* note 21, art. 189b(3), [1992] 1 C.M.L.R. at 695; *see* d'Afflitto, *supra* note 25, at 308 (explaining Council's acceptance of Parliament's amendments avoided lengthy Article 189b procedure).

162. Directive, *supra* note 4, O.J. L 281/31, at 50 (1995).

163. d'Afflitto, *supra* note 25, at 306; *see* Directive, *supra* note 4, art. 32, O.J. L 281/31, at 49-50 (1995) (requiring Member States to comply with Directive within three years).

164. Directive, *supra* note 4, recitals para. 8, O.J. L 281/31, at 32 (1995). Recognizing that the obstacles caused by differences between how Member State laws protect the processing of personal data, the Directive strives to remove obstacles to flows of personal data by harmonizing the Member State laws. *Id.* recitals paras. 7-8, O.J. L 281/31, at 31-32 (1995).

165. *See* EC Treaty, *supra* note 21, art. 7a, ¶ 2, [1992] 1 C.M.L.R. at 592 (setting forth definition of internal market as "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured"); BERMANN ET AL., *supra* note 23, at 432-42 (discussing Community commitment to completing internal market). In 1984, after the Community's period of "Eurostagnation" when harmonization of Member State law had slowed, the Council decided to promote an internal market. BERMANN ET AL., *supra* note 23, at 432. At the Council's request, the Commission

movement of goods, persons, services, and capital.[166] In order to promote the internal market, the Directive balances two competing values or objectives.[167] The Directive takes into account that Member States should protect the fundamental privacy right of individuals[168] while maintaining the free flow of personal data among the Member States.[169] To achieve this free flow of personal data, the Directive attempts to ensure that the Member States provide equivalent protection of personal data.[170] If national data protection laws are equivalent, then the Member States will not inhibit transfers of personal data between themselves.[171] Member States, however, cannot attain this free movement of personal data at the cost of individual privacy.[172] Thus,

---

issued a White Paper setting forth a program to complete an internal market. *Id.* at 432-33; Commission of the European Communities, Completing the Internal Market: White Paper from the Commission to the European Council, COM (85) 310 FINAL (June 1985). Because of the widespread support for the internal market program, the Community amended the Community treaties through the Single European Act ("SEA") to facilitate the completion of the internal market. *See* BERMANN ET AL., *supra* note 23, at 436-37 (noting that internal market program may have been frustrated without SEA's changes). For example, the SEA introduced Article 100a, which permits the Council to adopt measures by less than unanimity. *Id.* at 439; EC Treaty, *supra* note 21, art. 100a, [1992] 1 C.M.L.R. at 633. The Council adopted the Directive pursuant to Article 100a, so unanimity was not necessary to adopt the Directive. Directive, *supra* note 4, pmbl., O.J. L 281/31, at 31 (1995).

166. *See* Directive, *supra* note 4, recitals para. 3, O.J. L 281/31, at 31 (1995) (setting forth objectives of Directive).

167. *Id.* art. 1, O.J. L 281/31, at 38 (1995).

> Article 1. Objective of the Directive.
>
> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Id.

168. *Id.* art. 1(2), O.J. L 281/31, at 38 (1995).

169. *Id.* art. 1(1), O.J. L 281/31, at 38 (1995).

170. *Id.* recitals para. 9, O.J. L 281/31, at 32 (1995).

171. *See id.* (stating that "given the equivalent protection resulting from the approximation of national law, the Member States will no longer be able to inhibit the free movement between them of personal data").

172. *Id.* recitals para. 10, O.J. L 281/31, at 32 (1995). Because:

> the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy . . . . [T]he approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

Id.

to protect personal data, the Directive establishes data protection standards with which Member States must comply.[173]

The scope of the Directive is limited in at least four major respects.[174] The Directive protects the privacy of natural persons, but not legal persons.[175] Moreover, it pertains only to personal data, or information about an identified or identifiable natural person.[176] The Directive also does not apply to the processing of personal data in certain situations.[177] Further, the Directive authorizes exceptions to the data protection principles that it establishes.[178]

While the Directive's scope is limited in some respects, the Directive establishes comprehensive principles of data protection.[179] These principles require that Member State data protection laws impose obligations on controllers, grant data sub-

---

173. *See* d'Afflitto, *supra* note 25, at 309 (noting that Directive sets forth rules to achieve harmonization of data protection laws).

174. *See id.* at 313-15 (relating three elements that delineate scope of Directive); CATE, *supra* note 31, at 36 (discussing scope and definitions of Directive including broad exemptions). Although the Directive explicitly applies to automated data processing, it does cover manual processing if that processing forms (or is intended to form) part of a filing system. Directive, *supra* note 4, art. 3(1), O.J. L 281/31, at 39 (1995).

175. *See* Directive, *supra* note 4, recitals para. 24, O.J. L 281/31, at 33 (1995) (noting that "legislation concerning the protection of legal persons with regard to the processing of data which concerns them is not affected by this Directive."). The term "natural persons" refers to human beings. BLACK'S LAW DICTIONARY, *supra* note 67, at 1142. The term "legal persons" includes legal entities. Boehmer & Palmer, *supra* note 39, at 282.

176. *See* Directive, *supra* note 4, art. 2(a), O.J. L 281/31, at 38 (1995) (defining personal data as "any information relating to an identified or identifiable natural person").

177. *See id.* art. 3(2), O.J. L 281/31, at 39 (1995) (governing scope of Directive). The Directive shall not apply to the processing of personal data outside the scope of EC law such as processing concerning public security, defense, State security, and criminal law. *Id.* Nor shall it apply to processing done by a natural person in the course of a purely personal or household activity. *Id.*

178. *See* Directive, *supra* note 4, arts. 9, 11(2), 13, 18, 26, O.J. L 281/31, at 41-46 (1995) (governing exceptions to Directive); CATE, *supra* note 31, at 36 (discussing Directive's exceptions). Article 13 provides the broadest exceptions to the Directive's main data protection principles. Directive, *supra* note 4, art. 13, O.J. L 281/31, at 42 (1995) (exempting Member State laws which violate Directive's data protection principles if these Member State laws are necessary to safeguard important interests such as national security or criminal law enforcement).

179. *See* d'Afflitto, *supra* note 25, at 315-19 (examining Directive's main data protection principles); CATE, *supra* note 31, at 37-41 (discussing basic protection of Directive).

jects[180] certain rights, and create a supervisory authority to enforce these laws.[181] The Directive requires that, as part of her obligations, a controller must maintain data quality[182] and notify the data subject of processing.[183] Further, the controller must notify the national supervisory authority of the purpose for the

---

180. *See* Directive, *supra* note 4, art. 2(a), O.J. L 281/31, at 38 (1995) (noting that data subject is person identified by his personal data).

181. *See id.* recitals para. 25, O.J. L 281/31, at 33 (1995) (setting forth principles of protection); d'Afflitto, *supra* note 25, at 315-16 (outlining types of data protection principles that Directive secures).

182. *See* Directive, *supra* note 4, arts. 6-7, O.J. L 281/31, at 31-32 (1995) (setting forth standard of data quality). Article 6 states that under Member State law, the controller must ensure that personal data are:

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes . . . ;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected . . . ;
(d) accurate and, where necessary, kept up-to-date . . . ; and
(e) kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected . . . .

Id. art. 6, O.J. L 281/31, at 40 (1995).

Article 7 specifies criteria under which processing of personal data is lawful. *See id.* recitals para. 30, O.J. L 281/31, at 34 (1995) (setting forth criteria for lawful data processing). Under Article 7, controllers may process personal data only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for performance of a contract to which the data subject is a party . . . ; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest . . . ; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Id. art. 7, O.J. L 281/31, at 40 (1995).

Sensitive data such as personal data revealing race, ethnicity, political affiliation, religion, and health receive extra protection under Article 8 of the Directive. *Id.* art. 8, O.J. L 281/31, at 40-41 (listing special categories of data). The Directive prohibits controllers from processing personal data in these special categories unless certain exemptions apply. *Id.* art. 8(2)-(3).

183. *See id.* art. 10, O.J. L 281/31, at 41 (1995) (requiring controller to inform data subject of at least controller's identity, purposes of processing, and data subject's right of access). When a controller has not obtained the personal information from the data subject, the controller may be exempted from this duty to notify when doing so is impossible or requires disproportionate effort. *Id.* art. 11(2), O.J. L 281/31, at 42 (1995).

processing[184] and ensure sufficient data security.[185]

The Directive also guarantees data subjects certain rights.[186] These rights include the right to be informed when the controller is processing their personal data,[187] the right to access that data,[188] the right to object to processing,[189] and the right to have the controller rectify incorrect personal data.[190] Additionally, Member States must establish independent authorities with supervising, intervening, and consulting duties.[191]

---

184. *See id.* art. 18(1), O.J. L 281/31, at 43-44 (1995) (stating that controller "must notify the supervisory authority . . . before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes."). Member States may, however, simplify or exempt controllers from notification under certain conditions. *Id.* art. 18(2) & (4), O.J. L 281/31, at 44 (1995).

185. *See id.* art. 17, O.J. L 281/31, at 43 (1995) (governing security of data processing). "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, . . . and against all other forms of unlawful forms of processing." *Id.* art. 17(1), O.J. L 281/31, at 43 (1995).

186. *See id.* recitals para. 25, O.J. L 281/31, at 33 (1995) (explaining that data protection principles must be reflected in the rights conferred on individuals).

187. *See id.* arts. 10-11, O.J. L 281/31, at 41-42 (1995) (stating controller's obligation to inform data subject of collection of data subject's personal information); d'Afflitto, *supra* note 25, at 318 (explaining that data subject's right to be informed derives from controller's obligation to inform).

188. *See* Directive, *supra* note 4, art. 12, O.J. L 281/31, at 42 (1995) (governing right of access to personal data).

> Member States shall guarantee every data subject the right to obtain from the controller . . . without constraint at reasonable intervals and without excessive delay or expense . . . confirmation as to whether or not data relating to him are being processed and information at least as to the purpose of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed . . . .

Id. This right is among those subject to several exceptions and restrictions of Article 13. *Id.* art. 13, O.J. L 281/31, at 42 (1995).

189. *See id.* art. 14(a), O.J. L 281/31, at 42-43 (1995) (setting forth data subject's right "to object at any time on compelling legitimate grounds . . . to the processing of data relating to him").

190. *See id.* art 12(b), O.J. L 281/31, at 42 (1995) (explaining data subject's "right to obtain from the controller . . . as appropriate the rectification, erasure or blocking of data" which is incomplete or inaccurate).

191. *See id.* art. 28, O.J. L 281/31, at 47-48 (1995) (setting forth powers and duties of supervisory authority). For example, Member States should consult the authorities when drafting new data protection measures. *Id.* art. 28(2), O.J. L 281/31, at 47 (1995). Further, Member States must empower these authorities to investigate data processing and intervene when processing has violated the national data protection law. *Id.* art. 28(3), O.J. L 281/31, at 47 (1995).

3. Transfers of Personal Data to Third Countries

In addition to setting rules for the treatment of personal data within the Community, the Directive regulates the transfer of personal data to third countries.[192] Regulation of transfers to third countries is necessary because third countries, unaffected by the Directive, may not provide substantial data protection.[193] If a controller in a Member State transfers personal data to a third country with insufficient data protection, then the legal protection that the Member State provides such data under the Directive would be lost once the data arrives in the third country.[194] Thus, the Directive permits Member States to transfer personal data to a third country only if that third country ensures an adequate level of protection.[195]

The Directive recognizes that when determining whether to permit transfers of personal data to third countries, the Member States must balance the Directive's original two objectives.[196] The free flow of information to third countries is necessary for international trade.[197] Such transfers, however, cannot violate an individual's right to privacy.[198] In order to ensure that transfers of personal data to third countries do not cripple international trade while still protecting personal data, the Directive requires that the third countries ensure adequate protection of the personal data.[199] If the third country provides adequate protec-

---

192. *Id.* arts. 25-26, O.J. L 281/31, at 45-46 (1995).

193. *See* NUGTER, *supra* note 14, at 4 (discussing legitimate need to safeguard privacy in international context).

194. *See* Explanatory Memorandum of Amended Proposal, *supra* note 33, COM (92) 422 Final-SYN 287, at 34 (1992) (explaining that without Article 25, transfers to third countries could nullify Community data protection); Gellman, *supra* note 14, at 158 (describing need for Article 25).

195. *See* Directive, *supra* note 4, art. 25(1), O.J. L 281/31, at 47 (1995) (stating that "the transfer to a third country of personal data which are undergoing processing . . . may take place only if . . . the third country in question ensures an adequate level of protection."). In contrast, the Directive requires an equivalent level of protection Between Member States. *See id.* recitals para. 8, O.J. L 281/31, at 32 (1995) (demanding that "the level of protection . . . must be equivalent in all the Member States.").

196. *See id.* recitals paras. 56-57, O.J. L 281/31, at 36-37 (1995) (governing balance between Directive's two objectives with respect to data transfers to third countries).

197. *See id.* recitals para. 56, O.J. L 281/31, at 36-37 (1995) (stating that "cross-border flows of personal data are necessary to the expansion of international trade").

198. *See id.* recitals para. 57, O.J. L 281/31, at 37 (1995) (noting that "transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited").

199. *Id.* art. 25(1), O.J. L 281/31, at 45 (1995).

tion, then the transfer will not violate the individual's right to informational privacy.[200] In such an instance, because the transfer will not violate this right, personal data necessary for international trade may flow freely.[201]

Article 25[202] of the Directive sets forth the procedure by which Member States and the Commission should determine whether protection in a third country is adequate.[203] This procedure involves a case-by-case analysis of data transfers or sets of transfers rather than an overall country assessment.[204] Under Article 25's procedures, the Member States and the Commission must inform each other of cases where a third country does not provide an adequate level of protection.[205] The Commission then may determine, pursuant to the procedure described in Article 31(2), whether the third country fails to ensure adequate protection for transfers of a certain type.[206] If the Commission

---

200. *Id.* art. 1(1), O.J. L 281/31, at 38 (1995).

201. *Id.* art. 1(2), O.J. L 281/31, at 38 (1995).

202. *See id.* art. 25, O.J. L 281/31, at 45-46 (1995) (setting forth adequacy test for transfers to third countries).

203. *Id.*

204. *See* Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 294 (1993) [hereinafter Reidenberg, *Rules of the Road*] (noting that Amended Proposal provided for case-by-case analysis of data transfers to third countries). *Compare* Amended Proposal, *supra* note 145, art. 26, O.J. C 311/04, at 55-56 (1992), COM (92) 422 Final-SYN 287, at 104-07 (1992) (setting forth case-by-case analysis of transfers to third countries) *with* Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45-46 (1995) (adopting case-by-case approach to assessing transfers to third countries with language almost identical to Amended Proposal).

205. *See* Directive, *supra* note 4, art. 25(3), O.J. L 281/31, at 46 (1995) (instructing Member States and Commission to inform each other of particular cases where third country has inadequate data protection). Thus, this provision, unlike its earlier version in the Original Proposal, does not require Member States to assess the adequacy of a third county's overall data protection and decide if a total ban to that third country is necessary. *See* Reidenberg, *Rules of the Road*, *supra* note 204, at 293-94 (contrasting Original Proposal's provision for overall country assessment of adequacy with Amended Proposal's case-by-case approach); Original Proposal, *supra* note 145, art. 24, O.J. C 277/03, at 11 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990) (making no provisions for case-by-case analysis of data transfers to third countries); Amended Proposal, *supra* note 145, art. 26, O.J. C 311/04, at 55 (1992), COM (92) 422 Final-SYN 287, at 106 (1992) (providing for case-by-case analysis of third country transfers in light of all circumstances); Directive, *supra* note 4, art. 25, O.J. C 281/31, at 45-46 (1995) (adopting case-by-case review of data transfers to third countries). Instead, Article 25(3) provides for a case-by-case analysis of third country transfers. Reidenberg, *Rules of the Road*, *supra* note 204, at 294.

206. *See* Directive, *supra* note 4, art. 25(4) & (6), O.J. L 281/31, at 46 (1995) (setting forth consequences depending upon whether or not Commission finds third coun-

finds that the third country does not provide adequate protection under these circumstances, then Member States must prevent transfers of this type to the third country.[207] If the Commission, however, finds that the third country does ensure adequate protection, then the Member States must permit the transfers.[208] In addition, the Directive empowers the Commission to enter into negotiations with a third country that fails to provide an adequate level of protection so that the third country can remedy the situation.[209]

In Article 26, the Directive sets forth two categories of exceptions where Member States may permit the transfer of personal data to a third country that does not ensure an adequate level of protection.[210] Under Article 26(1), a Member State

---

tries' data protection adequate). The Directive requires that a Member State or the Commission inform the other parties of a third country that does not provide adequate protection for a data transfer. *Id.* art. 25(3), O.J. L 281/31, at 46 (1995). The Directive does not, however, require the Commission to make a formal determination of adequacy. *See id.* art. 25, O.J. L 281/31, at 45-46 (1995) (permitting, but not requiring, Commission to determine adequacy under Article 31(2) procedure).

If the Commission decides to assess a third country's level of protection, the Commission must make this assessment under the procedure provided for in Article 31(2). *Id.* art. 25(4) & (6), O.J. L 281/31, at 46 (1995). Under Article 31(2), a committee comprised of the representatives of the Member States and chaired by the representative of the Commission assists the Commission. *Id.* art. 31(1), O.J. L 281/31, at 49 (1995).

Under this procedure, the Commission representative first submits the Commission's proposed measures to the committee. *Id.* art. 31(2), O.J. L 281/31, at 49 (1995). Then the committee must deliver an opinion on the proposal. *Id.* This opinion will be decided by qualified majority, as set out in Article 148(2) of the EC Treaty, and the chairperson cannot vote. *Id.*

If the committee supports the measure in the draft, then the Commission's proposal shall apply immediately. *Id.* If the committee does not support these measures, then Commission must communicate its measures to the Council immediately. *Id.* The Council has three months to overrule the Commission's proposal by a qualified majority. *Id.* During this three month period, the Commission must not apply the measures, but when this period expires, the Commission can adopt the proposed measures. *Id.*

207. *See id.* art. 25(4), O.J. L 281/31, at 46 (1995) (stating that "[w]here the Commission finds . . . that a third country does not ensure an adequate level of protection . . . Member States shall take measures necessary to prevent any transfer of data of the same type to the third country in question.").

208. *See id.* art. 25(6), O.J. L 281/31, at 46 (1995) (noting that where "[t]he Commission may find . . . that a third country ensures an adequate level of protection . . . Member States shall take the measures necessary to comply with the Commission's decision.").

209. *Id.* art. 25(5), O.J. L 281/31, at 46 (1995).

210. *See id.* art. 26(1)-(2), O.J. L 281/31, at 46 (1995) (setting forth derogations from Article 25). These exceptions are very similar to the justifications for data process-

must exempt a transfer from the requirements of Article 25 if the transfer meets one of six conditions.[211] It is uncertain how broadly Member States will interpret these exceptions.[212]

Article 26(2) also provides Member States with an exception from Article 25.[213] Article 26(2) permits a Member State to authorize a transfer to a third country without adequate protection where the controller of the data determines that adequate safeguards of individuals' privacy rights exist.[214] If a Member State exempts a transfer under Article 26(2) rather than Article 26(1), then the Member State must inform the Commission and the other Member States of the authorization.[215] If the Commission or another Member State objects to the authorization, the Commission must decide whether the authorization was proper[216] and the Member States must comply with the Commission's decision.[217]

While the Directive establishes the procedure for determining where protection is adequate[218] and sets forth the exceptions

---

ing listed in Article 7 of the Directive. *See id.* art. 7, O.J. L 281/31, at 40 (1995) (listing criteria for making data processing legitimate).

211. *Id.* art. 26(1), O.J. L 281/31, at 46 (1995). The six derogations under Article 26(1) are: (1) the data subject has consented to the transfer; (2) the transfer is necessary for performance of a contract between the data subject and the controller; (3) the transfer is necessary for the conclusion or performance of a contract concluded in data subject's interest grounds; (4) the transfer is necessary for or legally required by an important public interest; (5) the transfer is necessary to protect data subject's vital interests; or (6) the transfer is made from a public register. *Id.* The Directive does not require Member States to inform the Commission and other Member States when they use the Article 25(1) exemptions. *See id.* art. 26(1), O.J. L 281/31, at 46 (1995) (making no mention of obligation to notify Commission or other Member States).

212. *See* Gellman, *supra* note 14, at 157 (analyzing Article 25 of Directive).

213. Directive, *supra* note 4, art. 26(2), O.J. L 281/31, at 46 (1995).

214. *See id.* art. 26(2), O.J. L 281/31, at 46 (1995) (noting that "such [adequate] safeguards may in particular result from appropriate contractual clauses.").

215. *Id.* art. 26(3), O.J. L 281/31, at 46 (1995).

216. *Id.* The Commission will reach its decision in accordance with the procedure laid down in Article 31(2). *Id.* This procedure involves referral by a representative of the Commission to a committee of Member State representatives. *Id.* art 31(1), O.J. L 281/31, at 49 (1995).

217. *Id.* art. 26(3)-(4), O.J. L 281/31, at 46 (1995). Thus, if the Commission decides that the authorization violated an individual's privacy rights, then the Member State could not authorize the transfer. *Id.* art. 26(3), O.J. L 281/31 at 46 (1995). If the Commission found that the authorization was proper because certain contractual clauses offered sufficient safeguards, however, then objecting parties must accept this decision. *Id.* art. 26(4), O.J. L 281/31, at 46 (1995).

218. *See id.* art. 25, O.J. L 281/31, at 45-46 (1995) (setting forth procedure for determining adequacy of third country's data protection).

where Member States may make a transfer to a third country whose protection is not adequate,[219] the Directive does not clearly explain what constitutes adequate protection.[220] Article 25(2) does note that Member States should assess the adequacy of a third country's level of protection in light of the circumstances surrounding the transfer.[221] These circumstances include the nature of the personal data, the purpose and nature of the proposed processing, the country of origin, the country of final destination, the rules of law in the third country, and the professional rules and security measures in the third country.[222] The Directive mentions these factors, but provides no other guidance as to how the supervisory authorities of the Member States should determine whether protection is adequate.[223] Consequently, it will be difficult for Member States to determine which third countries do not ensure an adequate level of protection and under what circumstances.[224]

4. Article 29 Working Party

Article 29 of the Directive establishes a Working Party[225] to advise the Commission on data protection matters and to contribute to the uniform application of the national data protection measures.[226] The Working Party is an independent advisory group composed of a representative from each Member State's supervisory authority, a representative of the Community, and a

---

219. *See id.* art. 26, O.J. L 281/31, at 46 (1995) (governing exceptions Article 25 of Directive).

220. *See id.* art. 25, O.J. L 281/31, at 45-46 (1995) (providing procedures to determine when third country ensures adequate protection, but not explicitly stating what constitutes adequate protection).

221. *See id.* art. 25(2), O.J. L 281/31, at 45-46 (1995) (setting forth factors by which Member States should assess adequacy of data protection).

222. *Id.*

223. *See id.* (listing surrounding circumstances, but not analyzing them).

224. Gellman, *supra* note 14, at 157 (noting uncertainty about how Member States will apply provisions on third country transfers).

225. Directive, *supra* note 4, art. 29(1), O.J. L 281/31, at 48 (1995); *see* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, First Annual Report, XV/5025/97-Final Corr. EN, adopted June 25, 1997, at 4 [hereinafter First Annual Report] (discussing role, composition, and progress of Working Party). The Working Party is formally named "A Working Party on the Protection of Individuals with regard to the Processing of Personal Data." *Id.*

226. *See* Directive, *supra* note 4, recitals para. 65, O.J. L 281/31, at 37 (1995) (stating that Working Party, completely independent in its functions, must advise the Commission and contribute to the uniform application of national rules).

representative of the Commission.[227] The Directive charges the Working Party to examine the Member States' data protection laws and give the Commission opinions on the level of protection in the EC Member States and in third countries.[228] Further, the Working Party may make recommendations relating to data protection in the Community.[229] The Working Party must forward these opinions and recommendations to the Article 31 committee[230] and the Commission.[231] After adopting measures pursuant to the Article 31 procedure,[232] the Commission must inform the Working Party of its decision.[233] Finally, the Working Party must submit an annual report on the data protection in the Community and in third countries to the Commission, the European Parliament, and the Council.[234] Through these three functions the Working Party has an opportunity to influence the interpretation of the Directive.[235]

In particular, the Working Party can influence the Commission's interpretation of what constitutes an adequate level of protection in a third country under Article 25.[236] By giving opinions on the level of protection in third countries, the Working Party

---

227. *See id.* art. 29(2), O.J. L 281/31, at 48 (1995) (noting that "[e]ach member of the Working Party shall be designated by the institution, authority or authorities which he represents."). These institutions and authorities shall nominate joint representatives if they have more than one supervisory authority. *Id.*

228. *See id.* art. 30(1), O.J. L 281/31, at 48 (1995) (setting forth Working Party's duties). In addition, the Working Party must advise the Commission on proposed amendments to the Directive, on additional measures to safeguard data protection, and on any other Community measure affecting data protection rights. *Id.* art. 30(1)(c), O.J. L 281/31, at 48 (1995). If the Working Party finds divergences between Member State data protection laws that might affect the equivalence of data protection, then the Working Party must inform the Commission of the divergences. *Id.* art. 30(2), O.J. L 281/31, at 48 (1995).

229. *Id.* art. 30(3), O.J. L 281/31, at 48 (1995).

230. *See id.* art. 31, O.J. L 281/31, at 49 (1995) (establishing committee of Member State representatives to assist Commission).

231. *Id.* art. 30(4), O.J. L 281/31, at 48 (1995).

232. *See id.* art. 31(2), O.J. L 281/31, at 49 (1995) (setting forth procedure for Article 31 committee).

233. *Id.* art. 30(5), O.J. L 281/31, at 48-49 (1995). The Commission must also report to the Council and Parliament on its response to the Working Party's opinion or recommendation. *Id.*

234. *Id.* art. 30(6), O.J. L 281/31, at 49 (1995). The Working Party's annual report shall be made public. *Id.*

235. *See id.* art. 30, O.J. L 281/31, at 48-49 (1995) (describing role of Working Party).

236. *See id.* art. 30, O.J. L 281/31, at 48-49 (1995) (setting forth powers of Working Party).

can help define adequate protection by identifying the third countries that it considers provide such protection.[237] In the Working Party's annual report, the Working Party must report to the Commission on data protection in third countries.[238] Although the Working Party cannot make recommendations about whether a third country ensures adequate protection in a specific case, the Working Party can take positions suggesting how Member States should assess adequacy.[239] While the Working Party has not taken any formal steps to define adequate protection in an opinion or an annual report, the Working Party did adopt a discussion document on June 26, 1997 that examines possible ways to determine whether third countries provide adequate protection.[240]

C. *Current U.S. Protection of Personal Data: Sectoral Approach*

The U.S. ad hoc, sectoral approach to data protection flows from the U.S. regulatory philosophy.[241] In the public sector, U.S. data protection regulates the treatment of personal data on the constitutional, federal, and state levels.[242] Data protection in the private sector involves targeted regulation at both the federal and state level as well as varying degrees of self-regulation.[243]

1. Overview of the Sectoral Approach

Unlike the Community, during the 1990s, the United States

237. *See id.* art. 30(1)(b), O.J. L 281/31, at 48 (1995) (empowering Working Party to give opinions on level of protection in third countries). The Working Party has not yet issued any opinions on the level of data protection in third countries, but on May, 29, 1997, it adopted Opinion 1/97 on Canadian initiatives relating to standardization in the field of protection of privacy. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/97, XV/5023/97-Final Corr. EN, adopted May 29, 1997.

238. *See* Directive, *supra*, note 4, art. 30(6), O.J. L 281/31, at 49 (1995) (requiring Working Party to report annually on data protection in Community and third countries). The Working Party adopted its First Annual Report on June 23, 1997. First Annual Report, *supra* note 225. This report did discuss data protection in third countries, but did not focus on what constitutes an adequate level of protection. *Id.*

239. *See* First Orientations, *supra* note 48, at 2 (explaining that although Working Party has no explicit role to give recommendations on specific transfers, its work can provide guidance on groups of transfers).

240. *Id.*

241. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 7 (commenting on framework of U.S. data privacy regulation).

242. *Id.* at 205.

243. *Id.* at 215.

has not adopted an omnibus approach to the protection of personal data.[244] Instead, the United States continues to address personal data problems through ad hoc, sector-by-sector solutions.[245] European data protection laws actively regulate the processing of personal data across both the private and public sectors.[246] In contrast, while U.S. data privacy legislation addresses the treatment of personal information by the government, few U.S. laws regulate the processing of such data by the business world.[247]

The United States' narrow approach to data protection follows from the U.S. philosophy that laws should ensure citizens' access to government, while still protecting them from government.[248] This U.S. tradition of a limited government enables the United States to regulate the public sector extensively, but generally prevents the federal government from limiting interactions between private citizens.[249] The U.S. Constitution established this tradition by focusing on the principles of federalism and separation of powers rather than upon restricting individuals' actions.[250] Further, the U.S. Supreme Court's rights jurisprudence protects individuals against the government rather than protecting individuals against each other.[251]

The U.S. commitment to the free flow of information also

---

244. *See* CATE, *supra* note 31, at 49-50 (noting complexity of U.S. data protection); SCHWARTZ & REIDENBERG, *supra* note 8, at 7 (describing U.S. regulatory framework).

245. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 7 (describing targeted U.S. regulation); Scott, *supra* note 65, at 487 (discussing lack of coherent data protection regulating system in United States).

246. *See* Explanatory Memorandum of Amended Proposal, *supra* note 33, COM (92) 422 Final-SYN 287, at 2 (1992) (explaining that Amended Proposal dropped distinction between public and private sectors); SCHWARTZ & REIDENBERG, *supra* note 8, at 5 (noting that European data protection laws actively regulate data processing).

247. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 5 (contrasting European and U.S. data protection laws).

248. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 500 (describing U.S. constitutional emphasis on restraining government); SCHWARTZ & REIDENBERG, *supra* note 8, at 6 (discussing U.S. regulatory philosophy); CATE, *supra* note 31, at 52 (explaining basic features of U.S. constitutional rights).

249. SCHWARTZ & REIDENBERG, *supra* note 8, at 6.

250. *Id.* State constitutions also emphasize the powers and limits of the state government rather than regulating actions between state citizens. *See id.* at 9-10 (noting California as rare exception).

251. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 502 (discussing U.S. constitutional emphasis on restraining government).

favors a narrow regulatory approach to data protection.[252] The traditional emphasis on protecting individuals against the government led to this commitment to the free flow of information.[253] In order to preserve this free flow, the government places minimal restrictions on the treatment of personal information by citizens while restricting its own use of such information.[254]

As a result of the United States' reluctance to regulate the private sector and its commitment to the free flow of information, the United States has adopted an ad hoc, sectoral approach to data protection.[255] Under this sectoral framework, comprehensive laws addressing both the private sector and public sector are rare.[256] Instead, the data privacy laws target either the government or business because these laws regulate how the government treats personal information differently than how businesses treat such information.[257] Further, while U.S. regulations targeted at the public sector occasionally have a broad scope,[258] those directed at the private sector generally address only specific issues.[259] To compensate for the minimal legal restrictions

252. *See id.* at 506 (explaining that in following principle of free flow of information, U.S. legislatures respond in ad hoc, sectoral manner).

253. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 6 (explaining U.S. commitment to assure freedom for press and communications). In contrast, the European approach to values the free flow of information less than the U.S. approach does. James R. Maxeiner, *Business Information and "Personal Data": Some Common-law Observations about the EU Draft Protection Directive*, 80 IOWA L. REV. 619, 622 (1995). While the EU Directive's second objective is to ensure the free flow of information, the Directive's first objective is to protect "the right to privacy with respect to the processing of personal data." Directive, *supra* note 4, art. 1, O.J. L 281/31, at 38 (1995).

254. SCHWARTZ & REIDENBERG, *supra* note 8, at 6.

255. *See id.* at 7 (explaining that United States adopts sectoral legislation to minimize interruption of free flow of information). The success of the ad hoc, sectoral approach is also due to strong lobbying against increased regulation of the private sector by American businesses. Reidenberg & Gamet-Pol, *supra* note 2, at 113.

256. SCHWARTZ & REIDENBERG, *supra* note 8, at 7.

257. *Id.* at 7-8.

258. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 506 n.47 (noting that at both federal and state levels, legislatures have sought broader regulation of public sector); *see, e.g.*, The Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996); California Information Practices Act of 1977, Cal. Civ. Code §§ 1798-1798.78 (West 1985 & Supp. 1998); New York Personal Privacy Protection Law, N.Y. Pub. Off. §§ 91-99 (McKinney 1988 & Supp. 1997-1998).

259. Reidenberg, *Setting Standards*, *supra* note 53, at 506; *see, e.g.*, The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998); The Electronic Communications Privacy Act, 15 U.S.C. §§ 2510-2511, 2701-2709 (1988 & Supp. V 1993), *amended by* 15 U.S.C.A. §§ 2510-2511, 2701-

upon businesses, the private sector has attempted to regulate itself through both industry standards and company policies.[260] Voluntary self-regulation is problematic, however, because neither the industry standards nor the companies' own policies are binding.[261]

Despite adopting such a complex regulatory framework, the United States has no single government organization to assess the various privacy issues related to data protection.[262] Instead, numerous federal agencies share the task of assessing informational privacy, often competing for jurisdiction.[263] The Clinton Administration has established the Information Infrastructure Task Force[264] ("IITF") to articulate and implement a vision for the National Information Infrastructure ("NII").[265] The IITF,

---

2709 (West Supp. 1997); The Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1994).

260. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 11 (describing industry self-regulation); REGAN, *supra* note 3, at 85 (noting that private sectors established data protection policies to thwart legislation).

261. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 11 (noting corporate policies lack enforcement mechanisms).

262. Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 922 (1996) [hereinafter Reidenberg, *Governing Networks*]. The Privacy Protection Study Commission ("PPSC") examined privacy issues in both public and private sector from 1974 to 1977, but the Commission no longer exists. REGAN, *supra* note 3, at 85. The Federal Privacy Board that the PPSC recommended was never formed. *Id.*

263. Reidenberg, *Governing Networks*, *supra* note 262, at 922. These agencies include the Federal Communications Commission, the Federal Trade Commission, the Commerce Department's National Telecommunications and Information Administration, the State Department, the United States Trade Representative, and the National Institute for Standards and Technology. *Id.*

264. *See* CATE, *supra* note 31, at 91 (relating history of the Information Infrastructure Task Force ("IITF")). The IITF consists of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies. *See* Information Infrastructure Task Force, *About the President's Information Infrastructure Task Force* (visited Feb. 15, 1998) <http://www.iitf.nist.gov/about.html> (also on file with *Fordham International Law Journal*). This task force is responsible for developing comprehensive technology, information, and telecommunications technologies. *See* CATE, *supra* note 31, at 91 & n.86 (describing role and structure of IITF). The Privacy Working Group, part of the Information Policy Committee, develops proposals on the protection of individual privacy. *Id.*

265. CATE *supra* note 31, at 91; *see* William J. Drake, *Introduction: The Turning Point*, *in* THE NEW INFORMATION INFRASTRUCTURE: STRATEGIES FOR U.S. POLICY 4-8 (William J. Drake ed., 1995) (describing National Information Infrastructure ("NII")). The NII is "a vast collection of networks, most of them privately owned and operated." *Id.* at 4. The NII has been defined both broadly and narrowly. *See id.* at 5 (contrasting broad and narrow definitions). The Clinton Administration defines the NII broadly as including all of the equipment used to transmit information, the information itself, the applications that allow individuals to use the information, the network standards that facili-

however, has adopted the ad hoc, sectoral approach to the NII, making comprehensive data protection changes unlikely.[266]

2. Public Sector

U.S. law in the public sector provides substantial protection to personal data.[267] Because the U.S. regulatory philosophy encourages regulation of the government[268] and because U.S. citizens recognize the importance of informational privacy,[269] the United States has developed a system of legal rules to protect personal information in the public sector.[270] Although the United States does not have a single law or constitutional provision ensuring that the government adopts fair information practices, the United States possesses a legal framework that protects informational privacy in the private sector on three basic levels.[271] U.S. constitutional protections provide some regulation of the government's treatment of personal data.[272] Federal legislation provides individuals with the most substantial protection of personal information.[273] Finally, state data protection laws often attempt to secure privacy for individuals, although

---

tate exchange of information between networks, and the people who create information, applications, and services. *Id.* Others have defined the NII more narrowly as "the computerized networks, intelligent terminals, accompanying applications and services people use to access, create, disseminate, and utilize digital information." *Id.*

266. *See* Reidenberg, *Governing Networks*, *supra* note 262, at 923 (discussing IITF sectoral thinking and reactive tendencies).

267. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 206 (reviewing U.S. data protection in public sector).

268. *Id.* at 6.

269. *See* REGAN, *supra* note 3, at 43 (citing Harris public opinion polls). Various public opinion surveys during the last twenty years demonstrate U.S. citizens' concern with threats to personal privacy. *See id.* at 46-68 (discussing significance of U.S. public opinion polls). *See generally* LOUIS HARRIS AND ASSOCIATES AND ALAN F. WESTIN, THE DIMENSIONS OF PRIVACY: A NATIONAL OPINION RESEARCH SURVEY OF ATTITUDES TOWARD PRIVACY (1979); LOUIS HARRIS AND ASSOCIATES AND ALAN F. WESTIN, THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE (1990).

270. SCHWARTZ & REIDENBERG, *supra* note 8, at 206.

271. *See id.* at 206 (summarizing protection of U.S. Constitution, federal statutes, and state law).

272. *See id.* at 206-07 (outlining U.S. constitutional protections of personal data); CATE, *supra* note 31, at 50-66 (discussing privacy protections in four constitutional areas). *See generally* SCHWARTZ & REIDENBERG, *supra* note 8, at 29-90 (examining data protection under U.S constitutional law).

273. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 277 (outlining U.S. statutory protections of personal data in public sector); CATE, *supra* note 31, at 76-79 (examining federal data protection statutes). *See generally* SCHWARTZ & REIDENBERG, *supra* note 8, at 91-128 (analyzing data protection under federal statutes).

they rarely provide significant protection.[274]

While the U.S. Constitution does not explicitly protect informational privacy,[275] the U.S. Supreme Court has found that in the public sector, certain constitutional provisions protect various privacy interests, including informational privacy.[276] For instance, the Supreme Court has upheld certain political rights such as associational privacy[277] and political privacy.[278] By protecting people from unreasonable searches and seizures, the Fourth Amendment also provides some protection of informational privacy.[279] Some commentators argue that the Fifth Amendment also protects privacy.[280]

In addition to the related rights that partially protect personal information, the U.S. Supreme Court eventually recognized a limited right to informational privacy.[281] The Supreme

274. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 208-09 (outlining U.S. data protection at state level); CATE, *supra* note 31, at 66-68 (discussing state constitutional data protection). *See generally* SCHWARTZ & REIDENBERG, *supra* note 8, at 129-51 (examining state data protection).

275. *See* REGAN, *supra* note 3, at 35 (noting that Bill of Rights does not mention "right to privacy").

276. Whalen v. Roe, 429 U.S. 589 (1977); REGAN, *supra* note 3, at 35; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 43-90 (examining U.S. constitutional protection of personal information). The U.S. Supreme Court has derived aspects of the right to privacy from the First, Third, Fourth, Fifth, and Ninth amendments as well as from the due process clause of the Fourteenth Amendment. REGAN, *supra* note 3, at 35.

277. Roberts v. U.S. Jaycees, 468 U.S. 609 (1984); NAACP v. Alabama, 357 U.S. 449 (1958); *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 44-45 (discussing associational privacy). The right to association has two branches: (1) freedom of expressive association and (2) freedom of intimate association. *Roberts*, 468 U.S. at 617. This freedom of expressive association involves the right to associate "for the advancement of beliefs and ideas." *NAACP*, 357 U.S. at 460; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 45-46 (discussing right to associate for expressive activity). Likewise, the freedom of intimate association protects the right to form and preserve certain types of highly personal relationships. *Roberts*, 468 U.S. at 618; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 49-51 (discussing right to intimate association).

278. *See* Watkins v. United States, 354 U.S. 178, 198-99 (1957) (relating need to balance privacy concerns against public interest); Sweezy v. New Hampshire, 354 U.S. 234, 250 (1957) (discussing right to engage in political expression and association).

279. *See* REGAN, *supra* note 3, at 35-38 (discussing Fourth Amendment privacy jurisprudence); SCHWARTZ & REIDENBERG, *supra* note 8, at 60-73 (examining Fourth Amendment data protection); CATE, *supra* note 31, at 57-60 (noting limitations of Fourth Amendment data protection).

280. *See* REGAN, *supra* note 3, at 38 (examining data protection by Fifth Amendment protection against self-incrimination); CATE, *supra* note 31, at 72-75 (discussing relation between data protection and Fifth Amendment).

281. *See* Whalen v. Roe, 429 U.S. 589 (1977) (recognizing right to informational privacy).

Court's jurisprudence began establishing an independent right to privacy by recognizing that the U.S. Constitution gave people the freedom to make decisions about marital and familial matters.[282] Later, in *Whalen v. Roe*,[283] the U.S. Supreme Court recognized a constitutional interest in protecting informational privacy.[284] The *Whalen* Court found that a New York law centralizing state drug prescriptions affected an interest in avoiding disclosure of personal matters.[285]

The federal government has created a statutory framework that regulates informational privacy in the public sector.[286] These statutory protections were necessary to secure informational privacy because the common-law privacy torts and the constitutional protections failed adequately to do so.[287] The most comprehensive of these federal laws is the Privacy Act,[288] but the subsequent statutes have supplemented this one.[289] While these federal statutes regulate the collection, use, and disclosure of personal information, they are difficult to enforce because an individual must bring suit against the government.[290]

The Privacy Act regulates the federal agencies'[291] collection,

---

282. Griswold v. Connecticut, 381 U.S. 479 (1965) (finding "the zone of privacy" under penumbra of First, Third, Fourth, Fifth, and Ninth Amendments); Roe v. Wade, 410 U.S. 113 (1973) (finding right to privacy under Fourteenth Amendment).

283. Whalen v. Roe, 429 U.S. 589 (1977).

284. *Id.* at 599; *see* REGAN, *supra* note 3, at 40 (discussing *Whalen v. Roe*).

285. *See Whalen*, 429 U.S. at 600 (recognizing "individual interest in avoiding disclosure of personal matters").

286. SCHWARTZ & REIDENBERG, *supra* note 8, at 207.

287. *See* REGAN, *supra* note 3, at 70 (explaining need for new statutory protections of informational privacy).

288. The Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996).

289. *See* The Computer Matching Act and Privacy Protection Act of 1988, 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o)-(r), (u) (1994 & Supp. 1996) (regulating federal data matching); 13 U.S.C. §§ 8-9 (1994) (regulating disclosure of census data); The Driver's Privacy Protection Act of 1994, 18 U.S.C.A. § 2721 (West Supp. 1997) (prohibiting release of motor vehicle records); I.R.C. §§ 6103, 7431 (1994), *amended by* I.R.C. § 6103 (West Supp. 1997) (prohibiting disclosure of income tax returns); 42 U.S.C. § 1306 (1994) (regulating disclosure of social security records); The Paperwork Reduction Act, 44 U.S.C. §§ 3501-3520 (1994), *amended by* 44 U.S.C.A. §§ 3501-3520 (West Supp. 1997) (regulating paperwork of federal government); SCHWARTZ & REIDENBERG, *supra* note 8, at 92 (noting that numerous federal laws address treatment of personal data in public sector).

290. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 128 (describing difficulty enforcing privacy statutes); CATE, *supra* note 31, at 79 (noting enforcement is expensive, time consuming, and often ineffective); IITF OPTIONS, *supra* note 7, at 12 (relating criticism of federal data protection as "paper tiger" with significant enforcement deficiencies).

291. *See* The Freedom of Information Act, 5 U.S.C. § 552(f) (1994 & Supp. II

maintenance, and dissemination of personal information.[292] The Privacy Act permits a federal agency to maintain only personal information that is relevant and necessary to accomplish the agency's purpose.[293] Under the Privacy Act, a federal agency must maintain relevant, accurate, timely, and complete records of personal information.[294] The agency must also establish security and confidentiality safeguards for the records.[295] The Privacy Act prohibits dissemination of personal information unless the dissemination is compatible with the purpose for which the agency collected the information.[296] Further, the Privacy Act ensures transparency of agency records by requiring every federal agency to publish annually notices of its record system in the Federal Register.[297]

In addition, the Privacy Act provides data subjects with certain rights to protect personal information controlled by federal agencies.[298] These individuals possess a right of access to information about themselves[299] and the right to request that the

---

1996) (applying Privacy Act to U.S. executive departments, independent regulatory agencies, government corporations, and government controlled corporations). The Privacy Act does not extend to either Congress or federal, state, or local courts. SCHWARTZ & REIDENBERG, *supra* note 8, at 172.

292. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 94 (listing requirements of Privacy Act); Scott, *supra* note 65, at 491-96 (explaining Privacy Act in detail).

293. 5 U.S.C. § 552a(e)(1). Each agency should collect information from the data subject if possible. *Id.* § 552a(e)(2). Further, personal information may not be collected regarding the subject's exercise of First Amendment rights. *Id.* § 552a(e)(7).

294. The Privacy Act of 1974, 5 U.S.C. § 552a(e)(5) (1994).

295. *Id.* § 552a(e)(10).

296. *Id.* §§ 552a(a)(7) & (b)(3). Under the "routine use" exemption of the Privacy Act, an agency can use or disclose personal information for purposes compatible with the purpose for which the agency collected the information. *Id.* Privacy advocates criticize the routine use exemption because federal agencies have construed it broadly. *See* CATE, *supra* note 31, at 78 (noting criticism of routine use exception); SCHWARTZ & REIDENBERG, *supra* note 8, at 95-100 (discussing broad interpretation of routine use exception). The Privacy Act permits eleven other exceptions to the non-disclosure rule. 5 U.S.C. § 552a(b); *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 94 (noting broad scope of some exceptions weakens Privacy Act).

297. 5 U.S.C. § 552a(e)(4).

298. *Id.* § 552a(d), (g), (i); SCHWARTZ & REIDENBERG, *supra* note 8, at 115.

299. The Privacy Act of 1974, 5 U.S.C. § 552a(d)(1) (1994). This right of access is not absolute, as it is limited by the scope of the Privacy Act as well as the exemptions for the federal agencies. *See id.* § 552(f) (limiting Privacy Act to federal agencies); *id.* § 552a(k)(1) (exempting personal information gathered either in anticipation of litigation or by some law enforcement agencies such as CIA). Agencies also must respond to requests for personal information. *Id.* § 552a(e)(3).

agency amend incorrect information.[300] The data subjects also have a right to sue the government for violations of the Privacy Act.[301] They may not, however, obtain an injunction[302] to force the agency to change its practices.[303]

Although the Privacy Act provides protections for individuals against the government, the Privacy Act does have certain limitations.[304] Its scope is limited as it generally regulates only federal agencies[305] and applies only to their use of information about U.S. citizens or legal residents.[306] In addition, federal agencies have interpreted some of the exceptions to the Privacy Act rather broadly.[307] Further, although the Privacy Act sets forth comprehensive regulation of federal agencies, no centralized enforcement mechanism exists to oversee federal agencies' compliance with the Privacy Act's limits on their collection, maintenance, and dissemination of personal information.[308] Individual enforcement through lawsuits is generally ineffective because damages are difficult to prove and limited injunctive relief

300. *Id.* § 552a(f). If a federal agency denies a request to amend personal information, review of this decision is available. *Id.* § 552a(g)(1); ROBERT ELLIS SMITH, PRIVACY: HOW TO PROTECT WHAT'S LEFT OF IT 210 (1979).

301. 5 U.S.C. § 552a(d)(3) & (g). If a federal employee knowingly and willfully violates the Privacy Act, then he may be subject to criminal penalties. *Id.* § 552a(i).

302. DOUGLAS LAYCOCK, MODERN AMERICAN REMEDIES 231 (2d ed. 1994); SCHWARTZ & REIDENBERG, *supra* note 8, at 115.

303. SCHWARTZ & REIDENBERG, *supra* note 8, at 115; *see id.* at 115-18 (discussing limited injunctive remedy under Privacy Act).

304. *See, e.g., id.* at 94 (noting two weaknesses of Privacy Act); Scott, *supra* note 65, at 492 (relating limited scope of Privacy Act).

305. The Freedom of Information Act, 5 U.S.C. § 552(f) (1994 & Supp. II 1996); *see* Scott, *supra* note 65, at 492 (noting that Privacy Act applies to all executive departments, independent regulatory agencies, government corporations, and government controlled corporations). The Privacy Act does not apply to U.S. Congress, the U.S. government, the governments of U.S. territories and possessions, the District of Columbia, federal courts, or state governments. Scott, *supra* note 65, at 492.

306. 5 U.S.C. § 552a(a)(2); Gellman, *supra* note 14, at 164.

307. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 94 (discussing routine use exemption).

308. 5 U.S.C. § 552a(v); Gellman, *supra* note 14, at 164. The primary Senate bill provided for a Federal Privacy Board, but the House Bill did not. BENNETT, *supra* note 1, at 72-73. The Senate and House sponsors reached a compromise by transforming the Federal Privacy Board into the Privacy Protection Study Commission and giving oversight responsibility to the Office of Management and Budget ("OMB"). *Id.* at 73. This compromise gave the OMB the authority to issue guidelines on the Privacy Act and to review the Privacy Act's effectiveness, but the OMB did not take an active role in this process. Gellman, *supra* note 14, at 164.

is available.[309]

The U.S. Congress enacted the Computer Matching and Privacy Protection Act of 1988[310] ("Matching Act") as a reaction to extensive data matching[311] under the Privacy Act.[312] Amending the Privacy Act, the Matching Act regulates data matching of federal agencies.[313] The Matching Act does not significantly change the substantive rights laid out in the Privacy Act, but instead seeks to protect these rights by establishing a procedure for automated comparisons of federal databases.[314] For instance, the Matching Act requires that an agency conduct a cost/benefit analysis before matching[315] and notify matching subjects of possible denials or terminations of government benefits after matching occurs.[316] The Matching Act also requires each federal agency to establish a Data Integrity Board to review data matching.[317]

While the Privacy Act and the Matching Act are the primary federal statutes that protect informational privacy, other federal regulation supports them.[318] For example, although the Free-

309. Oversight of Privacy Act of 1974: Hearings Before a Subcomm. of the House Comm. on Gov't Operations, 98th Cong., 1st Sess. 225 (1983) (testimony of Ronald Plesser, former Counsel to Privacy Protection Study Commission); *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 115-18 (discussing difficulties in enforcing Privacy Act). Foreigners are unable to enforce the Privacy Act because the Privacy Act grants them no rights. *Id.* Even if the Privacy Act gave foreigners rights, enforcement would still be almost impossible because they would be compelled to bring a suit in the United States. *Id.*

310. The Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o)-(r), (u) (1994 & Supp. II 1996).

311. SCHWARTZ & REIDENBERG, *supra* note 8, at 100-01. Data matching involves electronic comparison of computerized files with other computerized files to find individuals included on more than one file. *Id.*; REGAN, *supra* note 3, at 86.

312. *See* IITF OPTIONS, *supra* note 7, at 9 (describing Matching Act); REGAN, *supra* note 3, at 90-99 (discussing legislative history of Matching Act). Although the Privacy Act restricts dissemination of personal information, the federal agencies were matching data, claiming that matching was permissible under the "routine use" exemption of the Act. SCHWARTZ & REIDENBERG, *supra* note 8, at 101. U.S. Congress enacted the Matching Act to address the overuse of this exemption. *Id.*

313. IITF OPTIONS, *supra* note 7, at 9.

314. *Id.* at 9-10; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 101 (explaining additional procedures under Matching Act).

315. The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o)(1)(B) & (u)(4)(A) (1994).

316. *Id.* § 552a(p).

317. *Id.* § 552a(u); *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 121-23 (noting weak oversight of Data Integrity Boards).

318. *See* CATE, *supra* note 31, at 78-79 (discussing other laws addressing specific

dom of Information Act[319] ("FOIA") provides citizens a right of access to federal agency records, it exempts records containing personal information.[320] The U.S. Supreme Court affirmed this exemption in *Department of Justice v. Reporters Committee for Freedom of the Press*,[321] holding that the FOIA did not require disclosure of personal information because such disclosure did not advance the purpose of the FOIA, for it did not involve disclosure of government conduct.[322] Other federal statutes regulate how specific agencies treat personal information.[323] For instance, the U.S. Census Bureau[324] may only use census records for agency purposes[325] and the Internal Revenue Service[326] may not disclose tax returns without authorization.[327]

Most U.S. states have no omnibus fair information practices to regulate the public sector.[328] Although a few state constitutions address informational privacy,[329] most, like the federal Constitution, do not.[330] More states have adopted data privacy laws regulating how their state government treats personal infor-

---

topics or federal agencies). For example, the Right to Financial Privacy Act of 1978 regulates when the federal government can gain access to financial records of individuals and small partnerships. 12 U.S.C. §§ 3401-22 (1994); *see* Scott, *supra* note 65, at 497-98 (discussing Right to Financial Privacy Act).

319. The Freedom of Information Act, 5 U.S.C. § 552 (1994 & Supp. II 1996), *amended by* 5 U.S.C.A. § 552 (West Supp. 1997).

320. *Id.* § 552(b)(6) & (7)(C); IITF OPTIONS, *supra* note 7, at 10. Two of the FOIA's nine exemptions protect privacy. *Id.* §§ 552(b)(6) & (7)(C); SCHWARTZ & REIDENBERG, *supra* note 8, at 109; CATE, *supra* note 31, at 77.

321. Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

322. *Reporters Comm.*, 489 U.S. at 773.

323. *See* IITF OPTIONS, *supra* note 7, at 11 (describing other more specific data privacy measures); CATE, *supra* note 31, at 78-79 (discussing other federal laws).

324. 13 U.S.C. § 2, 4 (1994). The U.S. Census Bureau is an agency within the U.S. Department of Commerce. *Id.* § 2. The Census Bureau is responsible for taking a census of U.S. population every ten years. BLACK'S LAW DICTIONARY, *supra* note 67, at 224.

325. 13 U.S.C. §§ 9, 214 (1994).

326. *See* BLACK'S LAW DICTIONARY, *supra* note 67, at 816 (explaining that Internal Revenue Service ("I.R.S.") is part of U.S. Department of the Treasury). The I.R.S. is responsible for administering and enforcing most of the internal revenue laws. *Id.*

327. I.R.C. § 6103, 7431 (1997), *amended by* I.R.C. § 6103 (West Supp. 1997).

328. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 130 (discussing state data privacy legislation).

329. *See* CATE, *supra* note 31, at 78-79 (stating that eight state constitutions explicitly protect personal data); SCHWARTZ & REIDENBERG, *supra* note 8, at 9 (noting that Arizona, California, and Illinois constitutions expressly protect privacy); *see, e.g.*, ARIZ. CONST., art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. 1, § 7; ILL. CONST. art. I, § 6.

330. SCHWARTZ & REIDENBERG, *supra* note 8, at 9.

mation.[331] In fact, many states have a strong tradition of disclosure of state government activities.[332] Such permissive disclosure provides access to the government, but it also may facilitate improper releases of personal information.[333]

While the U.S. Constitution, federal statutes, and state regulation provide significant data protection in the public sector, this regulatory system has certain gaps symptomatic of an ad hoc, sectoral model.[334] The Privacy Act provides relatively comprehensive regulation of the public sector, but does not apply to the private sector.[335] The Matching Act, responding to a specific privacy problem, targets only federal data matching.[336] Further, no oversight agency effectively regulates data protection.[337] The Office of Management and Budget, responsible for overseeing the implementation of the Privacy Act,[338] has focused on administrative tasks rather than data protection.[339] The Data Integrity Boards established under the Matching Act only apply to matching of databases, and each one only regulates the agency of which it is a part.[340]

---

331. *See id.* at 131 (stating that 13 states have omnibus data protection laws and more have narrow targeted statutes).

332. *See id.* at 208 (reviewing U.S. data protection at state level).

333. *Id.* at 208-09.

334. *See id.* at 213 (discussing need for creation of federal data protection commission to provide consistent regulation). For example, Congress enacted the Financial Right to Privacy Act in 1978 in response to a Supreme Court decision holding that the government could access bank account information. *Id.* at 262; *see* 12 U.S.C. §§ 3401-3422 (1994) (preventing government access to financial information without court order).

335. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 92 (relating Privacy Act's comprehensive regulation of public sector).

336. *Id.* at 101.

337. *See id.* at 114, 114-28 (discussing enforcement of U.S. data protection in public sector). An early version of the Privacy Act provided for the creation of a Federal Privacy Board. REGAN, *supra* note 3, at 77. In a compromise, legislators eliminated provision for such an oversight agency and established the PPSC, a temporary review committee. *See id.* at 81-82 (describing compromise bill that Congress enacted as Privacy Act).

338. The Privacy Act of 1974, 5 U.S.C. § 552a(v) (1994).

339. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 124-25 (explaining OMB's limited concern for data protection). Further, the OMB's requirement that federal agencies designate a "Privacy Act official" has not provided significant enforcement of the Privacy Act. *Id.* at 120.

340. 5 U.S.C. § 552a(u); *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 121-23 (explaining narrow role of Data Integrity Boards).

3. Private Sector

In comparison to U.S. regulation of the public sector, U.S. regulation of the private sector approaches data protection in an even more ad hoc, sectoral manner.[341] In the private sector, no constitutional protections govern how citizens treat another's personal information.[342] Regulation of the private sector is generally context specific and company or industry specific.[343] For instance, the U.S. Congress has enacted legislation to control how businesses treat personal data, but these statutes target personal data in a particular area, or subsector, of the private sector such as telecommunications or employment.[344] Likewise, when individual companies and entire industries adopt self-regulation, these fair information practices only pertain to those companies and industries.[345] Further, the regulation achieved in the private sector has predominantly been reactive to problems of informational privacy.[346] Both the federal and the state legislatures have generally not acted until privacy issues arose.[347] Similarly, companies and industries in the public sector have not adopted company privacy polices and industry codes unless they perceive that informational privacy has become a problem that they should address.[348]

U.S. data protection in the private sector regulates the treat-

341. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 215 (noting complexity of targeted data protection in private sector).

342. *See id.* at 9 (stating that "[n]o direct substantive constitutional basis exists for the protection of individuals in the private sector"). The absence of constitutional protections regarding informational privacy in the private sector results from the American philosophy that the U.S. Constitution generally protects individuals from the government rather than from one another. CATE, *supra* note 31, at 50.

343. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 215 (outlining data protection in U.S. private sector).

344. *See* CATE, *supra* note 31, at 80 (discussing federal privacy regulation in U.S. private sector).

345. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 216-17 (describing nature of self-regulation in U.S. private sector).

346. Reidenberg, *Obstacle Course*, *supra* note 94, at S148; *see* Reidenberg, *Fortress or Frontier*, *supra* note 17, at 208-09 (describing ad hoc approach at federal and state levels).

347. *See* Reidenberg, *Obstacle Course*, *supra* note 94, at S148-49 (discussing U.S. ad hoc approach). The classic example of this ad hoc approach is the Video Privacy Act. SCHWARTZ & REIDENBERG, *supra* note 8, at 10. U.S. Congress enacted Video Privacy Act in reaction to the publication of Robert Bork's video rental history during his U.S. Supreme Court nomination process. *Id.*

348. *See* Reidenberg, *Obstacle Course*, *supra* note 94, at S150 (explaining that industries and companies often adopt self-regulation to avoid legislative action).

ment of personal data in various subsectors to different degrees.[349] In telecommunications and credit reporting, U.S. federal statutes provide substantial protection.[350] Federal regulation of banking and employment is weak, but these subsectors undertake significant self-regulation.[351] Some areas such as health care and direct marketing, however, involve almost no regulation at all.[352]

a. Telecommunications

U.S. regulation of telecommunications protects personal information generally,[353] but a few aspects of telecommunications require self-regulation because the sectoral legislation leaves a few gaps.[354] For example, the Electronic Communications Protection Act of 1986[355] ("ECPA") regulates how businesses collect, use, and disclose the contents of communications.[356] By federal statute, it is illegal to collect the contents of real-time communications,[357] subject to a various exceptions.[358] Likewise, it is ille-

349. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 215-218 (discussing varied rules and policies in U.S. private sector).

350. *See id.* at 219-20, 265 (noting significant data protection in context of telecommunications and credit reporting).

351. *See* IITF OPTIONS, *supra* note 7, at 21 (discussing U.S. data protection in financial services sector); SCHWARTZ & REIDENBERG, *supra* note 8, at 350 (explaining U.S. data protection in workplace).

352. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 154, 308 (noting lack of U.S. legislation regarding medical records and direct marketing information).

353. *See id.* at 219-20 (discussing U.S. data protection in telecommunications sector).

354. *See* IITF OPTIONS, *supra* note 7, at 16 (summarizing U.S. telecommunications data protection); SCHWARTZ & REIDENBERG, *supra* note 8, at 223 (explaining that United States aims regulation at particular area of telecommunications rather than at particular function of telecommunications).

355. The Electronic Communications Protection Act, 18 U.S.C. §§ 2510-2511, 2701-2709 (1994), *amended by* 18 U.S.C.A. § 2510-2511, 2701-2709 (West Supp. 1997).

356. *Id.* §§ 2510-2511; *see* CATE, *supra* note 31, at 84 (noting that Electronic Communications Protection Act ("ECPA") prohibits collection and disclosure of electronic communications); SCHWARTZ & REIDENBERG, *supra* note 8, at 225 (stating that ECPA regulates collection and use of message content). Regulation of wire communications involves only public telecommunications networks, not private networks such as those operated within private companies. 18 U.S.C. § 2510(1); *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 226 (discussing limits of ECPA).

357. 18 U.S.C. § 2511. Real-time communications include oral, wire, and electronic communications that are received immediately, not stored. *See* IITF OPTIONS, *supra* note 7, at 12-13 (distinguishing between protections of real-time communications and stored communications).

358. 18 U.S.C. §§ 2510-11; *see* IITF OPTIONS, *supra* note 7, at 12 (listing frequently

gal intentionally to access from a storage facility the contents of stored communications[359] without authorization.[360] Individuals who breach the ECPA are subject to civil and criminal penalties.[361]

No comprehensive telecommunication laws, however, address the treatment of the records of communications.[362] These telecommunications-generated records, or transactional data,[363] often produce significant amounts of personal information that telecommunications companies can reuse for other purposes or sell to defer costs.[364] The ECPA prevents the government from gaining access to toll billing records[365] of electronic communications without obtaining judicial authorization.[366] Although the ECPA prevented disclosure to the government, telecommunica-

---

used exceptions). For example, the government may intercept real-time communications for law enforcement purposes. 18 U.S.C. § 2517. The ECPA also exempts employers if the communication occurs in their ordinary course of business. *Id.* § 2510(5)(a) & 2511(2)(a)(1). Further, the ECPA permits interception of communications if one party consents. *Id.* § 2511(2)(c)-(d).

359. *See* 18 U.S.C. § 2510(17) (West Supp. 1997) (defining stored communications as electronic communications that are in storage as by-product, or incidental feature, of transmission of message).

360. The Electronic Communications Protection Act, 18 U.S.C. § 2701 (1994). Further, the storage facility cannot disclose the contents of a stored communication unless an exception applies. *Id.* § 2702; *see* IITF OPTIONS, *supra* note 7, at 13 (noting exceptions to non-disclosure rule).

361. 18 U.S.C. § 2701; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 237, 257 (describing remedies for breach of ECPA).

362. *See* IITF OPTIONS, *supra* note 7, at 16 (noting that Telecommunications Act regulates some, but not all, transactional data).

363. *See* CATE, *supra* note 31, at 85 (defining transactional information as data about telecommunications transactions). This transactional data is sometimes referred to as customer proprietary network information ("CPNI"), or telecommunication-related personal information ("TRPI"). *See* IITF OPTIONS, *supra* note 7, at 14 (defining CPNI as information relating to quantity, type, destination, and amount of use of telecommunications services); NTIA REPORT, *supra* note 3, at 6 (describing how TRPI is collected). Transactional data is personal information created in the course of subscription to or use of a telecommunications service. NTIA REPORT, *supra* note 3, at 6. This data may include basic subscriber information, routing data, billing data, and records of electronic purchases. *Id.*

364. NTIA REPORT, *supra* note 3, at 7.

365. *See* IITF OPTIONS, *supra* note 7, at 13 (defining toll billing records to include records of what phone line caller used, what numbers caller telephoned, when, and for how long).

366. 18 U.S.C. § 2703 (c)(1)(C); IITF OPTIONS, *supra* note 7, at 14. In 1994, U.S. Congress passed the Communications Assistance for Law Enforcement Act ("CALEA"). Pub. L. No. 103-414, Title II, 108 Stat. 4290 (codified in scattered sections of 18 U.S.C. & 47 U.S.C.) (1994) (also known popularly as the Digital Telephony Bill). The CALEA supplemented the ECPA and raised the government's level of proof to obtain a court

tions companies still could collect, reuse, and even sell transactional data to private entities.[367] Recent regulation has addressed this informational privacy issue.[368] Most significantly, the Telecommunications Act of 1996[369] ("Telecommunications Act") imposed new limits upon how telecommunications carriers[370] use transactional information.[371] For instance, telecommunications carriers can use transactional data only to provide service.[372] The Telecommunications Act does not, however, regulate non-telecommunications carriers.[373]

Telecommunications providers have attempted to regulate themselves.[374] In October 1995, before the U.S. Congress enacted the Telecommunications Act, the National Telecommunications and Information Administration[375] ("NTIA") recommended that service providers adopt a system of provider notice and customer consent to protect transactional data.[376] Some service providers have adopted this approach.[377] In 1995, an indus-

---

order. *See* IITF OPTIONS, *supra* note 7, at 14 (describing how CALEA modified protection of transactional data).

367. 18 U.S.C. § 2703(c)(1)(A); IITF OPTIONS, *supra* note 7, at 14.

368. *See* IITF OPTIONS, *supra* note 7, at 14-15 (explaining effect of Telecommunications Act of 1996).

369. The Telecommunications Act of 1996, 47 U.S.C.A. § 222 (West Supp. 1997).

370. *See* 47 U.S.C. § 153(44) (defining telecommunications carrier as provider of telecommunications services).

371. *See* IITF OPTIONS, *supra* note 7, at 14 (discussing data protection under Telecommunications Act). Before the Telecommunications Act, no legislation regulated telecommunications providers' collection and use of transactional data. CATE, *supra* note 31, at 85; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 241 (describing federal law before Congress enacted Telecommunications Act). Even under the Telecommunications Act, non-telecommunications carriers are not subject to any statutory restrictions. IITF OPTIONS, *supra* note 7, at 16.

372. 47 U.S.C. § 222.

373. *See id.* (applying to telecommunications carriers only).

374. *See* IITF OPTIONS, *supra* note 7, at 15 (discussing self-regulatory efforts in telecommunications sector).

375. *See* NTIA REPORT, *supra* note 3, at 25 n.18 (describing National Telecommunications and Information Administration ("NTIA")). The NTIA, a part of the U.S. Department of Commerce, is responsible for developing telecommunications and information policies to advise the U.S. President. *Id.* NTIA also presents Executive Branch views on telecommunications to the U.S. Congress, the Federal Communication Commission, state and local governments, and the public. *Id.*

376. *See id.* at Introduction D & III (presenting NTIA's system of notice and consent). The NTIA has continued to investigate how the private sector can improve self-regulation since publishing its report, Privacy and the NII. FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, *supra* note 7, at 22 n.7.

377. *See, e.g.*, Ctr. For Democracy & Tech., *Privacy Policy Chart – Online Service Providers* (visited Feb. 14, 1998) <http://www.cdt.org/privacy/online_services/chart.html>

try group, the Interactive Services Association, issued guidelines on the disclosure of online transactional data similar to the NTIA's recommended system.[378] In many cases, the terms of the contract between service providers and customers govern the providers' use of transactional data.[379] Further, many telecommunications companies usually treat transactional data as confidential in the interests of both subscribers and business customers.[380] Thus, the industry has attempted to employ self-regulation to cover the gaps created by sectoral regulation of telecommunications.[381]

b. Financial Services

As in the telecommunications industry, legislation concerning the financial sector regulates the treatment of personal information only generally, leaving many privacy concerns unaddressed.[382] For example, the U.S. Congress has not regulated the treatment of personal data by banks and other private financial institutions.[383] Statutory measures have not been necessary to ensure information privacy in banking because banks and other financial institutions traditionally have protected the privacy of customer information.[384] New technology has challenged this tradition, so the financial services industry has begun

---

(also on file with the *Fordham International Law Journal*) (charting notice and consent policies of four major online service providers).

378. IITF OPTIONS, *supra* note 7, at 15-16. Several online service providers have adopted these guidelines. *Id.* at 16.

379. *Id.* at 16.

380. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 246-48 (describing confidentiality policies of various telecommunications companies). Business customers of service providers often prefer that providers keep subscriber transactional information confidential rather disclose such information to both themselves and their competitors. *Id.* at 246-47. These same providers, however, often reuse this transactional data for other purposes. *Id.* at 248.

381. *See* IITF OPTIONS, *supra* note 7, at 16 (summarizing privacy regulation of telecommunications sector).

382. Reidenberg, *Fortress or Frontier*, *supra* note 17, at 210.

383. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 262 (discussing U.S. regulation of bank records in private sector); IITF OPTIONS, *supra* note 7, at 21 (noting absence of privacy statutes in U.S. financial services sector). While U.S. private banks are highly regulated institutions, most federal banking regulation addresses insolvency and lending. H. JEFF SMITH, MANAGING PRIVACY – INFORMATION TECHNOLOGY AND CORPORATE AMERICA 22 (1994).

384. *See* IITF OPTIONS, *supra* note 7, at 20 (explaining traditional confidentiality on banking industry).

self-regulation.[385] While some industry groups have promulgated voluntary privacy guidelines,[386] individual financial institutions have adopted internal policies on the use and disclosure of personal data.[387]

In comparison, the credit reporting industry, the first sector of U.S. business subject to a data protection law,[388] receives substantial regulation.[389] This supervision is appropriate because the three main credit bureaus together maintain files on nearly ninety percent of American adults[390] and the content of these files often determines whether an individual can obtain credit.[391] In response to the growth of the credit reporting industry during the 1960s, the U.S. Congress passed the Fair Credit Reporting Act[392] ("FRCA") in 1970, the first modern U.S. data privacy law, to regulate the collection, use, and disclosure of credit information.[393]

The FCRA permits consumer reporting agencies to disclose credit information to businesses with a legitimate need for the information.[394] Under the FCRA, if someone such as a creditor or employer makes an adverse decision based on the report, then that decision-maker must notify the consumer of the use of

---

385. *See id.* at 21 (describing self-regulation efforts of U.S. banking sector).

386. SCHWARTZ & REIDENBERG, *supra* note 8, at 263; IITF OPTIONS, *supra* note 7, at 21. Consumers Bankers Association recently issued guidelines for its members. *Id.* at 51 n.186.

387. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 263 (noting American Express and Citicorp adopted company policies). For example, Citicorp promises its credit card users that it will use Visa and Master Charge information only in connection with Visa or MasterCard business. CITIBANK, CITIBANK VISA AND MASTERCARD PRIVACY POLICY (1993) (also on file with the *Fordham International Law Journal*).

388. The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998).

389. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 265 (noting regulation of reporting industry).

390. IITF OPTIONS, *supra* note 7, at 21.

391. *See id.* (explaining that creditors use credit reports to assess consumers ability to repay credit).

392. The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998).

393. *See* Gellman, *supra* note 14, at 140 (discussing FCRA).

394. *See* 15 U.S.C. § 1681b(a)(3) (specifying credit, insurance, employment, obtaining government benefits, and other legitimate needs). If no legitimate business need exists, the consumer reporting agency may still disseminate credit information with the consumer's consent or pursuant to a subpoena or court order. *Id.* § 1681b(a)(1) & (2). Disclosure must be conducted "in a manner that is fair to the consumer with respect to the confidentiality, accuracy, relevancy, and proper use of such information." *Id.* § 1681(b); IITF OPTIONS, *supra* note 7, at 22.

the report and identify the source of the report.[395] Further, various provisions of the FCRA regulate how reporting agencies use credit information to ensure that the data is complete and accurate.[396] Individuals can enforce the FCRA though private lawsuits[397] and the Federal Trade Commission has recently taken a more active role in supervising compliance with the FRCA.[398] Despite the various obligations the FCRA imposes upon credit agencies and users of credit reports, privacy advocates have criticized the FCRA for applying only to credit agencies[399] and for defining the permissible business purposes for disclosure too broadly.[400]

While industry self-regulation addressed many of the FCRA's deficiencies, the U.S. Congress finally amended the FCRA in 1996.[401] Responding to increased consumer criticism and U.S. congressional attention, the credit reporting industry changed some of its practices.[402] Industry groups began to promulgate fair information policies.[403] Credit reporting bureaus adopted voluntary privacy standards to improve accuracy and use of personal information.[404] Although these industry efforts were partially intended to avoid new legislation, the U.S. Con-

395. 15 U.S.C. § 1681m.

396. *Id.* §§ 1681c-k. For example, consumer reporting agencies must delete most adverse information about consumers after seven or ten years, depending on the type of information. *Id.* § 1681. Consumers have a right to access their files and the agencies must establish procedures to deal with disputes over credit information. *Id.* §§ 1681g-i.

397. *Id.* §§ 1681n(1)-(3), 1681o; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 304 (describing remedies for violations of fair credit reporting rights).

398. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 304-05 (discussing enforcement of U.S. data protection regulation in credit reporting industry).

399. *See, e.g.*, Reidenberg, *Fortress or Frontier*, *supra* note 17, at 210-11 (noting that FCRA applies only to credit reporting agencies).

400. *See* IITF OPTIONS, *supra* note 7, at 22 (discussing criticism of FCRA).

401. *See id.* at 22-23 (discussing self-regulation of U.S. credit reporting and 1996 amendments to FRCA).

402. *See id.* (describing self-regulatory efforts of credit reporting industry).

403. *See, e.g.*, Senate Comm. on Banking, Housing, and Urban Affairs, The Consumer Reporting Act of 1994, S. Rep. No. 209, 103d Cong., 1st Sess. 37-38 (1993) (statement of Senators Shelby and Domenici) (touting 20 new credit reporting industry policies). For example, the Associated Credit Bureaus adopted mandatory information policies. IITF OPTIONS, *supra* note 7, at 22; Barry Connelley, *Credit Bureaus Adopt Initiatives in the Absence of a New Law*, CREDIT WORLD, July/Aug. 1993, at 7.

404. *See* IITF OPTIONS, *supra* note 7, at 23 (noting that Experian and Equifax, two of three leading credit reporting bureaus, adopted new codes of fair information practices). For instance, Experian, formerly TRW, published a set of "Fair Information Values." Gellman, *supra* note 14, at 143-44.

gress adopted sweeping changes for the FCRA in 1996.[405] These amendments included provisions imposing new accuracy obligations for creditors reporting to credit bureaus and new reinvestigation and notice obligations for credit bureaus.[406]

c. Employment

Legislation and business practices regulate the treatment of employee information in the workplace through a patchwork of data protection measures.[407] While federal and state statutes address the treatment of private sector employees' personal information, these statutes generally target specific employment practices.[408] Business practices often supplement this federal and state legislation.[409]

Various federal laws protect employee information in specific contexts.[410] For example, the FCRA[411] protects personal information when an employer decides not to hire an individual based upon a requested credit report.[412] The FCRA requires that the employer notify the individual of the report that it received and the name of the credit reporting agency and that the agency reveal the content of the report if requested.[413] The Om-

405. Omnibus Consolidated Appropriations Act, Pub. L. No. 104-208, div. A, tit. II, 110 Stat. 3009 (1996); *see* IITF OPTIONS, *supra* note 7, at 23 (discussing amendments to FCRA).

406. IITF OPTIONS, *supra* note 7, at 23.

407. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 524 (noting that legal rules, industry norms, business practice, and computer system architecture all protect employee personal information); SCHWARTZ & REIDENBERG, *supra* note 8, at 349-77 (analyzing various levels of U.S. data protection in workplace).

408. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 350 (outlining regulation of information practices in workplace). No comprehensive federal legislation regulates how employers treat workers' personal data. *Id.*

409. *Id.*

410. *See* CATE, *supra* note 31, at 80 (noting relatively little data protection of employment issues given extensive regulation of workplace); SCHWARTZ & REIDENBERG, *supra* note 8, at 349-77 (discussing federal laws regulating employment sector); Reidenberg, *Setting Standards*, *supra* note 53, at 524-28 (citing various federal legal rules governing treatment of personnel records); Pincus & Trotter, *supra* note 42, at 66-69 (reviewing current federal statutory protection of private sector employee information).

411. The Fair Credit Reporting Act, 15 U.S.C. §§§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998).

412. 15 U.S.C. §§ 1681a(k)(1)(B) & m(a); *see* Pincus & Trotter, *supra* note 42, at 66-67 (discussing FCRA's protection of employee information).

413. 15 U.S.C. § 1681g(a)(1) & (3). The individual requesting the credit report may also request that the credit reporting agency reinvestigate allegedly inaccurate information and correct the report if necessary. *Id.* § 1681i(a).

nibus Crime Control and Safe Streets Act[414] and the ECPA protect employee information in a specific context by prohibiting the collection and use of wire, oral, and electronic communications.[415] Other federal laws protect the treatment of specific types of employee information such as medical information,[416] payroll information,[417] equal employment opportunity information,[418] and information regarding union activity.[419] Further, while many state data privacy laws supplement federal legislation, these state laws also target particular types of employee information.[420]

Companies often institute fair information policies for employee information.[421] For instance, many businesses implement security programs[422] and provide employees access to their personnel records.[423] Companies frequently limit their collection of extraneous employee data to avoid claims of discrimination in the workplace.[424] These business practices are, however, rarely

414. 18 U.S.C. §§ 2510-2520 (1994), *amended by* 18 U.S.C.A. §§ 2510-2520 (West Supp. 1997); REGAN, *supra* note 3, at 6.

415. 18 U.S.C. §§ 2510-2511; *see* Pincus & Trotter, *supra* note 42, at 67 (discussing Omnibus Crime Control and Safe Street Act's protection of employee communications and exemptions under statute).

416. *See* 42 U.S.C. § 12112(d) (1994) (prohibiting collection of applicant's medical information when not specifically related to job performance); Occupational Safety and Health Act, 29 U.S.C. § 657 (1994) (requiring maintenance of certain employee medical records to monitor and evaluate job safety and health).

417. *See* Labor Management and Standards Act, 29 U.S.C. § 211(c) (1994) (prescribing payroll information that employers must collect).

418. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 364 (explaining that federal law often requires collection of sensitive data regarding job applicant's sex, race, ethnicity, or handicap, but restricts employer's use of such information).

419. *See* 29 U.S.C. § 158 (1994) (restricting collection of information about employee's union activity); 42 U.S.C. §§ 2000e, 2000e-2(a) (1994) (prohibiting discrimination in hiring, firing, or fixing terms of employment on basis of race, color, religion, sex, or national origin).

420. SCHWARTZ & REIDENBERG, *supra* note 8, at 350; *see* Reidenberg, *Setting Standards*, *supra* note 53, at 524-25 nn.149-52 (citing various state laws that regulate information practices directly or indirectly).

421. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 350, 350-77 (discussing company practices regarding treatment of employee information).

422. *See id.* at 360 (noting that many companies address security issues).

423. Reidenberg, *Setting Standards*, *supra* note 53, at 525; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 359 (noting that 87% of major U.S. companies give employees access to personnel files). Further, many businesses permit employees to amend incorrect records. SCHWARTZ & REIDENBERG, *supra* note 8, at 359-60.

424. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 354 (explaining company interest in specifying purposes for collection of employee information).

transparent[425] and not enforceable.[426]

d. Medical records

In the private health care subsector, protection of medical records is inadequate, inconsistent, and incomplete.[427] Like banking, even though no general federal statute regulates fair information practices in the health care industry,[428] traditional doctor-patient confidentiality prevented disclosure of sensitive personal information.[429] Recent developments in the health care sector, however, have jeopardized the informational privacy of patients.[430] Health care providers are now able to store massive amounts of medical information.[431] In addition, third par-

---

425. *See id.* at 361-62 (describing lack of transparency regarding how companies treat employee information).

426. *See id.* at 365-66 (discussing enforcement of data protection measures in U.S. employment sector).

427. *See* Gellman, *supra* note 14, at 137 (noting one reason for incompleteness is that Privacy Act covers only government's treatment of medical records); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 6-7 (1997) [hereinafter Schwartz, *Economic Health Care*] (noting significant agreement about insufficiency of current medical data protection in United States).

428. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 176-79 (noting narrow federal regulation protects medical information in private sector in strictly limited circumstances). For instance, anti-discrimination laws like the Americans with Disabilities Act ("ADA") and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulate specific aspects of health care data. 42 U.S.C. §§ 12101-12213 (1994) (protecting disabled individuals from employment discrimination); Pub. L. No. 104-191, 110 Stat. 1936 (1996) (regulating denials or discontinuances of health care coverage based on medical status); *see* Schwartz, *Economic Health Care*, *supra* note 427, at 39-41 (describing narrow protections of ADA and HIPAA).

429. IITF OPTIONS, *supra* note 7, at 17; *see* Gellman, *supra* note 14, at 138 (stating that "[u]ntil sometime in the second half of the twentieth century, the patchwork quilt of health record confidentiality rules was not perceived to be a significant problem."); Schwartz, *Economic Health Care*, *supra* note 427, at 13-14 (contrasting traditional deference to medical profession with modern control of doctors through processing and use of personal information).

430. IITF OPTIONS, *supra* note 7, at 17. Although new developments in medical information technology will cut costs and reduce delays, these advances are potentially harmful because health records often contain very personal information. *Id.*; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 157-59 (explaining that health care reform is likely to increase sharing of medical information).

431. IITF OPTIONS, *supra* note 7, at 17. The Medical Information Bureau, a nonprofit trade organization, maintains health records on 15 million Americans for 600 member insurance companies. *See* Jay Greene, *Your Medical Records – Perhaps Your Most Personal Information – Also are the Most Vulnerable to Public Scrutiny*, ORANGE COUNTY REG. (California), April 24, 1996, at C01, *available in* 1996 WL 7023964 (discussing increased storage of medical data and large number of inaccurate records); *see also* Schwartz,

ties not involved with patient care[432] frequently demand access to this medical information.[433] Moreover, these technology and market pressures are eroding the traditional doctor-patient confidentiality.[434]

In the absence of any comprehensive federal legislation regulating the treatment of medical records,[435] states and the health-care industry have attempted to protect personal medical information.[436] Unfortunately, the states and the industry are not in the position to adopt comprehensive, mandatory standards.[437] Many states have health-care confidentiality statutes, but these state laws cannot regulate the interstate use, maintenance, and disclosure of health information.[438] Likewise, while the voluntary privacy codes and new security measures adopted by health organizations and companies are laudable,[439] they pro-

---

Health Care Reform, *supra* note 39, at 300-06 (describing increased role of data protection in health care).

432. *See* IITF OPTIONS, *supra* 7, at 17 (noting that third parties not involved with patient care include employers, government agencies, credit bureaus, insurers, educational institutions, and the media).

433. *See id.* at 17 (discussing increased demands by third parties for medical information); Gellman, *supra* note 14, at 138 n.38 (noting that third parties pay most personal health bills for most people).

434. *See* IITF OPTIONS, *supra* note 7, at 18 (discussing pressures on doctor-patient confidentiality); Gellman, *supra* note 14, at 137 n.36 (explaining inadequacy of ethical rules that define confidentiality and noting rules do not apply to computer operators and health insurance companies).

435. Schwartz, *Health Care Reform*, *supra* note 39, at 315; IITF OPTIONS, *supra* note 7, at 18. Legislators have introduced several federal health records bills, but the U.S. Congress has not enacted any such measures. *See* IITF OPTIONS, *supra* note 7, at 18 & n.161 (citing recent proposals for increased protection of medical records).

436. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 179 (noting that states have adopted many different kinds of data protection measures). For example, states often recognize a confidential doctor-patient relationship. *Id.* at 180. State common law also sometimes protects personal data. *See id.* at 180-81 (examining protection of tort right against public disclosure).

437. *See id.* at 179-84 (relating deficiencies of state medical record data protection). "The interstate flow of medical information calls for a federal response to these issues of data protection." *Id.* at 183.

438. *See* Gellman, *supra* note 14, at 138-39 (noting development of health care as interstate business); SCHWARTZ & REIDENBERG, *supra* note 8, at 166 (stating that "[i]n an age of prevalent interstate data transfers, this lack of uniformity is itself an additional weakness in American medical data protection."); IITF OPTIONS, *supra* note 7, at 18 (recognizing emerging consensus that state laws can no longer protect medical data).

439. *See* IITF OPTIONS, *supra* note 7, at 17-18 (describing various self-regulation attempts by health care sector). For example, the American Health Information Management Association ("AHIMA") supports legislation protecting the confidentiality of medical records. *Id.* at 18; *AHIMA's Role in Health Information Confidentiality Issue* (visited

vide minimal data protection.[440]

e. Direct Marketing

The direct marketing industry is the least regulated sector even though this subsector deals with large volumes of personal information.[441] New technologies in information processing have significantly aided direct marketing businesses by improving how they exchange and process personal data.[442] The creation and use of name lists, however, implicate information privacy concerns.[443] For example, direct marketers can predict consumer behavior by cross-referencing various lists and compiling profiles from personal information.[444] Not only does profil-

---

Feb. 14, 1998) <http://www.ahima.org/media/press.releases/history.html> (also on file with the *Fordham International Law Journal*) (describing AHIMA as association of 35,000 professionals who capture, record, and analyze patient medical data). The Physician Computer Network, Inc. has developed internal security measures to protect personal information used in their new software that link physicians to insurance companies, clinical laboratories, and hospitals. IITF OPTIONS, *supra* note 7, at 17; *Medicine: No Restrictions on Drug Data*, L.A. TIMES, May 18, 1994, at A12.

440. *See* IITF OPTIONS, *supra* note 7, at 18 (explaining narrow scope of self-regulation, lack of enforcement powers, and limited adoption of self-regulation provide only minimal protection).

441. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 308 (contrasting lack of any sectoral law targeting direct marketing with sectoral laws in telecommunications and financial services); IITF OPTIONS, *supra* note 7, at 25 (describing proliferation of databases and consumer lists). For instance, the direct marketing industry contributed about US$75 billion to the gross national product of United States. CAVOUKIAN & TAPSCOTT, *supra* note 3, at 91.

442. *See* IITF OPTIONS, *supra* note 7, at 24 (describing advantages of new technology for direct marketing industry). Extensive databases and new technology such as caller identification and automatic number identification ("ANI") allow businesses to compile and store consumer lists, but this, in itself, does not implicate privacy concerns. Reidenberg, *Setting Standards*, *supra* note 53, at 517 n.93.

443. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 308-11 (discussing how international direct marketing involves processing of detailed demographic information and intimate personal data); CAVOUKIAN & TAPSCOTT, *supra* note 3, at 90 (noting that faster computers have allowed direct marketers to develop specific direct marketing techniques). For example, Mandev List Services offer lists that include European subscribers to Time Magazine, buyers of nightgowns, and women who buy certain beauty products. SCHWARTZ & REIDENBERG, *supra* note 8, at 308.

444. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 312-14 (discussing how direct marketers profile personal data); CAVOUKIAN & TAPSCOTT, *supra* note 3, at 55-56 (explaining how profiles are used). Businesses in direct marketing use Internet trails, transactional data from other purchases or communications, subscriber information, and public records to compile such profiles. *Id.* Direct marketers use profiles to create lists of potential consumers with specific characteristics. *Id.* at 14. For example, direct marketing catalogs advertise lists of women who wear wigs and of impotent middle-aged men. SCHWARTZ & REIDENBERG, *supra* note 8, at 321-22.

ing reveal personal information, but it also permits businesses to limit both the information and offers that an individual receives.[445]

Despite the threat to informational privacy that direct marketing poses, almost no sectoral laws target direct marketing.[446] Direct marketers have no duty to notify consumers of the collection of marketing data and virtually no law prohibits the secondary use of such data.[447] While the Federal Trade Commission[448] ("FTC") has become actively involved in consumer privacy issues, it has limited itself to educating consumers and businesses about the use of personal information online[449] and holding workshops to study consumer privacy issues.[450]

The direct marketing industry has tried to compensate for this lack of formal regulation by setting industry standards.[451] The Direct Marketing Association[452] ("DMA"), the largest direct marketing trade association in the United States, has adopted an

---

445. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 536-17 (explaining that new information technology can lead to imbalance of political power and manipulation of citizens).

446. Reidenberg, *Setting Standards*, *supra* note 53, at 517; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 315 (noting that cable television and video rental laws indirectly limit direct marketing).

447. IITF OPTIONS, *supra* note 7, at 25; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 317 (noting limits only on use of transactional data for cable television and video rentals).

448. *See* BLACK'S LAW DICTIONARY, *supra* note 67, at 614 (describing Federal Trade Commission as federal agency created in 1914 responsible for "promot[ing] free and fair competition in interstate commerce through prevention of general trade restraints").

449. *See* IITF OPTIONS, *supra* note 7, at 26 (describing efforts of Federal Trade Commission ("FTC") to educate private sector). In 1995, the FTC's Bureau of Consumer Protection began a Consumer Privacy Initiative to educate consumers and businesses. *Id.*

450. Federal Trade Commission, *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (1996) *available on* Federal Trade Commission Home Page, *Workshop on Consumer Privacy on the Global Information Infrastructure* (visited Oct. 24, 1997) <http://www.ftc.gov/bcp/privacy/privacy1.htm> (also on file with the *Fordham International Law Journal*). The FTC's Staff Report concluded that workshop participants agreed upon certain necessary elements of fair information practices online; notice, consumer choice, data security, and consumer access. *Id.* at 3-4.

451. Reidenberg, *Setting Standards*, *supra* note 53, at 518; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 309 (noting that "industry ardently promotes self-regulation").

452. IITF OPTIONS, *supra* note 7, at 54 n.237. The Direct Marketing Association ("DMA") is a direct marketing trade association composed of approximately 3,500 manufacturers, wholesalers, and retailers. *Id.*

ethical code and set voluntary, self-regulatory standards.[453] The DMA can suspend membership in the organization for violations of the code and recommends that companies adopt their own information policies.[454] Nonetheless, these industry and business policies are permissive[455] and often are ignored.[456] Although industry organizations and individual companies seek to improve data protection, enforcement of these standards will continue to be difficult because the information is so valuable[457] and the standards are voluntary.[458]

II. *DIFFERENT APPROACHES TO ASSESSING ADEQUACY OF DATA PROTECTION*

The Directive requires that Member States prevent transfers of personal data to countries outside the Community that do not ensure adequate data protection.[459] Whether the Directive will prohibit certain data transfers to the United States depends, in part, upon what constitutes an adequate level of protection.[460] While the Directive notes that adequacy should be assessed in light of all the circumstances surrounding the transfer, it does not elaborate upon this standard.[461]

Which data protection measures will qualify as adequate

---

453. *See id.* at 25 (discussing direct marketing efforts at self-regulation). The DMA has issued "Guidelines for Personal Information Protection" and a *Manual for Fair Information Practices.* SCHWARTZ & REIDENBERG, *supra* note 8, at 309.

454. IITF OPTIONS, *supra* note 7, at 25. DMA also sponsors services to allow consumers to decrease the amount of unsolicited mail and telemarketing that they receive. *Id.*

455. *See* SCHWARTZ & REIDENBERG, *supra* note 8, at 316 (explaining that DMA guidelines permit direct marketers to collect personal data for any "direct marketing purpose").

456. *See id.* at 309-10 (citing examples of direct marketing companies ignoring self-regulation).

457. CAVOUKIAN & TAPSCOTT, *supra* note 3, at 96.

458. IITF OPTIONS, *supra* note 7, at 25; *see* SCHWARTZ & REIDENBERG, *supra* note 8, at 338 (noting industry and company codes offer no remedies to individuals).

459. *See* Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45-46 (1995) (setting forth standard for transfers to third countries).

460. *See id.* art. 25(4), O.J. L 281/31, at 46 (1995) (requiring Member States to prevent data transfers to third country where Commission finds that third country does not ensure adequate protection). Whether these transfers will be prevented also depends upon whether the derogations from Article 26 will exempt the transfer in question. *See id.* art. 26, O.J. L 281/31, at 46 (1995) (giving exceptions to Article 25).

461. *See id.* art 25(2), O.J. L 281/31, at 45-46 (1995) (setting forth factors to be used to determine whether third country's protection is adequate, but not explaining how to apply these factors).

protection has not been established.[462] Earlier approaches to data protection do not explain the Directive's standard of adequacy.[463] The Directive itself sets forth the surrounding circumstances by which adequacy should be judged, but the Directive does not explain how these factors should be applied to specific transfers.[464] To clarify what constitutes an adequate level of protection, the Article 29 Working Party adopted a discussion document analyzing possible ways to assess adequacy.[465]

A. *Adequate Protection Before the Directive*

No explanation of adequate protection precedes the Directive in either earlier data protection measures or prior drafts of the Directive.[466] Earlier data protection measures establish a standard of equivalency,[467] not adequacy.[468] Neither the OECD Guidelines nor the COE Convention indicate what constitutes adequate protection because neither set forth an adequacy standard for transfers of data to third countries.[469] Likewise, the na-

462. *See* Gellman, *supra* note 14, at 157 (relating uncertainty about how Article 25 will be interpreted and applied).

463. *See, e.g.*, COE Convention, *supra* note 121, art. 12, at 320 (using equivalency standard); Original Proposal, *supra* note 145, art. 24, O.J. C 277/03, at 10 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990) (proposing adequacy standard be judged by overall country assessment).

464. *See* Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45-46 (1995) (listing, but not explaining, surrounding circumstances).

465. *See* First Orientations, *supra* note 48 (focusing on central question of assessing adequacy).

466. *See* OECD Guidelines, *supra* note 127, pt. 3, art. 17, at 426 (employing equivalency standard); COE Convention, *supra* note 121, art. 12, at 320-21 (adopting equivalency standard); Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 474-77 (noting that European national data protection laws use equivalency standard); Original Proposal, *supra* note 145, art. 24, O.J. C 277/03, at 10 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990) (proposing standard of adequacy that employs overall country assessment instead of Directive's case-by-case analysis); Amended Proposal, *supra* note 145, art. 26, O.J. C 311/04, at 55-56 (1992), COM (92) 422 Final-SYN 287, at 104-07 (1992) (detailing same adequacy standard as Directive, but providing no explanation); Common Position, *supra* note 145, art. 25, O.J. L 93/1, at 14 (1995) (setting forth identical text on transfers to third countries as Directive).

467. *See* Schwartz, *Restrictions on Internal Data Flows*, *supra* note 17, at 473 (identifying equivalency standard with data protection laws that require equivalent level of protection before data transfer).

468. OECD Guidelines, *supra* note 127, pt. 3, art. 17, at 426 (employing equivalency standard); COE Convention, *supra* note 121, art. 12, at 320-21 (adopting equivalency standard); Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 474-77 (noting that European national data protection laws use equivalency standard).

469. *See* OECD Guidelines, *supra* note 127, pt. 3, arts. 16-18, at 426 (allowing re-

tional legislation of most European countries establish a standard of equivalency, not of adequacy.[470]

Similarly, prior drafts of the Directive do not clarify Article 25's adequacy standard.[471] Although the Original Proposal required that a third country ensure adequate data protection,[472] that initial draft envisaged a more restrictive approach to adequacy than the Directive now contains.[473] The Original Proposal contemplated blacklisting[474] countries with inadequate protection, preventing all transfers to these countries after an overall country assessment.[475] Consequently, the Original Proposal's approach to assessing adequacy does not reflect the Directive's

---

strictions of data transfers to third countries that do not provide equivalent protection); COE Convention, *supra* note 121, art. 12, at 320-21 (permitting restrictions of data transfers to another signatory party where other party does not provide equivalent protection). Although the COE Convention did not explicitly discuss data transfers to third countries, the COE Convention has been interpreted as requiring equivalent protection of personal data in third countries. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 478 (explaining that third countries like United States are subject to COE Convention equivalency standard). The COE Convention, however, does not mention adequate protection of personal data. *See* COE Convention, *supra* note 121, art. 12, at 320-21 (setting forth provisions on transfers of data across national borders).

470. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 474-77 (examining equivalency standard in European countries such as Belgium, Denmark, France, Germany, the Netherlands, Portugal, Spain, and the United Kingdom). For example, Portugal and Spain explicitly establish an equivalency standard. *Id.* at 474. Various other European countries such as Belgium, France, Denmark, and the United Kingdom have adopted laws that implicitly require equivalent data protection. *Id.* at 474-75.

471. Original Proposal, *supra* note 145, art. 24, O.J. C 277/03, at 10 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990); Amended Proposal, *supra* note 145, art. 26, O.J. C 311/04, at 55-56 (1992), COM (92) 422 Final-SYN 287, at 104-07 (1992); Common Position, *supra* note 145, art. 25, O.J. L 93/1, at 14 (1995).

472. *See* Original Proposal, *supra* note 145, art. 24(1), O.J. C 277/03, at 10 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990) (setting forth adequacy standard).

473. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 542-43 (suggesting that Common Position contains less restrictive provision on third country transfers); Common Position, *supra* note 145, art. 25, O.J. L 93/1, at 14 (1995) (setting forth standard of adequacy eventually included in Directive).

474. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 542 (discussing blacklisting of third countries with inadequate data protection). Blacklisting a third country involves restricting all data transfers because of inadequate protection. *See* Reidenberg, *Rules of the Road*, *supra* note 204, at 294 (noting that in contrast to Original Proposal, Amended Proposal did not provide for blanket restrictions).

475. *See* Original Proposal, *supra* note 145, art. 24, O.J. C 277/01, at 10 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990) (setting forth adequacy standard that entailed overall country assessment); Reidenberg, *Setting Standards*, *supra* note 53, at 542 (explaining adequacy standard of Original Proposal).

case-by-case approach.[476]

Although the Amended Proposal and the Common Position adopted a case-by-case approach to assessing adequacy, these two drafts provide no greater explanation of how to assess adequacy than the Directive.[477] The Amended Proposal's provision on adequacy explains what constitutes adequate protection the same way as the Directive.[478] The Common Position uses the identical words as the Directive.[479]

B. *Adequacy According to the Text of the Directive*

While the Directive potentially restricts international trade and may disrupt EU-U.S. relations, Article 25 does not explain what constitutes an adequate level of protection.[480] Recognizing the necessity of data transfers to third countries, Article 25(2) strives to balance the free flow of information against informational privacy by assessing adequacy in the context of the circumstances surrounding each transfer.[481] Although each of these surrounding circumstances will affect whether a third country affords adequate protection, the Directive only lists these circumstances.[482]

Commentators recognize several problems with Article 25(2)'s contextual analysis of a third country's data protection.[483] Scholars point out that a case-by-case analysis of all of

476. *Compare* Original Proposal, *supra* note 145, art. 24, O.J. C 277/03, at 10 (1990), COM (90) 314 Final-SYN 287, at 65-66 (1990) (setting forth overall country assessment) *with* Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45-46 (1995) (setting forth case-by-case analysis of data transfers).

477. *See* Amended Proposal, *supra* note 145, art. 26(2), O.J. C 311/04, at 55 (1992), COM (92) 422 Final-SYN 287, at 106 (1992) (introducing clause requiring adequacy of protection to be assessed in light of circumstances surrounding each data transfer or set of transfers); Common Position, *supra* note 145, art. 25(2), O.J. L 93/1, at 14 (1995) (retaining clause providing for analysis of third countries in light of circumstances).

478. *Compare* Amended Proposal, *supra* note 145, art. 26(2), O.J. C 311/04, at 55 (1992), COM (92) 422 Final-SYN 287, at 106 (1992) *with* Directive, *supra* note 4, art. 25(2), O.J. L 281/31, at 45-46 (1995).

479. *Compare* Common Position, *supra* note 145, art. 25(2), O.J. L 93/1, at 14 (1995) *with* Directive, *supra* note 4, art. 25(2), O.J. L 281/31, at 45-46 (1995).

480. Directive, *supra* note 4, art. 25, O.J. L 281/31, at 45-46 (1995).

481. *Id.* recitals paras. 56-57, O.J. L 281/31, at 36-37 (1995).

482. *See id.* art. 25(2), O.J. L 281/31, at 45-46 (listing circumstances by which adequate protection must be assessed, but not explaining how to use these circumstances).

483. *See* Boehmer & Palmer, *supra* note 39, at 294 (discussing cumbersome case-by-

the surrounding circumstances can be cumbersome.[484] For example, if a corporate branch in a Member State wants to transfer employee records to different branches in the United States, then this transfer would require a complex analysis of not only the U.S. federal regulation and the corporation's business practices,[485] but also the laws of each state where the branches were located.[486] Another commentator poses a problem with Article 25(2)'s requirement that professional rules be taken into account.[487] Although these business practices, whether industry-wide or company-specific, contribute significantly to the protection of personal data, they are rarely either binding or transparent.[488] Thus, business practices are unclear indicators of whether a third country adequately protects personal data.[489]

The Article 29 Working Party plays a significant role in determining what constitutes adequate protection.[490] Under the Directive, the Working Party's involvement in the decision-making process is, however, much less direct than that of the Member States, the Commission, or the Article 31 Committee.[491] The Working Party has no explicit role in making decisions about particular data transfers.[492] The group's work can provide gui-

---

case analysis); Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 485-86 (explaining that business practices are difficult data protection measures to assess).

484. Boehmer & Palmer, *supra* note 39, at 294.

485. *See* Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 486 (noting that professional rules mentioned in Article 25(2) include business practices of single company or of entire industry).

486. *See* Boehmer & Palmer, *supra* note 39, at 294 (noting that assessment of adequacy might be different for each state); Directive, *supra*, note 4, art. 25(2), O.J. L 281/31, at 45-46 (1995) (requiring analysis of general and sectoral laws as well as professional rules).

487. Schwartz, *Restrictions on International Data Flows*, *supra* note 17, at 485-86.

488. *See id.* (noting that "companies sometimes refuse to share information regarding their professional standards, which are, moreover, generally subject to unilateral change.").

489. *See id.* (explaining that some scholars assert that business practices should not be considered independently when assessing adequacy).

490. *See* Directive, *supra* note 4, art. 30, O.J. L 281/31, at 48-49 (1995) (providing that Working Party must give opinions on level of protection in third countries and report annually on data protection in third countries).

491. *See* First Orientations, *supra* note 48, at 2 (noting that decisions about particular data transfers are "carried out by the Member States in the first instance, and then the Commission under the Comitology procedure laid down in Article 31").

492. *Compare* Directive, *supra* note 4, art. 30, O.J. L 281/31, at 48-49 (1995) (providing Working Party with authority to give opinions on level of protection, but not to make decisions about specific transfers) *with id.* arts. 25 & 31, O.J. L 281/31, at 45-46,

dance, nonetheless, on how to assess adequacy in general.[493] Further, pursuant to Article 30(1)(b), the Working Party can submit to the Commission opinions on the adequacy of protection in third countries after examining some individual cases.[494] Thus, the Working Party's other work may have greater influence than mere guidance because the Member States might recognize that work as an indication of future opinions.[495]

The Working Party's positions on adequacy are influential because under the Directive, each Member State's supervisory authority designates representatives to serve as the members of the Working Party.[496] Further, these representatives are experts in the field on data protection.[497] The Working Party's positions on adequacy may also influence the Member States because the members of the Working Party formulate these positions as the representatives of the Member States.[498]

C. *Article 29 Working Party's Approach to Assessing Adequacy*

In June 1997, the Article 29 Working Party adopted a discussion document examining possible ways to assess adequacy of third country data protection.[499] The document, First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy[500] ("First Orientations"),

---

49 (setting forth roles of Member States, Commission, and Article 31 Committee with regard to determining whether third country's data protection is adequate).

493. *See* First Orientations, *supra* note 48, at 2 (explaining that Working Party's work is "intended to provide guidance regarding a broad mass of cases").

494. Directive, *supra* note 4, art. 30(1)(b), O.J. L 281/31, at 48 (1995); First Orientations, *supra* note 48, at 2-3.

495. *See* Directive, *supra* note 4, art. 30(1)(b), O.J. L 281/31, at 48 (1995) (setting forth Working Party's power to give opinions on adequacy of protection in third countries).

496. *See id.* art. 29(2), O.J. L 281/31, at 48 (1995) (describing composition of Article 29 Working Party).

497. *See* First Annual Report, *supra* note 225, at 22-25 (listing representatives of Working Party and their positions in national supervisory authorities).

498. *See* Directive, *supra* note 4, at 29(2), O.J. L 281/31, at 48 (1995) (stating that representatives of Member State supervisory authorities shall compose Working Party). Even if a Member State's Working Party representative disagrees with the majority of the Working Party, the Member State is likely to follow the Working Party's position on adequacy, as this position constitutes the position of the majority of the national supervisory authorities. *See id.* art. 29(2) & (3), O.J. L 281/31, at 48 (1995) (noting that Working Party makes decisions by majority of representatives of supervisory authorities).

499. First Orientations, *supra* note 48.

500. *Id.*

functions as a white paper,[501] presenting the evolving doctrine of the Working Party.[502] This paper is significant, nonetheless, because the Working Party suggests an approach to assessing the level of protection afforded by third countries.[503] The group suggests that adequacy should be assessed on a case-by-case basis, evaluating both the content of the third country's data protection rules and that country's procedural mechanisms for ensuring that the rules are effective.[504]

1. Procedure to Assess Adequacy

In the first section of the Working Party's First Orientations, the Working Party outlines a procedural approach to assessing adequacy.[505] Here, the Working Party recognizes that Article 25 establishes a case-by-case approach for assessing the adequacy of a data transfer or a set of transfers.[506] The Working Party also acknowledges that Member States are not capable of making an individual detailed analysis of every transfer of personal data to third countries.[507] The paper suggests, therefore, that Member States develop a decision-making procedure by which they can

---

501. *See* Europa, *Official Documents – White Papers* (visited Feb. 15, 1998) <http://europa.eu.int/search97cgi/s97r_cgi. . .=white¶paper& ViewTemplate=EUROPA_ view. hts> (also on file with the *Fordham International Law Journal*) (explaining that "[a] White Paper is a document presenting detailed and debated policy both for discussion and political decision."); *cf.* Europa, *Official Documents – Green Papers* (visited Feb. 15, 1998) <http://europa.eu.int/comm/off/green/index.htm> (also on file with the *Fordham International Law Journal*) (explaining that "[a] Green Paper is a document presented for public discussion and debate.").

502. *See* First Orientations, *supra* note 48, at 2 (implying that Working Party intended First Orientations to provide guidance to Member States and Commission). Although the Working Party does have *de jure* authority to "make recommendations on all matters relating to the protection of persons regarding to the processing of personal data in the Community," the Directive does not explicitly authorize the group to issue recommendations on the adequacy of protection in third countries. Directive, *supra* note 4, art. 30(3), O.J. L 281/31, at 48 (1995). The Working Party does, however, have *de facto* authority to make such recommendations. *See* First Orientations, *supra* note 48, at 2-3 (noting that Working Party can give provisional views on adequacy of protection regarding particular data transfers).

503. *See* First Orientations, *supra* note 48, at 1 (focusing on adequacy in the context of Article 25(1) & (2), not in the sense used in Article 26(2) exemptions).

504. *See id.* at 4 (discussing what constitutes adequate protection).

505. *See id.* at 1-4 (describing procedural approach to assessing adequacy).

506. *Id.* at 1.

507. *See id.* at 1-2 (stating that "given the huge number of transfers of personal data leaving the Community on a daily basis and the multitude of actors involved in such transfers, no Member State, whatever the system it chooses to implement Article 25, will be able to ensure that each and every case is examined in detail.").

examine some cases in detail, but permit most transfers.[508]

The Working Party suggests that Member States could develop provisional white lists[509] to create categories of data transfers that need not be examined individually.[510] Although the Original Proposal provided for blacklisting third countries with inadequate protection,[511] the Working Party abandons this approach.[512] Instead, Member States could develop white lists of countries that ensure an adequate level of protection.[513] Under Article 25's case-by-case approach, Member States would need to base their white lists on several representative cases rather than an abstract analysis of the law.[514]

While the Working Party favors white listing, the group acknowledges two difficulties with this approach to assessing adequacy.[515] The Working Party recognizes that Member States cannot automatically white list all transfers to a third country that does not have uniform data protection.[516] Instead, Member States must determine whether the various laws and business practices of the third country provide adequate protection in certain sectors and white list those sectors.[517]

---

508. *See id.* at 2 (discussing need for procedural mechanism for assessing adequacy).

509. *See id.* at 2 (noting that white list of third countries would consist of countries deemed to provide adequate protection).

510. *See id.* at 2-3 (discussing white lists).

511. *See* Reidenberg, *Setting Standards*, *supra* note 53, at 543 (noting that Original Proposal contemplated blacklisting).

512. *See* First Orientations, *supra* note 48, at 3 (rejecting blacklisting). The Working Party explains that even if a third country is not white-listed, Member States should not infer that the third country is black-listed, but instead "that no guidance regarding that particular country is yet available." *Id.* The group recognizes that black-listing countries would be politically sensitive. *Id.*

513. *Id.* at 2 (discussing how to develop white lists).

514. *Id.* Recall that Article 25(2) requires that adequacy be assessed in the context of the circumstances surrounding a data transfer. Directive, *supra* note 5, art. 25(2), O.J. L 281/31, at 45-46 (1995). Article 25(3) requires that Member States and the Commission notify one another of cases where a third country does not provide adequate protection within the meaning of Article 25(2). *Id.* In the context of the emphasis that these two provisions place upon analyzing particular "transfers or sets of transfers," the Working Party seeks to maintain the case-by-case analysis. *See* First Orientations, *supra* note 48, at 1-4 (outlining case-by-case procedure for assessing adequacy).

515. First Orientations, *supra* note 48, at 2-3.

516. *See id.* at 2 (presenting problem of assessing adequacy of third countries that lack uniform data protection). For example, a Member State should not white list all transfers to a third country that protects personal information in some, but not all, sectors. *Id.*

517. *See id.* at 2 (noting that "care would need to be taken in deciding whether the

Further, the Working Party also recognizes that the Directive involves various parties in assessing adequacy of third countries.[518] The paper explains the complementary roles of the Member States, the Commission, and the Working Party in assessing adequacy.[519] The Member States ordinarily should make a preliminary decision about whether protection is adequate for a particular transfer.[520] Then the Commission, working with the Article 31 Committee, must decide whether transfers to the third country should be prevented or permitted.[521] The Working Party has no role in determining adequacy in particular cases, but it can give formal opinions on the level of protection in third countries and provide informal guidance on how to assess adequacy in general.[522]

Next, the Working Party explains the second step of its recommended procedure.[523] These experts recognize that Member States will need to examine specific data transfers to third countries that are not white listed with regard to that type of transfer.[524] The manner in which the Member States analyze these non-white listed transfers will depend upon whether controllers or Member States' supervisory authorities are responsible for assessing adequacy.[525] If controllers assess adequacy, then they should be able to handle the limited data transfers that they

---

protection afforded to a particular data transfer was representative of the entire country or only of a particular sector or state"). For instance, a Member State examining the United States would have to examine the U.S. Constitution, federal and state law, and business practices, to assess whether any U.S. sector protected data adequately. *See id.* (recognizing added difficulty to third countries with federal systems).

518. *See id.* at 2 (describing roles of Member States, Commission, Article 31 Committee, and Working Party in assessing adequacy of third country data protection).

519. *Id.*

520. *See id.* (noting that Member States make decisions about particular data transfers). *But see* Directive, *supra* note 4, art. 25(3), O.J. L 281/31, at 46 (1995) (providing Commission with authority to make decisions on particular transfers also).

521. First Orientations, *supra* note 48, at 2; Directive, *supra* note 4, arts. 25(4), 25(6), 31(2), O.J. L 281/31, at 46, 49 (1995).

522. First Orientations, *supra* note 48, at 2-3; Directive, *supra* note 4, art. 30(1)(b), O.J. L 281/31, at 48 (1995).

523. First Orientations, *supra* note 48, at 3-4.

524. *Id.* at 3. The third countries may be either not white listed at all or partially white listed, but not in the sector of the particular transfer in question. *See id.* at 2 (describing possibility of partial white listing).

525. *Id.* at 3. A footnote in the Working Party's paper explains that a Member State may impose the duty to assess adequacy on the data controllers and/or the supervisory authorities. *See id.* at 1 n.1 (explaining that Member States can establish different administrative procedures under Article 25).

make.[526] In contrast, if the Member State assigns the duty to assess adequacy to its supervisory authority, then this authority will be responsible for a large volume of transfers.[527] Because these transfers may be so numerous, the Working Party suggests that the authorities prioritize these non-white listed transfers.[528] After identifying the transfers that pose the most serious threats to data privacy, the national authorities could examine these transfers first.[529] Identifying such transfers will also help the authorities assess what measures are necessary to protect personal data against these risks to privacy.[530]

The Working Party outlines a provisional list of data transfer categories that pose particular risks to individual privacy.[531] For instance, the first category of transfers that the paper identifies

---

526. *See id.* at 3 (implying that compared to huge volume of transfers to be assessed by supervisory authorities, transfers to be assessed by controllers will be manageable).

527. *Id.* The Working Party suggests that the Member States might assign the duty to assess adequacy to the supervisory authorities in one of two ways. *Id.* at 1 n.1. An authority could authorize data transfers before they take place or verify them *ex post facto*. *Id.*

528. *Id.* at 3.

529. *Id.* Under this system of prioritization, national supervisory authorities would still be responsible for requiring that all transfers receive adequate protection. *Id.* The supervisory authorities, however, could focus most of their attention and resources on the priority cases. *Id.*

530. *Id.*

531. *See id.* at 3-4 (stating that Working Party will issue more specific and detailed paper discussing risky transfer categories). This list of data transfers posing a particular threat to privacy includes:

- — those transfers involving certain sensitive categories of data as defined by Article 8 of the directive;
- — transfers which carry the risk of financial loss (e.g. credit card payments over the Internet);
- — transfers carrying a risk to personal safety;
- — transfers made for the purposes of making a decision which significantly affects the individual (such as recruitment or promotion decisions, the granting of credit, etc.);
- — transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- — transfers which may result in specific actions which constitute a significant intrusion into an individual's private life, such as unsolicited telephone calls;
- — repetitive transfers involving massive volumes of data (such as transactional data processing over telecommunications networks, the Internet etc.);
- — transfers involving the collection of data in a particularly covert or clandestine manner (e.g. Internet cookies).

Id.

are those that involve sensitive personal data.[532] Such sensitive information includes an individual's race, religion, ethnicity, political opinions, and medical records.[533] Another category involves transfers that may result in intrusions into an individual's private life.[534] For example, some direct marketing techniques might constitute such an intrusion.[535]

2. Standard to Assess Adequacy

After presenting a procedure by which Member States can assess adequacy, the Working Party describes the minimum requirements for adequate protection.[536] The Working Party concludes that an analysis of adequate protection must examine the two basic elements of adequate protection.[537] These two elements are the content of the applicable rules and the means of enforcing these rules.[538] Drawing upon the rights and obligations set down in the Directive, the Working Party identifies six basic content principles that ensure adequate data protection.[539] The group also recognizes that to be effective data protection principles must be followed in practice.[540] Thus, a third country must have enforcement mechanisms[541] to guarantee compliance with the content principles.[542]

---

532. *Id.* at 3.

533. *See* Directive, *supra* note 4, art. 8(1), O.J. L 281/31, at 40 (1995) (listing special categories of personal data to which Working Party refers in first category).

534. First Orientations, *supra* note 48, at 4.

535. *See id.* (noting unsolicited phone calls as possible intrusion).

536. *See id.* at 4-7 (explaining what constitutes adequate protection). The Working Party recognizes that these minimum requirements must not be too rigid. *Id.* at 5. The group suggests that the list of requirements might be supplemented or reduced where necessary. *Id.*

537. *Id.* at 5.

538. *Id.*

539. *See id.* at 5-6 (listing content principles as (1) purpose limitation principle, (2) data quality and proportionality principle, (3) transparency principle, (4) security principle, (5) rights of access, rectification, and opposition, and (6) restrictions on onward transfer to other third countries). To derive these principles, the Working Party took into account the provisions of the other data protection texts such as the COE Convention and the OECD Guidelines. *See id.* at 4-5 (describing elements of earlier data protection measures).

540. *Id.* at 4.

541. *See id.* (giving sanctions, remedies, liabilities, supervisory authorities, and notification as examples of procedural enforcement mechanisms).

542. *Id.* The Working Party cites the enforcement mechanisms included in European data protection laws and the EC Directive. *Id.* The group, however, acknowledges that third countries often do not have extensive enforcement mechanisms. *Id.*

The basic content principles for adequate protection reflect the standards of the Directive.[543] According to the Working Party, data protection measures in a third country should require that controllers process personal information for a specific purpose and not reuse that data for an incompatible purpose.[544] Personal information should be accurate and, where necessary, kept up to date as well as adequate, relevant, and not excessive.[545] Further, the controller should inform data subjects of the purpose for the processing, the controller's identity, and any other information necessary to ensure fairness.[546] In addition, the controller should implement appropriate technical and organizational security measures to protect the personal data.[547] The third country's data protection measures should also provide the data subject with a right to access personal data, a right to correct inaccurate data, and a right to object to processing of the data.[548] Finally, the Working Party concludes that the third country should allow further transfers of the data to another third country only if the other third country provides adequate data protection.[549]

In addition to the six basic content principles, the Working Party suggests that certain types of transfers might be subject to additional requirements.[550] For example, a transfer of sensitive data should receive additional safeguards, such as a requirement that the data subject explicitly consent to the transfer.[551] Further, before a transfer of personal data for direct marketing purposes, the controller should permit the data subject to opt-out of

543. *Id.* at 4-5. The content principles also reflect the general "consensus as to the content of data protection rules which stretches well beyond the fifteen states of the Community." *Id.* at 4.

544. *See id.* at 5 (describing purpose limitation principle derived from Directive, art. 6(1)(b) as first content principle).

545. *See id.* (stating data quality and proportionality principle derived from Directive, art. 6(1)(c) & (d) as second content principle).

546. *See id.* at 5 (describing transparency principle derived from Directive, art. 10 as third content principle).

547. *See id.* (stating security principle derived from Directive, art. 17 as fourth content principle).

548. *See id.* (describing principle securing rights of access, rectification, and opposition derived from Directive, arts. 12(a), 12(b), and 14 as fifth content principle).

549. *See id.* at 5-6 (stating principle regarding restrictions on onward transfers to other third countries as sixth content principle).

550. *See id.* (explaining that in some instances, transfers will need to meet additional requirements).

551. *Id.* at 6.

the transfer.[552]

The Working Party proceeds to discuss what enforcement mechanisms are necessary for data protection measures to constitute adequate protection.[553] The Working Party acknowledges that to provide adequate protection a third country needs some mechanism to ensure compliance with the content principles.[554] Although most Member States favor omnibus data protection laws enforced by independent supervisory authorities, the Working Party does not require third countries to adopt such an approach.[555] Instead, the Working Party identifies three essential objectives of an enforcement system.[556] The third country's procedural framework must deliver a good level of compliance with the data protection rules.[557] The enforcement system should help individual data subjects enforce their rights.[558] Finally, the third country's procedural system should provide the data subject with a method to obtain appropriate redress.[559]

III. *PARTIAL ADEQUACY OF U.S. DATA PROTECTION ASSESSED UNDER THE WORKING PARTY'S APPROACH*

The Member States and the Commission should conclude that U.S. protection ensures adequate protection in some contexts, but not in others. The United States provides adequate protection in the public sector, but not in the private sector as a whole. Nonetheless, Member States and the Commission should

552. *Id.* The Working Party notes that transfers involving automated individual decisions might also involve additional requirements. *Id.*

553. *See id.* at 6-7 (discussing requirements for enforcement mechanism of content principles).

554. *See id.* at 4 (concluding that enforcement mechanism is essential to data protection).

555. *See id.* at 6 (recognizing that requiring third country to adopt omnibus laws would be too formalistic).

556. *Id.* at 6-7.

557. *Id.* at 6. The procedural system need not ensure total compliance, but it should generate controllers and data subjects aware of their roles in the system. *Id.* Further, other enforcement mechanisms like sanctions and direct verification of transfers are valuable. *Id.* at 6-7.

558. *Id.* at 7. The individual should be able to enforce his rights rapidly and effectively, without prohibitive cost, through an independent investigative mechanism. *Id.*

559. *Id.* The Working Party notes that a system of independent arbitration with compensation and sanctions is necessary. *Id.*

white list[560] transfers in the context of specific areas of the private sector such as telecommunications and credit reporting. U.S. data protection in other subsectors such as banking and employment may also provide adequate protection if the self-regulation that they adopt is demand effective. In some specific areas of the private sector, however, neither formal legislation nor effective self-regulation exists, so protection in these areas is certainly inadequate.

A. *Member States and the Commission Should Analyze U.S. Data Protection by Sector*

Article 25 of the Directive provides that the Member States and the Commission should assess U.S. data protection on a case-by-case basis.[561] Only by examining a particular transfer or set of transfers can the Member States determine whether the United States has an adequate level of protection in light of all the circumstances.[562] Although the Working Party acknowledged that Article 25 provides for a case-by-case approach, the Working Party recognizes that Member States could not examine every data transfer to a third country like the United States.[563] Consequently, the Working Party suggests that the Member States and the Commission develop provisional white lists of countries that provide adequate protection.[564] The Working Party also recognizes that where many third countries do not have omnibus data protection, Member States and the Commission should not assess data protection overall.[565] Instead, the Member States should white list those sectors that do ensure adequate protection, but not those that fail to do so.[566] If a third country does not provide adequate protection in a particular sec-

560. *See supra* note 509 (discussing white listing).

561. *See supra* note 204 and accompanying text (noting that procedure for assessing level of data protection in third countries involves case-by-case analysis).

562. *See supra* note 221 and accompanying text (explaining that Article 25(2) requires Member States to assess third countries adequacy in light of surrounding circumstances).

563. *See supra* note 507 and accompanying text (relating Working Party's recognition that detailed analysis of every transfer is impossible).

564. *See supra* note 510 and accompanying text (discussing provisional white lists).

565. *See supra* note 516 and accompanying text (stating Working Party's position that Member States should not white list all transfers where third country's data protection laws are not uniform).

566. *See supra* note 517 and accompanying text (explaining partial white listing).

tor, then the Member States should analyze specific transfers, giving priority to those that pose particular threats to privacy.[567]

When assessing the level of U.S. data protection under the Working Party's suggested procedure, the Member States should analyze data transfers to the U.S. that are representative of particular sectors, not of the entire country. Because the United States approaches data protection in an ad hoc, sectoral manner, Member States should not judge the adequacy of U.S. protection as a whole. Member States should instead assess the level of data protection that the United States provides in different sectors and white list those sectors that provide adequate protection.[568] The U.S. public and private sectors should be examined separately because U.S. data protection laws regulate the government and private citizens differently.[569] Member States should analyze the adequacy of data protection in the U.S. public sector as a unit because federal regulation of the public sector generally applies to the entire public sector.[570]

In contrast, Member States should assess adequacy in the U.S. private sector by particular subsectors such as telecommunications and direct marketing. This specific analysis is necessary because U.S. data protection in the private sector generally targets particular areas.[571] Federal and state laws regulating the private sector apply in specific contexts.[572] Further, self-regulation of the private sector has been adopted in specific industries or by particular companies rather than by the entire public sector.[573]

Finally, Member States should analyze individual data transfers to those U.S. sectors or subsectors that are not white listed. The Member States will need to give priority to those transfers to

---

567. *See supra* notes 523-33 and accompanying text (relating Working Party's specific analysis of transfers in sectors without adequate protection).

568. *See supra* note 517 and accompanying text (discussing partial white listing).

569. *See supra* notes 244-59 and accompanying text (relating different regulation of private and public sectors in United States).

570. *See supra* notes 286-322 and accompanying text (discussing federal statutes that regulate entire public sector).

571. *See supra* note 343 and accompanying text (noting sectoral regulation of private sector).

572. *See supra* note 344 and accompanying text (stating that federal statutes in private in private sector target particular areas).

573. *See supra* note 345 and accompanying text (relating narrowly targeted self-regulation in private sector).

the United States that pose particular threats to privacy.[574] Member States should determine which specific transfers deserve priority by ascertaining whether the specific transfers fall into one of the categories of transfers that pose a risk to individual privacy.[575]

B. *U.S Data Protection in the Public Sector Is Adequate*

The Member States should find that U.S. data protection in the public sector ensures an adequate level of protection because regulation of the U.S. public sector complies with the Working Party's minimum requirements for adequate protection. U.S. data protection in the public sector embodies most of the content principles outlined by the Working Party.[576] Further, this data protection provides enforcement mechanisms that satisfy the objectives set forth by the Working Party.[577]

1. U.S. Data Protection in the Public Sector Reflects the Content Principles

U.S. regulation of the public sector reflects most of the content principles suggested by the Working Party and derived from the Directive.[578] Data protection laws in the U.S. public sector reflect the purpose limitation principle, which requires controllers to process data for a specific purpose and to reuse such data only for a compatible purpose.[579] For instance, under the Privacy Act,[580] a federal agency can maintain only personal data necessary and relevant to accomplish the agency's purpose.[581] The Privacy Act also prohibits disclosure of personal data unless disclosure is compatible with the purpose for which the govern-

574. *See supra* notes 528-30 and accompanying text (explaining need to prioritize transfers that do not fall into white-listed sector).

575. *See supra* notes 531-35 and accompanying text (discussing categories of particularly risky transfers outlined by Working Party).

576. *See supra* notes 543-49 and accompanying text (describing six basic content principles).

577. *See supra* notes 553-59 and accompanying text (relating three essential objectives of enforcement system).

578. *See supra* notes 267-340 (discussing U.S. regulation of public sector at constitutional, federal, and state level).

579. *See supra* note 544 and accompanying text (relating purpose limitation principle).

580. The Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996).

581. *Id.* § 552a(e)(1).

ment collected the data.[582] Further, specific laws regulate when the U.S. Census Bureau and the Internal Revenue Service can disclose personal data.[583]

U.S. data protection regulation in the public sector embraces other content principles. The Privacy Act protects data quality[584] by requiring that federal agencies maintain relevant, accurate, timely, and complete records.[585] In addition, the Privacy Act encourages transparency[586] by requiring federal agencies to publish lists of the personal data that they maintain.[587] U.S. laws like the Privacy Act also oblige federal agencies take measures to ensure security[588] and confidentiality of personal data.[589] Finally, the Privacy Act guarantees most data subjects the right to access and correct[590] personal information.[591]

U.S. regulation of the public sector, however, does not embody the Working Party's content principles in two respects. The right to access and correct personal data under the Privacy Act applies only to citizens and legal residents of the United States, not EU citizens.[592] U.S. data protection law also makes no provision for further transfers to non-EU countries.[593]

Despite these two deficiencies, the Member States should conclude that U.S. data protection in the public sector satisfies the content principles set forth by the Working Party. Although the Working Party suggests six content principles, it recognizes that this list might need to be supplemented or reduced.[594] In the public sector, U.S. data protection reflects a significant por-

---

582. *Id.* § 552a(a)(7) & (b)(3).

583. *See supra* notes 323-27 and accompanying text (discussing federal statutes that regulate public sector in specific contexts).

584. *See supra* note 545 and accompanying text (stating data quality and proportionality principle).

585. 5 U.S.C. § 552a(e)(5).

586. *See supra* note 546 and accompanying text (relating transparency principle).

587. The Privacy Act of 1974, 5 U.S.C. § 552a(e)(4) (1994).

588. *See supra* note 547 and accompanying text (describing security principle).

589. *See supra* note 295 and accompanying text (noting Privacy Act requires certain safeguards).

590. *See supra* note 548 and accompanying text (stating principle securing right to access and correct personal data).

591. *See supra* notes 299-300 and accompanying text (relating right of access under Privacy Act).

592. 5 U.S.C. § 552a(a)(2).

593. *See supra* note 549 and accompanying text (stating principle that requires restrictions on further transfers of personal data to non-EC countries).

594. *See supra* note 536 (noting that list of content principles in not rigid).

tion of the content principles. At present, Member States and the Community should excuse the limited scope of the Privacy Act because Congress enacted this statute long before the Directive required third countries to provide adequate protection. Perhaps the Community should urge the United States to expand the scope of the Privacy Act at some later point, but the Privacy Act's present failure to cover non-U.S. citizens should be excused.

Similarly, Member States should excuse the failure of U.S. data protection to restrict further data transfers to third countries without adequate protection. The restriction of data transfers to non-EU countries without adequate protection is a new data protection principle that the Directive itself introduced.[595] In fact, the United States can hardly be expected to restrict onward transfers to third countries without adequate data protection when the Working Party is still explaining what constitutes adequate protection. Thus, Member States should recognize that U.S. data protection in the public sector embodies a substantial portion of the Working Party's content principles.

2. U.S. Data Protection in the Public Sector Provides Effective Mechanisms for Enforcing the Content Principles

U.S. regulation of personal data in the public sector ensures effective application of the content principles through procedural and enforcement mechanisms. Although the United States can certainly improve enforcement of data protection regulation in the public sector,[596] such data protection satisfies the three objectives established by the Working Party.[597] Consequently, Member States should conclude that data protection in the U.S. public sector complies with the enforcement requirements set forth in the Working Party's First Orientations.

U.S. data protection in the public sector satisfies the Working Party's three enforcement objectives.[598] For example, U.S. statutes deliver a good level of compliance with the content prin-

595. *See supra* notes 466-76 (noting that no earlier data protection measures used adequacy standard).

596. *See supra* notes 334-40 and accompanying text (discussing deficiencies of data protection in U.S. public sector).

597. *See supra* notes 553-59 (explaining three essential enforcement objectives).

598. *See supra* notes 286-340 (explaining enforcement of various federal statutes that regulate U.S. public sector).

ciples.[599] The Privacy Act requires each federal agency to publish a list of its records[600] and provides data subjects with the right to sue for violating the statute.[601] The Matching Act[602] improves compliance by establishing procedures to regulate data matching and by creating the Data Integrity Boards to regulate federal agency data matching.[603] While the Privacy Act and the Matching Act do not enable data subjects to enjoin federal agencies to change their practices,[604] the Working Party recognizes that perfect compliance is impossible.[605]

Further, the U.S. system allows individual data subjects to exercise their rights and obtain redress in the courts.[606] Although enforcement of U.S. data privacy statutes is often difficult,[607] the Privacy Act does permit individuals to sue to enforce their rights.[608] The Privacy Act also provides redress for data subjects. An individual can appeal when a federal agency denies a request to amend incorrect personal information.[609] Further, an individual can sue the federal agency for Privacy Act violations.[610] A government employee may even be found criminally liable for knowingly and willfully violating the Privacy Act.[611]

Member States should conclude that U.S. data protection in the public sector is adequate because U.S. regulation provides effective enforcement of the content principles. Admittedly, the U.S. system has no independent authority to enforce data protection rules and enforcement is often slow and costly. Nonethe-

---

599. *See supra* note 557 and accompanying text (noting that one objective of enforcement system must be to ensure good level of compliance).

600. The Privacy Act of 1974, 5 U.S.C. § 552a(e)(4) (1994).

601. *Id.* § 552a(d)(3) & (g).

602. The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. §§ 552a(a)(8)-(13), (e)(12), (o)-(r), (u) (1994 & Supp. II 1996).

603. *See supra* notes 313-17 and accompanying text (discussing regulation of Matching Act).

604. *See supra* note 303 and accompanying text (noting limited injunctive power of Privacy Act).

605. *See supra* note 555 and accompanying text (relating flexibility of Working Party's approach).

606. *See supra* notes 558-59 (stating that two objectives of enforcement system must be to help individuals enforce their right and to provide appropriate redress).

607. *See supra* note 309 and accompanying text (discussing difficulties with enforcing Privacy Act).

608. The Privacy Act of 1974, 5 U.S.C. § 552a(d)(3) & (g) (1994).

609. *Id.* § 552a(f).

610. *Id.* § 552a(d)(3) & (g).

611. *Id.* § 552a(i).

less, the Working Party recognizes that third country data protection measures need not be identical to Member State data protection measures.[612] Consequently, because the U.S. laws embody most of the content principles and provide mechanisms to enforce these principles, Member States should find that the United States ensures an adequate level of protection for data transfers in the public sector.

C. *U.S. Data Protection in the Private Sector Is Generally Inadequate, But Data Protection in Particular Areas of the Private Sector Is Adequate*

The Member States should conclude that U.S. data protection in the private sector does not provide an adequate level of protection in general. Specific subsectors such as telecommunications and the credit reporting industry, however, should be white listed. Further, the Member States may also white list other specific areas of the U.S. private sector, such as, employment and banking after determining that those sectors provide adequate self-regulation. Moreover, those areas in the U.S. private sector that do not ensure adequate protection such as health care and direct marketing should not be blacklisted. Instead, Member States should analyze such data transfers on a case-by-case basis, giving priority to transfers that pose a particular risk to privacy.

1. U.S. Data Protection in the Private Sector Is Inadequate on the Whole

The Member States should not white list all data transfers to the U.S. private sector because data protection in the private sector as a whole fails to reflect the Working Party's minimum requirements for adequate protection. Under the ad hoc, sectoral approach, U.S. regulation of the private sector is not uniform.[613] Because there are no comprehensive data protection measures in the private sector, significant gaps in data protection exist. For example, while a federal statute protects video rental

612. *See supra* note 555 and accompanying text (noting that Working Party's approach to enforcement mechanism is not too formal).

613. *See supra* notes 341-44 and accompanying text (discussing sectoral nature of U.S. data protection in private sector).

records,[614] medical records are basically unregulated at the federal level.[615] Further, self-regulation does not solve this problem because businesses and industries have not uniformly adopted self-regulation.[616] Consequently, due to the patchwork of data protection regulation in the private sector, Member States should not find that the entire private sector provides adequate protection.

2. U.S. Data Protection in Certain Areas such as Telecommunications and Credit Reporting Is Adequate

Although Member States should not white list the entire private sector, particular areas of the private sector do ensure adequate protection. For example, the credit reporting industry and a significant portion of the telecommunications sector satisfy most of the Working Party's requirements. Regulation of both credit reporting and telecommunications embody the content principles. Data protection in these two areas also provides sufficient enforcement. Finally, self-regulation in both sectors supplements any deficiencies in legislation.[617]

Members States should white list most data transfers to the United States in the field of telecommunications. U.S. statutes regarding telecommunications embody many of the Working Party's content principles.[618] The ECPA[619] and the Telecommunications Act[620] reflect the purpose specification principle and the data quality principle by regulating the collection, maintenance, and disclosure of personal data.[621] Security of telecommunications data is ensured by the ECPA as well as by self-regula-

---

614. *See supra* note 53 (noting Video Privacy Protection Act's regulation of video rental records).

615. *See supra* notes 427-40 and accompanying text (discussing lack of U.S. data protection regarding medical records).

616. *Compare supra* notes 374-81 (describing significant self-regulation of telecommunications) *with supra* notes 451-458 (describing poor self-regulation of direct marketing).

617. *See supra* note 485 (noting that self-regulation by company or industry qualifies as professional rules under Directive's adequacy standards).

618. *See supra* notes 543-49 (describing Working Party's content principles).

619. The Electronic Communications Protection Act, 18 U.S.C. §§ 2510-2511, 2701-2709 (1994), *amended by* 18 U.S.C.A. §§ 2510-2511, 2701-2709 (West Supp. 1997).

620. The Telecommunications Act of 1996, 47 U.S.C.A. § 222 (West Supp. 1997).

621. *See supra* notes 356, 370-70 and accompanying text (relating data protection of ECPA and Telecommunications Act).

tion.[622] Further, the ECPA ensures a good level of compliance and provides redress for individuals.[623] The Telecommunications Act does not cover non-telecommunications carriers, however, so data transfers to non-telecommunications carriers might not have adequate protection.[624]

Likewise, regulation of the credit reporting industry reflects the Working Party's content principles. The FCRA[625] regulates the collection and subsequent use of credit information[626] and protects data quality by ensuring that data is complete and accurate.[627] The statute also guarantees a right to access and correct credit information.[628] In addition to the FCRA, the credit reporting industry has adopted voluntary privacy standards to protect personal data.[629] Moreover, the FCRA provides substantial enforcement mechanisms.[630]

U.S. data protection in telecommunications and credit reporting should be considered adequate. Although regulation of these sectors does not meet all of the content principles, this regulation does satisfy most of them. Further, regulation of telecommunications and credit reporting provides some enforcement measures. Thus, if Member States decide to white list any areas of the U.S. private sector, they should at least white list transfers in the context of telecommunications and credit reporting.

3. U.S. Data Protection in Other Specific Areas such as Banking and Employment May Be Considered Adequate

While legislation in some specific areas of the private sector

622. *See supra* notes 360, 380 and accompanying text (discussing security of telecommunications).

623. *See supra* note 361 and accompanying text (noting enforcement of ECPA).

624. *See supra* note 373 and accompanying text (mentioning limited scope of Telecommunications Act).

625. The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994), *amended by* 15 U.S.C.A. §§ 1681-1681u (West Supp. 1998).

626. *See supra* notes 393-394 and accompanying text (noting data protection of FRCA).

627. 5 U.S.C. §§ 1681c-k.

628. *Id.* § 1681m.

629. *See supra* notes 402-04 and accompanying text (discussing self-regulation of credit reporting industry).

630. *See supra* notes 397-98 and accompanying text (explaining enforcement of FCRA through private law suits and FTC oversight).

does not constitute adequate protection, significant self-regulation in those industries may provide adequate protection. No comprehensive data protection laws regulate either banking[631] or the workplace.[632] Both of these areas of the private sector, however, engage in significant self-regulation. The financial services industry has traditionally protected customer information and recently has adopted data protection policies.[633] Similarly, in addition to complying with a few narrow statutes that protect employee information, many employers have instituted fair information practices.[634]

Member States should place specific areas of the U.S. private sector that have adopted substantial self-regulation on provisional white lists if this self-regulation is comprehensive and ensures enforcement of the Working Party's content principles. If self-regulation targets only a portion of the companies in a specific industry, however, then that industry's protection does not provide adequate protection. Further, even if self-regulation in a specific area is comprehensive, Member States should white list that area only if the statutory regulation and the self-regulation reflect the Working Party's six content principles and ensure their enforcement.[635]

4. U.S. Data Protection in Many Areas of the Private Sector such as Health Care and Direct Marketing Are Not Adequate

Member States should not white list many areas of the U.S. private sector. For instance, data protection in health care and direct marketing is inadequate. No federal legislation regulates the treatment of medical records, and state laws and the health care industry provide meager protection of personal medical information.[636] Likewise, almost no sectoral laws regulate direct

631. *See supra* notes 383-84 and accompanying text (noting lack of comprehensive privacy legislation regulating banking).

632. *See supra* note 407 and accompanying text (relating patchwork regulation of employee information).

633. *See supra* notes 383-87 and accompanying text (discussing self-regulation of banking industry).

634. *See supra* notes 421-26 and accompanying text (describing self-regulation by employers).

635. *See supra* note 538 and accompanying text (explaining Working Party's suggested minimum requirements for adequate protection).

636. *See supra* notes 435-40 and accompanying text (describing minimal federal and state regulation of medical records).

marketing and industry efforts are generally ineffectual.[637] Thus, these two specific areas, like many other areas in the private sector, do not provide an adequate level of protection for data transferred to the United States.

While the Member States should not partially white list specific areas that lack adequate protection, the Member States also should not blacklist these areas. The Working Party suggests that instead the Member States should analyze specific transfers in these areas that are not white listed.[638] Under this approach, the Member States will need to give priority to transfers that pose particular risks to privacy.[639] Specific transfers in the context of both health care and direct marketing should probably be given priority because they would likely fall under the categories of particularly risky transfers outlined by the Working Party. For example, transfers of medical data to the United States should receive priority because such transfers involve sensitive data as identified in Article 8 of the Directive.[640] Likewise, transfers in the context of direct marketing pose a threat to privacy because these transfers may result in actions that will constitute significant intrusions into an individual's private life.[641]

CONCLUSION

Under the Working Party's suggested approach for assessing the adequacy of a third country's data protection, the Member States and the Commission should find that although U.S. ad hoc, sectoral data protection does not ensure adequate protection across the board, U.S. regulation is adequate in many significant areas. Primarily, U.S. privacy laws in the public sector and a few areas of the private sector such as telecommunications and credit reporting provide adequate protection. Further, the Member States will probably conclude that U.S. legislation gov-

637. *See supra* notes 446-58 and accompanying text (discussing lack of privacy legislation regarding direct marketing).

638. *See supra* note 523-33 and accompanying text (relating Working Party's procedure for assessing adequacy of data transfers to third countries where transfers are not white listed).

639. *See supra* note 529 and accompanying text (explaining that Member States should first analyze transfer posing most serious threats to privacy).

640. *See supra* notes 531, 533 and accompanying text (describing transfers involving sensitive data as transfers that deserve priority).

641. *See supra* notes 534-35 and accompanying text (noting that transfers that may constitute intrusion into individual's private life deserve priority).

erning banking and employment is not sufficient, but significant self-regulation in these areas may constitute adequate protection. Member States will likely find that in some areas of the private sector such as health care and direct marketing, both privacy laws and self-regulation are still not adequate. If so, Member States will not white list transfers to the United States in these areas.