THE PERFECT STORM: THE SAFE HARBOR AND THE DIRECTIVE ON DATA PROTECTION

I. INTRODUCTION

With the stunning recent growth of international electronic commerce, issues of personal privacy have become far more visible. Consumers express increasing concern with the ability to control their private information, and many nations are responding by considering or passing regulations.[1] Such regulations are classified as data protection laws.[2]

The concept of data protection in U.S. law falls within the loose conglomeration of rights that comprise privacy law. The terms are often muddied, and require a clearer definition. As

1. *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, art. 1, Europ. T. S. No. 108, *available at* http://conventions.coe.int/treaty/en/Treaties/Html/108.htm [hereinafter Convention].

2. *Id.*

Professor Joel Reidenberg has suggested, "The terminology for standards of fair information practice has been poorly defined in the United States."[3] He continues:

> The term "privacy" is often used to describe the allocation of rights to personal information. This rhetoric is confusing. "Privacy" serves as a catch-all term, protecting a variety of interests ranging from government intrusion into the bedroom to the inviolability of telephone communications. Although fair information practices may be subsumed under the broad "privacy" label, the standards represent a narrower and distinct interest: maintaining the integrity of personal information and fairness to the individuals about whom the data relates. Specifically, such standards apply to the collection, storage, use, and disclosure of personal information.[4]

U.S. privacy laws generally deal with concepts of "invasion."[5] They stem from what Warren and Brandeis immortalized as "the right to be let alone" in their landmark *Harvard Law Review* article first arguing for the creation of an individual right to privacy.[6] Privacy laws also deal with the specific disclosure of "private" facts; behind this apparent tautology is the concept that freely available information should be unprotected.[7] Privacy laws function more to define what is not protected than what is.

Both of these legal foundations will have difficulty weathering new technologies and attitudes about personal data privacy. The invasion concept, while flexible to a point, may fail

---

3. Joel Reidenburg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995).

4. *Id*.

5. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (arguing that "the law of privacy comprises four distinct kinds of invasions of four different interests of the plaintiff"). *See also* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977) (describing four privacy torts, including 1) intrusion on the right of publicity (based on the appropriation of an individual's name or likeness); 2) intrusion into an individual's private affairs; 3) public disclosure of embarrassing private facts; and 4) publicly placing the individual in a false light).

6. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

7. *See* RAYMOND T. NIMMER, INFORMATION LAW ¶ 8.04 (2000).

to encompass broad issues of the passivity of modern data collection.[8] Further, the collection of such information, even if seen as publicly available and not worthy of protection, is significantly impacted by the new ability to store and analyze enormous amounts of such information. New technologies allow the creation of massive databases of so–called public information, which while unprotected by U.S. law, may reveal singly private patterns.[9]

These technologies also impact the psychological foundations of privacy laws. The new passivity of collection and the ease with which such data is used and transferred has begun to create growing concerns among American consumers about electronic privacy.[10]

The foundry for much change in data protection legislation

---

8. See Toby Lester, *The Reinvention of Privacy*, THE ATLANTIC MONTHLY, Mar. 2001, at 28.

> People give away vast amounts of valuable information about themselves, wittingly or unwittingly, by using credit cards, signing up for supermarket discount programs, joining frequent-flyer clubs, sending e–mail, browsing on the Internet, using electronic tollbooth passes, mailing in rebate forms, entering sweepstakes, and calling toll–free numbers. Such behaviors are essentially voluntary (although a somewhat abstract case can be made that they are the product of what has been called "the tyranny of convenience"), but many other ways of participating in everyday life basically *require* the divulging of information about oneself.

Id.

9. Consider a fictional example from Neal Stephenson's novel *Cryptonomicon*. Two mathematicians active in the effort to break German codes in the Second World War worry that if German Intelligence is able to capture the personnel records for their secret code–breaking base, they will notice an unusually large number of tall women working there (their height necessary to reach the tops of the large machines used to crack the German codes.) This information, normally freely available, now takes on enormous significance, and must be kept private. NEAL STEPHENSON, CRYPTONOMICON 146-47 (1999).

10. Author and privacy consultant Alan Westin suggests that the American population can be divided into three categories: 1) privacy fundamentalists (approximately twenty–five percent), 2) privacy unconcerned (approximately twelve percent), and 3) privacy pragmatists (approximately sixty–three percent) who "are always balancing the potential benefits and threats involved in sharing information, and are particularly concerned about . . . 'function creep'—that is, the secondary use (deliberate or inadvertent) of information that was originally divulged for one purpose only." Lester, *supra* note 8, at 34.

has been the European Union. European data protection standards have gradually evolved to address the issues above, granting broad rights to data subjects in an effort to address the passivity issue, and broad control rights to deal with the potential for escalating secondary uses.[11]

Two documents in the 1980s, the Organisation for Economic Cooperation and Development's (OECD's) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[12] and the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[13] were the first European attempts to consolidate and harmonize national data protection legislation.

The range of these documents was extended by an E.U. directive, Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.[14] The Directive sought to further limit the collection and use of personal data, and granted individuals significant rights to access collected data and consent to its collection.[15]

The Directive also forced European nations to ensure that any non-participatory nation provides an adequate level of protection before data may be transferred to that nation.[16] This presented a significant problem for U.S. organizations seeking to participate in Europe's growing information marketplace. The United States Department of Commerce and the European Commission entered into protracted negotiations to reach an agreement whereby U.S. organizations could meet the adequacy

11. *See, e.g.* Org. for Econ. Co-Operation and Dev., Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, *available at* http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM [hereinafter Guidelines].

12. *Id*.

13. Convention, *supra* note 1, art. 1.

14. Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Directive].

15. *See id*. arts. 10, 11, 18, 26, 42, 45, 68-70.

16. *Id*. arts. 25-26.

requirements.[17] The result was the Safe Harbor Privacy Principles,[18] a voluntary program through which a U.S. organization could receive certification that its data protection standards were adequate within the meaning of the Directive.[19]

This paper will analyze the refinements in European data protection standards that resulted in the ultimate passage of the Directive. Part II is an analysis of the OECD Guidelines, and Part III covers the Council of Europe Convention. Part IV is an examination of the Directive, focusing on the new commitment to individual rights and limited collection and use principles it requires. Part V is a discussion of the Safe Harbor Principles, and their inadequacy in light of the broad protections guaranteed by the Directive.

II. THE OECD GUIDELINES

The first effort to reconcile inconsistent international data protection laws occurred in 1981.[20] The Organisation for Economic Co-operation and Development[21] Council set forth the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Guidelines).[22] As the preface to the Guidelines suggests, "[t]he development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data."[23] At the date the Guidelines were

---

17. UNITED STATES DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (July 21, 2000) *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

18. *Id*.

19. *See id*.

20. NIMMER, *supra* note 7, ¶ 8.25[2][a].

21. The OECD is a research organization whose member countries meet to exchange information and develop policy. *See* Org. for Econ. Co–Operation and Dev., *What is OECD*, *at* http://www1.oecd.org/about/general/index.htm (last updated Aug. 2, 2001) [hereinafter OECD]. The OECD currently has thirty member countries representing Europe, North America and Asia. Org. for Econ. Co–Operation and Dev., *Membership*, *at* http://www1.oecd.org/about/general/member-countries.htm (last updated Oct. 1, 2001).

22. Guidelines, *supra* note 11.

23. *Id*. Preface.

promulgated, nine OECD member countries had passed privacy protection legislation, and five more nations were considering draft bills.[24]

The OECD Council recognized that these varying regulatory schemes were a valuable preservation of human rights, but that the disparities could disrupt the free flow of personal data.[25] The Guidelines thus attempt to balance privacy and individual liberties with the removal of "unjustified obstacles to transborder flows of personal data."[26] The Guidelines contain eight principles to achieve this end:

- *Collection limitation principle*: Data collection should be by fair means, with the knowledge or consent of the subject.
- *Data quality principle*: The data should be relevant to the purpose for which it is to be used, and should be accurate, complete and kept current.
- *Purpose specification principle*: A purpose should be specified at or before collection, and subsequent uses must comply with that purpose.
- *Use limitation principle*: No disclosure or use should occur for purposes other than the specified use without consent of the subject or authorization by law.
- *Security safeguards principle*: There should be reasonable precautions to protect data against loss and unauthorized access.
- *Openness principle*: Developments, practices, and policies of personal data use, along with the existence and nature of the data, should generally be open.
- *Individual participation principle*: The individual should be allowed to verify the existence of data concerning him, to obtain the information, and to

24. Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden, and the United States passed legislation. *Id*. Belgium, Iceland, the Netherlands, Spain, and Switzerland prepared draft bills. *Id*.

25. *Id*.

26. *Id*.

correct or erase any challenged data relating to him.

- *Accountability principle*: Persons who control the data are responsible for compliance with national law regarding the data protection rules.[27]

These eight basic principles are intended to serve as a framework for the protection of data privacy at the national level.[28] The Guidelines apply to personal data, defined as "any information relating to an identified or identifiable individual," and apply to both the public and private sectors.[29] They are minimum standards, and may be supplemented by appropriate national legislation or regulation.[30]

The Guidelines make clear, however, that any supplementation or modification should not unjustifiably interfere with the transborder flow of information.[31] The preservations of individual liberty offered through the eight principles above are thus balanced against the stated goal of preserving the free flow of data between Member countries.[32] The principles offer individuals some quality control over their personal data, and suggest that data collection and processing rights are limited.[33]

The division between quality rights and limitations on collection and use in the Guidelines tends to blur, however.

---

27. *Id.* §§ 7-14; *See also* NIMMER, *supra* note 7, ¶ 8.25[2][b].

28. Guidelines, *supra* note 11, § 23.

29. *Id*. §§ 1(b), 2.

30. *Id*. §§ 6, 19. Member countries are encouraged to: a) adopt appropriate domestic legislation; b) encourage and support self-regulation; c) provide for reasonable means for individuals to exercise their rights; d) provide for adequate sanctions and remedies for failure to comply; and e) ensure that there is no unfair discrimination against data subjects. *Id*. §19.

31. *Id*. § 18.

32. *See id*. §§ 15-18. Part Three of the Guidelines requires that Member countries: 1) consider the implications of data transfer and export for other Member countries; 2) act reasonably to ensure the security of transborder flows of personal data; 3) refrain from restricting transborder flows of data except where the recipient does not substantially observe the Guidelines or the re–export would circumvent its domestic privacy legislation; and 4) avoid developing laws, policies and practices which would create obstacles to transborder flows of personal data. *Id*.

33. *See* NIMMER, *supra* note 7, ¶ 8.25[2][a]. The eight principles of the OECD limit the collection of data and its use without consent, as well as the individual's right to disclosure, openness, and accuracy. *See* Guidelines, *supra* note 11, §§ 7-14.

Section 8, the Data Quality principle, clearly offers data subjects some quality rights by suggesting data be accurate, complete and up-to-date.[34] Paired with section 13, the Individual Participation principle (granting data subjects the ability to confirm the existence of data, to obtain the data, and to correct or destroy it if challenged),[35] the Guidelines grant data subjects a fairly broad right of control.

Section 7, the Collection Limitation principle, contains a mixture of control and use rights by acting both to limit collection of personal data, and also requiring "the knowledge or consent of the data subject."[36] Section 12, the Openness Principle, requires disclosure of both data practices and policies and the means to determine the existence and nature of personal data.[37] It also requires openness about the use of the data, as well as the identity of the data controller.[38] Openness in the existence and nature of data falls more closely under the right to data quality, while disclosure of use, policy, purpose and the controller's identity are collection and use rights.[39] Of course, a policy of openness provides little benefit without an accompanying remedy, which does not directly exist in Section 12.[40]

The goal of the Guidelines is to create a system whereby each OECD Member country has basic data privacy regulations in place,[41] not just for the protection of individual liberties, but to ease the regulatory burden that would result from widely

---

34. Guidelines, *supra* note 11, § 8.

35. *Id*. § 13.

36. *Id*. § 7.

37. *Id*. § 12.

38. *Id*. "Data controller" is defined by the Guidelines as "a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf." *Id*. § 1(a).

39. *See id*. §§ 7, 8, 12.

40. *See id*. § 12. Section 13 does provide a mechanism for the subject to exercise control over his data, as discussed above, but it functions independently of any recommendation of "openness," which appears instead to be an administrative convenience. *Id*. § 13.

41. *Id*. §25 (recommending Member countries set minimum standards of privacy protection).

varying privacy standards. As the Preface to the Guidelines states, "there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers . . . [r]estrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance."[42]

The OECD commitment to the free flow of information is not surprising given its stated goal of developing market economies.[43] The Guidelines are certainly not toothless, granting individuals substantial rights in both the collection and use of personal data,[44] and although they are not legally binding,[45] by 1994 all OECD Member countries had adopted the Guidelines.[46]

The construction of transnational regulations regarding data privacy almost requires such a framework—a broad preservation of liberties serves to protect individual citizens while encouraging Member countries to enact substantially similar legislation, easing regulatory and management burdens in a classically federal manner. The Council of Europe took a similar approach in 1981.[47]

III. COUNCIL OF EUROPE CONVENTION (TREATY 108)

The approach of the OECD Guidelines, offering a set of basic principles to preserve individual rights while easing restrictions on the flow of information between nations, is also reflected in the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal

---

42. *Id*. Preface.

43. OECD, *supra* note 21. ("The OECD groups 30 member countries in an organisation that, most importantly, provides governments a setting in which to discuss, develop and perfect economic and social policy . . . [e]ssentially, membership is limited only by a country's commitment to a market economy.")

44. *See* NIMMER, *supra* note 7, ¶ 8.25[2][c].

45. Guidelines, *supra* note 11, § 20.

46. OECD DOCUMENTS: PRIVACY AND DATA PROTECTION: ISSUES AND CHALLENGES 3 (1994) (survey of implementation of OECD Guidelines). *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).

47. Convention, *supra* note 1, art. 1 (recognizing the necessity of reconciling respect for privacy and the free flow of information).

Data[48] ("Convention"). The Convention was opened on January 28, 1981 and entered into force on October 1, 1985.[49]

The Convention, as a treaty, differs from the Guidelines in that it is legally binding on all signatory nations.[50] The Convention is non-self-executing; it does not impose direct legal norms on signatories.[51] It does, however, require the establishment of domestic data protection legislation to give effect to its principles[52] and it provides basic safeguards for the processing of data.[53] The Convention also applies only to data processed automatically,[54] while the OECD Guidelines apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."[55]

Like the OECD Guidelines, the Convention offers eight basic principles for data protection.[56] The Convention principles differ from the Guidelines by offering substantive restrictions on the content of the data files.[57] Article 5 governs data quality, requiring data to be relevant, accurate, processed and stored

---

48. *Id*.

49. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Summary, *available at* http://conventions.coe.int/treaty/en/Summaries/Html/108.htm (last updated Oct. 22, 2001).

50. *Id*.; *see also* Convention, *supra* note 1, art. 4.

51. Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 477 (1995).

52. *Id*.

53. *Id*.; "[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." Convention, *supra* note 1, art. 4.

54. Convention, *supra* note 1, art. 1; article 2 defines automatic processing as "the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval, or dissemination." *Id*. art. 2.

55. Guidelines, *supra* note 11, § 2.

56. Convention, *supra* note 1, arts. 4-11.

57. *See id*.; *see also* NIMMER, *supra* note 7, ¶ 8.25[2][b]; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Explanatory Report*, *opened for signature* Jan. 28, 1981, Europ. T.S. No. 108 § 18, *available at* http://conventions.coe.int/treaty/en/Reports/Html/108.htm [hereinafter Explanatory Report].

fairly, and kept only as long as required to meet its purpose,[58] thus mirroring several sections of the OECD Guidelines.[59] Article 6, though, provides new substantive restrictions not offered by the Guidelines, preventing the automatic processing of "[p]ersonal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life" without appropriate safeguards.[60]

Article 7 provides for the physical security of data,[61] much like section 11 of the Guidelines.[62] Article 8 offers safeguards for the data subject, enabling any person:

- to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
- to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
- to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
- to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.[63]

---

58. Convention, *supra* note 1, art. 5.

59. Guidelines, *supra* note 11, §§ 7-10; Article 5 of the Convention does add two significant restrictions: the storage and use restrictions ("personal data undergoing automatic [data] processing shall be . . . stored for specified and legitimate purposes and not used in a way incompatible with those purposes") and the preservation restriction ("personal data undergoing automatic [data] processing shall be . . . preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored"). Convention, *supra* note 1, art. 5.

60. Convention, *supra* note 1, art. 6.

61. *See id*. art. 7

62. Guidelines, *supra* note 11, § 11.

63. Convention, *supra* note 1, art. 8.

The basic principles of the Convention emphasize quality and control of personal data by data subjects.[64] The Council used the human rights principles contained in article 10 of the European Human Rights Convention,[65] which guarantees freedom of expression,[66] and article 19 of the International Covenant on Civil and Political Rights,[67] which provides for the same,[68] as bedrock foundations to support its commitment to personal data rights.[69]

As the explanatory report to the Convention explains, "certain rights of the individual may have to be protected vis-à-vis the free flow of information regardless of frontiers, the latter principle being enshrined in international and European instruments on human rights."[70] These instruments are a potential foundation for data privacy legislation, as the guarantees of informational freedom contained in them may be limited "to the extent strictly justified for the protection of other individual rights and freedoms, in particular the right to respect for individual privacy."[71] The Council's recognition that data

64. *See id*. arts. 5-8.

65. *See id*. art. 19; Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5, art. 10, *available at* http://conventions.coe.int/treaty/EN/Treaties/html/005.htm [hereinafter Human Rights Convention].

66. Human Rights Convention, *supra* note 65, art. 10.

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers . . . [t]he exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society.

Id.

67. Explanatory Report, *supra* note 57, § 19; *see also* International Covenant on Civil and Political Rights, Dec. 16 1966, art. 19, *available at* http://www.unhchr.ch/html/menu3/b/a_ccpr.htm [hereinafter Covenant on Rights].

68. Covenant on Rights, *supra* note 67, art. 19. "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." *Id*.

69. Explanatory Report, *supra* note 57, § 19.

70. *Id*.

71. *Id*.

protection legislation could potentially subvert a human rights commitment to freedom of expression, and its finding that any such impact would be justified by the necessity for individual privacy, further cements its legal impact.[72]

Article 12 of the Convention provides the framework for regulating transborder data flows.[73] It prevents the signatories from prohibiting transborder flows of applicable data solely on the basis of privacy protection.[74] It does provide an exception for signatory nations that have "specific regulations for certain categories of personal data,"[75] permitting nations providing such specific regulations to block the transfer of data to nations that

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Human Rights Convention, *supra* note 65, art. 10;

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Covenant on Rights, *supra* note 67, art. 19.

72. The report notes that article 8 of the Human Rights Convention does offer privacy protection as a basic human right. Explanatory Report, *supra* note 57, § 19.

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well–being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Human Rights Convention, *supra* note 65, art. 8.

73. *See* Convention, *supra* note 1, art. 12.

74. *Id*. art. 12(2).

75. *Id.* art. 12(3)(a).

lack equivalent levels of protection.[76] A nation may also prohibit exportation of data to an intermediary intended for re–export to a non-complying third nation.[77]

The Convention does not directly prohibit data transfers to non-signatory nations.[78] Article 23, however, does provide for accession to the Convention by non-member states.[79] In addition, the Explanatory Report suggests "[i]t does not seem advisable . . . to rely solely on the European Human Rights Convention for data protection, *inter alia*, because it is a 'closed' instrument, which does not permit the participation of non–European and non–member States."[80] It is clear from the language in these provisions that the Council intended the Convention to apply to exports of data to non-signatory nations, and the Convention has been interpreted in a consistent manner.[81]

The limitations on data collection and processing rights, combined with the potential impact on non-signatory nations, make the Convention an important step toward a unified European data protection policy. Taken together with the OECD Guidelines, a framework was now in place to consider comprehensive data protection legislation.

IV. THE DATA PROTECTION DIRECTIVE

By 1995, most European nations had data protection legislation in place.[82] The data protection commissioners of the European Union's member states issued a resolution for the creation of a single, binding standard for all E.U. members.[83] The pressure stemmed from the explosion in transactions of personal data between member states[84] and the desire for "the

76. *See id*.; *see also* Directive, *supra* note 14, art. 25.

77. Directive, *supra* note 14, art. 25.

78. Schwartz, *supra* note 51, at 478; *see also* Convention, *supra* note 1, art. 12.

79. Convention, *supra* note 1, art. 23.

80. Explanatory Report, *supra* note 57, § 19.

81. *See* Schwartz, *supra* note 51, at 478.

82. *See id*. at 474-77. *See also* DATA PROTECTION IN THE EUROPEAN UNION: THE STATUTORY PROVISIONS (Simitis et al. eds. 1992).

83. Schwartz, *supra* note 51, at 480.

84. *Id*. at 481.

establishment of common standards securing in the interest of the citizens' fundamental rights . . . a 'high level' of protection was no less categorically sought."[85]

The European Commission, the European Union's executive body,[86] proposed and amended several directives creating comprehensive data protection legislation.[87] In 1995, the European Parliament approved a final version, Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Directive).[88]

The Directive is intended to "harmonize" national data protection legislation,[89] a term of art in the European Union meaning "formal attempts" to homogenize laws of Member Nations, and establish "a basic structure . . . to which member states must conform."[90] The Directive is a legally binding document for all fifteen Member Nations of the European Union.[91]

Article 2 of the Directive is a comprehensive definition section.[92] "Personal data" is "any information relating to an identified or identifiable natural person . . . ."[93] An "identifiable person," undefined in the Guidelines[94] and the Convention,[95] is a

85. Spiros Simitis, The EU Directive on Data Protection and the Globalization of the Processing of Personal Data (Summary), *available at* http://www.privacyexchange.org/iss/confpro/bcsimitis.html (last visited Jan. 12, 2001).

86. European Commission, Role of the European Commission, *at* http://europa.eu.int/comm/role_en.htm (last visited Jan. 11, 2001). The Commission 1) initiates Community policy and represents the general interest of the European Union, 2) acts as the guardian of the E.U. treaties to ensure that European legislation is applied correctly, and 3) manages policies and negotiates international trade and cooperation agreements. *Id*.

87. Myers, *supra* note 46, at 118-19.

88. Directive, *supra* note 14.

89. Schwartz, *supra* note 51, at 481.

90. GEORGE A BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 430 (1993).

91. *Id*. at 480-81.

92. Directive, *supra* note 14, art. 2.

93. *Id*.

94. *See* Guidelines, *supra* note 11, § 1.

95. *See* Convention, *supra* note 1, art. 2.

person:

> who can be identified, directly or indirectly, . . . by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[96]

The Directive covers the "processing" of all such personal data, which includes operations such as:

> collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[97]

As one commentator suggests, "[g]iven the expansive definitions . . . it is difficult, if not impossible, to conceive of any personally identifiable information or use of that information that would not be theoretically governed by laws adopted in accordance with the Directive."[98]

Article 2 sets out two more important definitions.[99] A "controller" is "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."[100] Thus the Directive applies to data collection and privacy in both the public and the private sectors.

The "data subject's consent" is "any freely given specific and informed indication of [a data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed."[101] The definition is open ended as to when consent must be given, and in what manner, as well as whether consent must be obtained upon each reprocessing of the subject's data; some of these gaps are filled by article 7 of the Directive, as discussed below.

Article 6 of the Directive establishes broad principles of data

---

96. Directive, *supra* note 14, art. 2.

97. *Id*.

98. James Harvey, *An Overview of the European Union's Personal Data Directive*, 15 COMPUTER LAW. 19, 20 (1998).

99. Directive, *supra* note 14, art. 2.

100. *Id*.

101. *Id*.

quality.[102] It expressly provides that personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected;
- accurate and, where necessary, kept up-to-date;
- erased or corrected if inaccurate or incomplete;
- kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data was collected or for which they are further processed.[103]

These quality restrictions are far broader than the principles set out in the OECD Guidelines.[104] They reflect two value judgments: that processing and collection rights are limited, and that individuals have the right to control the accuracy and breadth of the data.[105] These two ideas give the Directive a broader scope than any previous data protection agreement.[106] The Guidelines and the Convention framed the issue of data protection around individual rights as a method to synchronize national data protection legislation and simplify the transborder flows of personal data;[107] the Directive reframes the data protection issue solely in terms of individual liberties.[108]

---

102. *See id*. art. 6.

103. *Id*.

104. *Compare* Guidelines, *supra* note 11, §§ 7-14 (stating specific provisions defining each principle), *with* Directive, *supra* note 14, art. 6 (leaving greater room for interpretation).

105. *See* Directive, *supra* note 14, art. 6; *see also* NIMMER, *supra* note 7, ¶ 8.25[3].

106. *See* Harvey, *supra* note 98, at 19-20 ("[I]t is difficult, if not impossible, to conceive of any personally identifiable information or use of that information that would not be theoretically governed by laws adopted in accordance with the Directive.").

107. See discussion, *supra* notes 71-72, and accompanying text.

108. *See* Simitis, *supra* note 85, ¶ 4 ("The OECD sees in the proposed rules first and foremost a means permitting to soothe the growing apprehensions and to secure thus an unhindered expansion of the computer industry. The Council of Europe . . . attenuates its range by obscure and confusing references to the free flow of informations

In the Directive, the data subject becomes the primary focus, and the principles of narrow usage and collection of data and broad rights of control create a new paradigm for data protection.[109] As Professor Spiros Simitis states, data protection had become "the touchstone for the credibility of the [U]nion's explicit commitment to the respect and the implementation of the fundamental rights of its citizens."[110]

Article 7 of the Directive is titled "Criteria for Making Data Processing Legitimate."[111] It requires the "unambiguous consent" of the data subject as a precondition for processing.[112] As an E.U. explanatory report suggests, the data subject must agree "freely and specifically" to all potential uses of his personal data, and may do so only after being adequately informed of such uses by the collector.[113] Personal data may be processed without consent only if necessary to fulfill a contractual or other legal obligation, to protect the "vital interests of the data subject," or if in the public interest.[114]

Interpreted in its broadest sense, this requirement of unambiguous consent suggests that each new use of personal data requires the authorization of the data subject. Article 7 may stop the use of data passively collected by a company in the course of doing business for other purposes, and could alter the ability of electronic commerce businesses to profile customers, personalize information and track behavior.[115]

Articles 10 and 11 of the Directive require certain information be provided to the data subject.[116] Article 10 governs

---

[*sic*].").

109. *See id*. ¶ 8 ("The Directive may, thus, not be the first attempt to internationalize data protection, but it definitely marks, compared to both the OECD rules and the council of Europe convention [*sic*], a qualitative change.").

110. *Id*. ¶ 6

111. Directive, *supra* note 14, art. 7.

112. *Id*.

113. European Union, Data Protection: Background Information, Nov. 3, 1998, *at* http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm [hereinafter Background Informa-tion].

114. Directive, *supra* note 14, art. 7.

115. Harvey, *supra* note 98, at 20.

116. Directive, *supra* note 14, arts. 10-11.

data collected from the subject.[117] The Controller must provide 1) his identity to the data subject, 2) the purposes of the processing for which the data are intended, 3) information regarding recipients of the personal data, 4) whether replies to questions are obligatory or voluntary, and 5) the existence of the right of access to and the right to correct the personal data concerning the subject.[118] Article 11 extends these requirements to personal data not gathered directly from a data subject.[119]

Article 12 grants data subjects a right of access to data.[120] It requires that every data subject have the right to obtain confirmation that data relating to him is being processed and the purposes of such processing, the categories of the data, and the recipients.[121] It also requires that the data itself be available in an intelligible form, with the rectification, erasure or blocking of incorrect or incomplete data by the data subject as appropriate.[122]

The Directive enforces these individual liberties by requiring that Member Nations adopt a private right of action for violations.[123] Article 22 requires that Member States "provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question."[124] Article 23 adds that "any person who has suffered damage as a result of an unlawful processing operation . . . is entitled to receive compensation from the [C]ontroller for the damage suffered."[125] Article 24 requires Member States to "lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this

117. *Id*. art. 10.

118. *Id*.

119. *Id*. art 11. Article 11 does not extend the duty of the Controller to inform the data subject whether replies to the questions are obligatory because the data are not gathered directly from the subject, thus the data subject has already answered any questions, and the issue is moot. *See id.*

120. *See id*. art. 12.

121. *Id*.

122. *Id*.

123. *Id.* arts. 22-24.

124. *Id*. art. 22.

125. *Id*. art. 23.

Directive."[126]

One of the most important and far–reaching principles advanced by the Directive is a change in focus on the transfer of data between Member Nations and third countries which have not adopted the Directive.[127] Article 25 allows a transfer of personal data for processing to a non-member country only if the country "ensures an adequate level of protection."[128] This was a major shift; a majority of national data protection laws subjected transfers to an "equivalency" standard,[129] perhaps reflecting the goals of the Convention and Guidelines as discussed above of easing the economic impact of transborder data restrictions. The Directive, with its stronger principles of data quality and control by the subject, strengthens these standards.

The adequacy of the protection is "assessed in the light of all the circumstances surrounding [the] transfer," including:

- the nature of the data,
- the purpose and duration of the proposed processing operations,
- the country of origin and final destination,
- the rules of law, both general and sectoral, in the third country in question, and
- the professional rules and security measures complied with in that country.[130]

If a third country does not ensure an adequate level of protection as determined by the Commission, Member States are required by the Directive to "take the measures necessary to prevent any transfer of data of the same type."[131]

Article 26 allows very limited exceptions to the adequacy

---

126. *Id*. art. 24.

127. *See id*. arts. 25-26; *see also* Peter Blume, *An EEC Policy for Data Protection*, 11 COMPUTER L.J. 399, 417-18 (1992) (discussing the potential political sensitivity of the issue as it reflects a policy supporting "Fortress Europe" and the possibility that the Directive may become a major incentive for the United States to enact comprehensive data protection legislation).

128. Directive, *supra* note 14, art. 25.

129. Schwartz, *supra* note 51, at 480.

130. Directive, *supra* note 14, art. 25

131. *Id*.

requirements.[132] These are very similar to the exceptions in article 7 for the processing of data without consent.[133] Article 26 allows transfers to states that do not meet the adequacy requirements of article 25 if the data subject has given unambiguous consent, if the transfer is necessary for the public interest (presumably national security), or for the exercise of a legal claim, or if the transfer is necessary to protect the vital interests of the subject.[134]

One important exception to article 26 concerns the potential use of contract to ensure the basic principles of data quality and control.[135] Article 26 permits a transfer if:

> the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights such safeguards may in particular result from appropriate contractual clauses.[136]

The possible impact of the adequacy standards was not lost on observers who suggested a potential "blackout" in data flows between the European Union and the rest of the world[137] or a prospective "trade war" over the standard.[138] The European Union responded that "[t]he aim of the Directive is to promote the flow of information, not impede it . . . . By setting a high standard, the Directive fosters consumer confidence and thus encourages the development of electronic commerce."[139] By November 2000, Belgium, Denmark, Spain, Greece, Italy, The Netherlands, Austria, Portugal, Sweden, Finland, and the United Kingdom had implemented national legislation in

---

132. *Id*. art. 26.

133. *Id*. art. 7.

134. *Id*. art. 26.

135. *Id*.

136. *Id*.

137. *See* Susan Binns, Technical Briefing for Journalists on Data Protection—EU/US Dialogue, Dec. 10, 1998, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/euus.htm (last visited Nov. 5, 2001).

138. *Id*.

139. *See* European Commission, Data Protection: Background Information, Nov. 3, 1998, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm.

conformance with the Directive, and all of the other Member States had either submitted legislation or were awaiting its entry into force.[140]

V. UNITED STATES DATA PROTECTION AND THE SAFE HARBOR

As the Data Protection Directive neared implementation in 1998, the European Union began to pressure the United States into adopting either the Directive or its own comprehensive data protection scheme.[141] As data protection commissioner Spiros Simitis said, "[d]on't imagine for a moment that you can get away with paying lip service to privacy. Europe requires a régime of real protection. That is the new global position."[142]

The United States felt the pressure applied by the Europeans; U.S. businesses pressed for non–legislative solutions such as contracts and self–regulation.[143] Meanwhile, technologists set out to develop informational privacy mechanisms hoping to meet Directive standards.[144] When asked about the formation of a U.S. data protection authority, as article 28 of the Directive requires,[145] Ira Magaziner, the Clinton administration technology adviser, responded "We don't recognize the validity of that approach . . . . We would say the U.S. has equivalent privacy protection. I don't believe it is lesser. I believe it is different."[146]

The source of this showdown is the lack of comprehensive and coherent data protection law in the United States.[147] The

---

140. *See* European Commission, Data Protection: Status of Implementation of Directive 95/46, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm (last visited Oct. 15, 2001).

141. *See* Simon Davies, *Europe to U.S.: No Privacy, No Trade*, WIRED NEWS, May 1998, *available at* http://www.wired.com/wired/archive/6.05/europe_pr.html.

142. *Id*.

143. *See id*.

144. *See id*.

145. Directive, *supra* note 14, art. 28.

146. Davies, *supra* note 141.

147. *See generally* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW xv-1 (1996) (outlining U.S. data protection methods and indicating that U.S. data protection practices are generally not as thorough as those of Europe); s*ee also* NIMMER, *supra* note 7, ¶¶ 8.01-8.24 (noting that U.S. statutory privacy protection is piecemeal at best).

Constitutional right to privacy in the United States relates solely to government intrusion into private matters.[148] Data privacy restrictions relating to private entities are covered by a collection of tort law[149] and federal regulations.[150]

The United States has proven historically resistant to the adoption of comprehensive data protection legislation.[151] The U.S. business community and Congress instead looked to self-regulation to provide adequate data protection.[152] External pressures including the rapid development of new technologies easing the ability to collect and transfer personal data,[153] along with the more direct need for new regulations occasioned by the Directive,[154] pressed the United States into action.

The Department of Commerce began negotiations with the European Commission upon the entry into force of the Data Directive.[155] They reached an agreement issued by the Department of Commerce on July 21, 2000 called "Safe Harbor

148. *See*, *e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485 (1965); Katz v. United States, 389 U.S. 347, 350 (1967).

149. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977). The Restatement defines four unique torts: 1) intrusion on the right of publicity (based on the appropriation of an individual's name or likeness); 2) intrusion into an individual's private affairs; 3) public disclosure of embarrassing private facts; and 4) publicly placing the individual in a false light. *Id*.

150. Most federal regulations are context specific, relating either to the nature of the information sought or the class of individuals covered. *See*, *e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2000) (regulating the acquisition and use of personal data by federal agencies); Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq*. (1994) (regulating collection, communication and disclosure of consumer credit reports); Family Educational and Privacy Rights Act, 20 U.S.C. § 1232(g) (1994) (restricting disclosure of student educational records); and Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1994) (prohibiting disclosure of consumer video rental histories).

151. Reidenberg, *supra* note 3, at 500.

152. *Id*. at 498. Reidenberg suggests that businesses may develop personal information standards from "(a) the[ir] technical network structure, (b) industry codes of conduct, (c) company policies, (d) contractual arrangements, and (e) pressures for good corporate citizenship." *Id*. at 509.

153. *See* Andy Walton, *E–Business vs. 'None of Your Business': The U.S. and E.U. Have Agreed on "Safe Harbor" Privacy Protection. But is it Really Safe?*, June 9, 2000, *at* http://www.cnn.com/SPECIALS/2000/e.europe/stories/privacy/; *see also* discussion *supra* notes 31 and 59 and accompanying text.

154. *See* Reidenberg, *supra* note 3, at 498-99.

155. James A. Harvey and Karen M. Sanzaro, *An Overview of the Proposed Safe Harbor Privacy Requirements*, 17 COMPUTER LAW. 19 (2000).

Privacy Principles" (Safe Harbor).[156]

The Safe Harbor is designed to create a presumption of adequacy for U.S. organizations receiving personal data from European nations,[157] as required by Article 26 of the Data Directive.[158] The Safe Harbor is based on seven Principles[159] supplemented by a Frequently Asked Questions document[160] (FAQ).

The seven Safe Harbor principles are:

- *Notice*: requires clear and conspicuous disclosure before data collection of the purposes and uses of data collection, contact information, the types of third parties to whom the data is disclosed, and the choices offered for limiting use and disclosure.
- *Choice*: requires the organization provide an opportunity to "opt–out" of data disclosures to third parties or data used for a purpose other that the one it was originally collected for. Sensitive information requires an opt–in choice.
- *Onward Transfer*: requires application of the Notice and Choice provisions listed above before transfer to a third party.
- *Security*: requires reasonable precautions against loss and unauthorized access.
- *Data Integrity*: requires personal data be relevant for the purposes for which it is used.
- *Access*: requires providing access to individuals and the ability to correct, amend or delete inaccurate information.
- *Enforcement*: requires mechanisms for assuring

156. United States Dep't of Commerce, Safe Harbor Privacy Principles, (July 21, 2000), *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm [hereinafter Safe Harbor].

157. *Id*.

158. Directive, *supra* note 14, art. 26.

159. Safe Harbor, *supra* note 156.

160. United States Dep't of Commerce, Safe Harbor Documents, Frequently Asked Questions (FAQs) (July 21, 2000), *available at* http://www.export.gov/safeharbor/sh_documents.html [hereinafter FAQ].

compliance.[161]

A quick examination of these principles shows they match neatly with both the OECD Guidelines[162] and the Council of Europe Convention,[163] but do not match the broad restrictions on use and access provided by the Directive.[164] The irony in potentially inadequate adequacy standards was not lost on the European Working Party on the Protection of Individuals with Regard to the Processing of Personal Data,[165] which released an opinion in May 2000 noting that it was "particularly concerned to see . . . further improvements of the principles."[166]

Safe Harbor provides three methods for an organization to adhere to the Principles.[167] The organization may qualify by "joining a self-regulatory privacy program that adheres to the Principles, . . . developing [its] own self-regulatory privacy policies provided that they conform with the Principles,"[168] or if it is "subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy."[169]

At present, U.S. organizations may qualify only through one of the first two methods.[170] The European Commission has not approved model contract provisions,[171] and has not approved any

---

161. Safe Harbor, *supra* note 156.

162. Guidelines, *supra* note 11, §§ 7-14.

163. Convention, *supra* note 1, art. 5, 7.

164. *See* Directive, *supra* note 14, arts. 1-24.

165. Directive articles 29 and 30 require the commission of an advisory committee to "give the Commission an opinion on the level of protection in the Community and in third countries." *Id*. art. 30.

166. Data Protection Working Party, Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles", (May 16, 2000) *available at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32en.htm [hereinafter Opinion].

167. Safe Harbor, *supra* note 156.

168. *Id*.

169. *Id*.

170. Harvey and Sanzaro, *supra* note 155, at 19.

171. *Id*. Note that article 26 of the Directive permits a transfer if "the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights such safeguards may in particular result from appropriate contractual clauses." Directive, *supra* note 14, art. 26. As of this writing, the Commission

U.S. law as containing sufficient standards for certification.[172]

Safe harbor protection starts on the date an organization self-certifies to the Department of Commerce.[173] When an organization joins, it agrees to continue to apply the Safe Harbor Principles "for as long as [it] stores, uses, or discloses [such data], even if it subsequently leaves the safe harbor."[174] An organization is not required to subject all personal data transfers to the Principles, but after it joins it must subject all data transfers from the European Union to these Principles.[175]

The Principles provide exceptions if necessary: 1) to meet public interest requirements; 2) where statutes, government regulations or case law create conflicting obligations or explicit authorizations; or 3) where the effect of the Directive or a Member State's law is to allow exceptions, to be applied in comparable contexts.[176]

The European Union recognizes two U.S. government bodies as qualified to investigate non-compliance and obtain relief for misrepresentations of adherence to Safe Harbor.[177] These are the Department of Transportation, on the basis of its authority to investigate and remedy unfair trade practices,[178] and the Federal Trade Commission, under the same authority.[179] Adherence with the Safe Harbor through self-certification is accomplished by requiring organizations to register yearly with the Department of Commerce.[180]

---

has not promulgated a model for adherence, and contract–based adherence standards will be judged on a case–by–case basis. *Id*.

172. Harvey and Sanzaro, *supra* note 155, at 19.

173. Safe Harbor, Frequently Asked Questions (FAQs), FAQ # 6—Self–Certification, *available at* http://www.Export.gov/safeharbor/FAQ6SelfCertFINAL.htm (last visited Mar. 13, 2002) [hereinafter FAQ 6].

174. *Id*.

175. *Id*.

176. Safe Harbor, *supra* note 156.

177. Safe Harbor Annex, List of U.S. Statutory Bodies Recognized by the European Union, *available at* http://www.export.gov/safeharbor/ANNEX.htm (last visited Mar. 13, 2002) [hereinafter Annex].

178. Annex, *supra* note 177; s*ee also* 49 U.S.C. § 41712 (1994).

179. Annex, *supra* note 177; s*ee also* Federal Trade Commission Act, 15 U.S.C. § 45 (1994).

180. FAQ # 6, *supra* note 173.

The Department of Commerce will maintain and make available a list of all organizations submitting self-certification letters.[181] All organizations that self–certify must also include a notice of adherence in their privacy policies.[182] Currently, only thirty U.S. organizations have filed letters of self-certification.[183] The Commerce Department has scheduled a series of seminars to encourage participation, stressing the importance of Safe Harbor and the ease of self-certification and compliance.[184]

The Safe Harbor Principles do not match the breadth and depth of the Data Protection Directive.[185] They replace the Directive's principles of limited collection and use as a fundamental right with an opt-out provision; the data subject is granted a lower degree of control over his personal data.[186] The opt-in provision for sensitive data is weakened by limits on the provision of an opt-in choice for certain categories of sensitive data.[187]

The access rights provided by the Directive[188] and Safe Harbor[189] are also widely divergent. Consider, for example, the following from the FAQ:

> [E]xperience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand

181. *Id*.

182. *Id*.

183. *See* United States Department of Commerce, Safe Harbor List, *available at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Mar. 13, 2002).

184. *See* Declan McCullagh, *Safe Harbor is a Lonely Harbor*, WIRED NEWS, Jan. 5, 2001, *at* http://www.wired.com/news/print/0,1294,41004,00.html.

185. *See* Directive, *supra* note 14, art. 6; *and* Safe Harbor, *supra* note 156.

186. *See* Safe Harbor, *supra* note 156.

187. Safe Harbor, Frequently Asked Questions (FAQs), FAQ 1: Sensitive Data, *available at* http://www.export.gov/safeharbor/FAQ1sensitivedataFINAL.htm (last visited Mar. 13, 2002) [here-inafter FAQ #1].

188. *See* Directive, *supra* note 14, arts. 10-11

189. Safe Harbor, Frequently Asked Questions (FAQs), FAQ 8: Access, *available at* http:// www.export.gov/safeharbor/FAQ8accessFINAL.htm (last visited Mar. 13, 2002) [hereinafter FAQ #8].

> the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.[190]

Compared with the broad rights of access granted by the Directive in article 11,[191] the access rights promulgated by the Safe Harbor fall short. The FAQ cites the Explanatory Report to the OECD Guidelines in stating "an organization's access obligation is not absolute."[192] But, as the Explanatory Report also suggests, "[t]he right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard."[193]

VI. CONCLUSION

The Safe Harbor agreement is consistent with the protections afforded by the OECD Guidelines and the Council of Europe Convention, both proposed in the early 1980s.[194] Since then, public demand for better data protection legislation in the European Union, and its need to harmonize such legislation[195] have resulted in broad limitations on the collection and use of personal data in the European Union.

The Safe Harbor, designed to ease U.S. concerns with compliance to the Directive,[196] is not succeeding in its appointed

---

190. *Id*.

191. *See* Directive, *supra* note 14, art. 11.

192. *See* FAQ # 8, *supra* note 189 (requiring greater disclosure to the data subject of the purposes for the personal data use).

193. Guidelines, *supra* note 11, § 58.

194. *See* Guidelines, *supra* note 11; Convention, *supra* note 1.

195. *See* Marc Rotenberg, The European Union Data Directive and Privacy, Testimony and Statement Before the Committee on International Relations, U.S. House of Representatives (May 7, 1998), *available at* http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html [hereinafter "Rotenberg"]. "[The Directive] grew out of specific circumstances related to the integration of the European economies and the need to harmonize national privacy laws. It also reflects a widely held belief that privacy is a fundamental human right, entitled to full protection in law." *Id*.

196. *See* Safe Harbor, *supra* note 156.

task.[197] U.S. organizations may be waiting for the Working Party to promulgate model contracts for data protection adequacy, but in the interim adoption of the Safe Harbor will continue to be very slow.

Absent comprehensive data protection legislation, or the creation of a U.S. data protection authority,[198] the Safe Harbor is likely to continue to face struggles in adoption. While less onerous than the Directive, and offering easy compliance,[199] the Safe Harbor offers little incentive for certification and individual privacy rights far less substantial than its European counterparts.

However, the approach to data protection in the United States may pose significant hurdles to the adoption of a more stringent data protection standard.[200] While the European standards find their inspiration in the preservation of a right to privacy,[201] the U.S. model continues to be based on a concept of limited government involvement in the marketplace, and the substitution of private agreements for regulation.[202]

The continued promulgation of sector-specific privacy legislation by the United States and the self-regulatory

---

197. *See* McCullagh, *supra* note 184.

198. The newly elected 107th Congress has made noises about enacting more privacy legislation. *See* John Gartner, *New Congress to Push Privacy*, WIRED NEWS, Jan. 7, 2001, *at* http:// www.wired.com/news/print/0,1294,40965,00.html.

199. Organizations may check self–certifications online. *See* United States Dep't of Commerce, Safe Harbor Workbook, *available at* http://www.export.gov/SafeHarbor/sh_workbook.html (last visited Mar. 13, 2002).

200. *See* Reidenberg, *supra* note 3, at 503.

> The constitutional emphasis on protection against the government formed the basis of a legal canon that enshrines free flows of information and minimal restrictions on the treatment of information. . . . The prevailing U.S. doctrine for the treatment of personal information does not look to the positive use of regulation to secure such freedom. To ensure information is freely available, American courts have long been committed to the "marketplace of ideas." Under this canon, democracy functions best when ideas, no matter how well founded or repugnant, vie openly for acceptance in society.

Id.

201. *See* discussion *supra* notes 70-72 and accompanying text.

202. Reidenberg, *supra* note 3, at 501.

approach are not likely to soothe the European Union's concerns.[203] A potential solution may exist in the need for international standards and uniformity to lower transaction costs for U.S. companies.[204] As Professor Reidenberg comments,

> The call for standards of fair information practice is not a call for interventionist or intrusive government regulation . . . . Instead, the call for standards is a call to equalize the playing field. In an Information Society, the private sector has not satisfactorily handled the making of norms through technical or corporate sources.[205]

The Guidelines and Convention were promulgated in part through the cooperation of government agencies and companies concerned with streamlining varying standards of data protection across Europe. The Safe Harbor, motivated in large part by the increased pressure created by the Directive, may yet succeed as a device designed to provide the same basic standards for both data subjects and collectors.

*Mike Ewing**

203. *See* discussion *supra* notes 159-168 and accompanying text.

204. *See* Rotenberg, *supra* note 195. "I think the problems with the sectoral approach will become increasingly apparent as commerce on the Internet grows. The Internet offers the ideal environment to establish uniform standards to protect personal privacy. For the vast majority of transactions, simple, predictable, uniform rules offer enormous benefits to consumers and businesses." *Id*.

205. Reidenberg, *supra* note 3, at 551.

* This Comment received the Baker & Mackenzie (Houston) Writing Award.