"SAFE HARBOR" AND THE EUROPEAN UNION'S DIRECTIVE ON DATA PROTECTION

Jordan M. Blanke[*]

I. Introduction
II. Background
III. The Directive
IV. Transfer of Personal Data to Third Countries
V. Data Protection Law in the United States
VI. Self-Regulation
A. Notice/Awareness
B. Choice/Consent
C. Access/Participation
D. Integrity/Security
E. Enforcement/Redress
1. Self-Regulation
2. Private Remedies
3. Government Enforcement
VII. Safe Harbor Principles

I. INTRODUCTION

After two years of negotiation, the United States Department of Commerce (DOC) and the European Union have agreed upon a set of Safe Harbor Privacy Principles (Safe Harbor). While it is not as rigorous as many privacy advocates had hoped it would be, there is no doubt that the negotiations and the efforts of many United States companies to forestall potential government regulation by adopting more well-defined privacy policies have focused more attention on information privacy and fair information practices.

In October 1998, the European Union's Directive on Data

[*] Professor of Computer Information Systems and Law, Stetson School of Business and Economics, Mercer University, Atlanta, Georgia.

Protection (Directive)[1] became effective. It includes a provision permitting the transfer of personal data[2] to a non-European Union country only if that country "ensures an adequate level of protection."[3] In order to avoid any disruption in the flow of such data, the DOC began negotiations with the European Commission.[4] The goal was a set of "safe harbor" principles, under which United States companies adopting them would be able to continue to self-regulate their privacy policies. This paper discusses the development and requirements of these "safe harbor" principles.

II. BACKGROUND

While most Americans probably would consider privacy to be a basic and fundamental right, United States law provides very little uniform protection for personal data. While specific laws do protect some of this information, they generally apply to public, rather than private institutions, or are sectoral in application. In contrast, laws and regulations in Europe are far more extensive than those in the United States with respect to the protection of personal data.[5] In fact, the term "data protection" is a well-

[1] EUR-Lex: Community Legislation in Force, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995 O.J. (L 281) 31 (last modified Nov. 3, 1999) <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html> [hereinafter Directive].

[2] "Personal data" is a term of art defined in the Directive as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity." *Id*. at art. 2(a).

[3] *Id*. at art. 25(1).

[4] The European Commission is made up of twenty members, two each from France, Germany, Italy, Spain and the United Kingdom, and one from each of the other member states. According to the European Union Web site, the Commission has three distinct functions: initiating proposals for legislation; guarding of Treaties; and being the manager and executor of Union policies and of international trade relationships. *The European Commission—The Driving Force for European Union,* (visited Dec. 17, 2000) <http://europa.eu.int/inst/en/com.htm>.

[5] For excellent discussions of data protection in Europe, *see* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997); PETER P. SWIRE & ROBERT E. LITAN,

known and well-defined term familiar to the average European.[6]

In 1980 the Organization for Economic Cooperation and Development (OECD)[7] issued what was then one of the most comprehensive policy statements on data protection and privacy. In its *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines),[8] the OECD set forth many of the basic principles still evident today in data protection laws:

> Collection Limitation Principle
>
> 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> Data Quality Principle
>
> 8. Personal data should be relevant to the purposes for which they

NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998); and PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996). The latter work was produced as a result of a request by the European Commission to the authors to conduct a study of U.S. data protection law. *See also* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1 (1999).

[6] *See* SCHWARTZ & REIDENBERG, *supra* note 5, at 5.

[7] *See About OECD – What is OECD* (last modified June 11, 2000) <http://www.oecd.org/about/general/index.htm>. The OECD is a group of 29 member countries, including the United States, Canada, Japan and most European countries. According to a statement on its Web site, it is

> an organisation that, most importantly, provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experiences, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalised world must form a web of even practice across nations. Their exchanges may lead to agreements to act in a formal way - for example, by establishing legally-binding codes for free flow of capital and services, agreements to crack down on bribery or to end subsidies for shipbuilding. But more often, their discussion makes for better informed work within their own governments on the spectrum of public policy and clarifies the impact of national policies on the international community. And it offers a chance to reflect and exchange perspectives with other countries similar to their own.

Id.

[8] *Organization for Economic Cooperation and Development (OECD), Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980) (visited Dec. 19, 2000) <http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/priv.htm>

are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

(a) with the consent of the data subject; or

(b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him

(i) within a reasonable time;

(ii) at a charge, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with

measures which give effect to the principles stated above.[9]

While these OECD Guidelines were not binding, they were very influential, particularly in Europe. In 1981, the Council of Europe[10] recommended for adoption by its member states a convention,[11] providing for data protection consistent with the OECD Guidelines. Many of the member countries ratified the convention and enacted appropriate legislation. However, before all member countries could do so, the European Community, now known as the European Union (EU),[12] was created. In 1995, the EU adopted the Directive.[13]

III. THE DIRECTIVE

In addition to "personal data,"[14] the Directive defines several other important terms. "Processing of personal data" or, simply "processing," is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means. . ."[15] 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

---

[9] *Id.*

[10] *See About the Council of Europe* (visited Dec. 19, 2000) <http://www.coe.fr/eng/present/about.htm>. The Council of Europe now has 41 member states. According to a statement on its Web site,

> Its main role is to strengthen democracy, human rights and the rule of law throughout its member states. The defence and promotion of these fundamental values is no longer simply an internal matter for governments but has become a shared and collective responsibility of all the countries concerned. The Council of Europe is also active in enhancing Europe's cultural heritage in all its diversity. Finally, it acts as forum for examining a whole range of social problems, such as social exclusion, intolerance, the integration of migrants, the threat to private life posed by new technology, bioethical issues, terrorism, drug trafficking and criminal activities.

Id.

[11] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Council of Europe, Europ. T.S. No. 108.

[12] The fifteen member countries of the European Union are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom.

[13] *See* Directive, *supra* note 1.

[14] *Id.* at art. 2(a).

[15] *Id.* at art. 2(b).

processing of personal data."[16] A "processor" is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."[17]

The Directive does not apply to the processing of personal data in the course of an activity that falls outside the scope of EU law, such as public security, defense, state security, or enforcement of criminal law, nor does it apply to a natural person in the course of a purely personal or household activity.[18] The latter exclusion would apply, for example, where an individual maintains an address book with names and telephone numbers of friends.

The thrust of the Directive's data protection comes from Articles 6 and 7. Article 6 states:

> 1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.[19]

Article 7 addresses the issue of consent:

> Member States shall provide that personal data may be processed only if:
>
> (a) the data subject has unambiguously given his consent; or

[16] *Id.* at art. 2(d).
[17] *Id.* at art. 2(e).
[18] *See* Directive, *supra* note 1, at art. 3(2).
[19] *Id.* at art. 6.

> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (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 in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; 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 which require protection under Article 1 (1).[20]

Article 8 provides an even stricter requirement for so-called sensitive data. It states that "[m]ember States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[21]

There are several exceptions to this restriction. It does not apply if "the data subject has given his explicit consent to the processing," except where the applicable law may not permit such consent.[22] Thus, a country may decide not to allow even the data subject himself to consent to the processing of certain sensitive data. Other exceptions to Article 8(1) apply if the processing is necessary in order for the controller to meet obligations in the area of employment law, "is necessary to protect the vital interests of the data subject,"[23] is "carried out in the course of legitimate activities"[24] of a non-profit-seeking body, is necessary in order to establish or exercise legal claims, or "is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management

[20] *Id.* at art. 7.
[21] *Id.* at art. 8(1).
[22] *Id.* at art. 8(2)(a).
[23] Directive, *supra* note 1, at 8(2)(c).
[24] *Id.* at 8(2)(d).

of health-care services."[25]

When information is collected directly from the data subject, the controller or his representative must provide the data subject with (a) information about the identity of the controller, (b) the purposes of the processing, and (c) if necessary under the circumstances to guarantee fair processing of the information, (1) "the recipients or categories of recipients of the data," (2) whether the responses are "obligatory or voluntary," and (3) "the existence of the right of access and the right to rectify the data."[26]

When information is not obtained from the data subject, the controller or his representative must provide the data subject with substantially the same information as above, at the time of the recording of the data, or if a disclosure to a third party is envisioned, no later than the time when the data are first disclosed.[27]

Article 12 of the Directive addresses the right of access to the data:

> Member States shall guarantee every data subject the right to obtain from the controller:
>
> (a) 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 purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
>
> - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
>
> - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
>
> (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
>
> (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a

[25] *Id.* at arts. 8(2)(b)-(e) & 8(3).

[26] *Id.* at art. 10.

[27] *Id.* at art. 11(1).

disproportionate effort.[28]

The data subject is given the right to object, "free of charge, to the processing of data relating to him that the controller anticipates will be used for purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for direct marketing. . ."[29]

The Directive requires that generally controllers must notify the country's supervisory authority before carrying out any processing operation.[30] The notification must include (a) the name and address of the controller and his representative, (b) the purposes of the processing, (c) a description of the categories of data and data subjects, (d) the recipients or categories of recipients of the data, and (e) any proposed transfers of data to third countries,[31] such as any non-EU member country.

IV. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Of particular importance to the United States (and other non-EU member countries) are Articles 25 and 26. Article 25 provides that transfers of personal data to a third country can only be made if that country ensures an "adequate level of protection."[32]

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[33]

Article 26 provides for some exceptions or derogations where there is not an adequate level of protection.[34] Most notable are

[28] Directive, *supra* note 1, at art. 12.
[29] *Id.* at art. 14(b).
[30] *See id.* at art. 18(1).
[31] *See id.* at art. 19(1) (a)-(e).
[32] *Id.* at art. 25(1).
[33] Directive, *supra* note 1, at art. 25(2).
[34] *See* i*d.* at art. 26.

exceptions where (a) "the data subject has given . . . consent unambiguously," (b) the transfer of data is "necessary for the performance of a contract between the data subject and the controller," (c) the transfer of data is "necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party," (d) the transfer of data is "necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims," or (e) the transfer of data is "necessary in order to protect the vital interests of the data subject."[35] There is also an exception where the controller adduces adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals; such safeguards may result from contractual clauses.[36]

V. DATA PROTECTION LAW IN THE UNITED STATES

There is no comprehensive data protection law in the United States. This explains why the Directive requires only "adequate" protection as opposed to "equivalent" protection, which was the standard in early drafts of the Directive.[37] The recognition by the EU that the United States would probably never, and certainly not in the short term, have equivalent protection, along with the understanding of the importance of the free flow of data between the United States and the EU, required adoption of the less stringent standard.

In the United States, data protection laws are piecemeal. They generally apply to public institutions, rather than private ones.[38] There are some laws that regulate private institutions, but they are very sectoral, that is, they apply only to a specific industry or application.[39] Finally, there is some case law interpreting Constitutional protection that comes close to defining an area of information privacy law.[40]

---

[35] *Id.* at art. 26(1) (a)-(e).

[36] *See id*. at art. 26(2).

[37] *See* SWIRE & LITAN, *supra* note 5, at 33.

[38] *See infra* notes 41-58 and accompanying text (discussing the Freedom of Information Act and the Computer Matching and Privacy Act of 1988).

[39] *See infra* notes 59-68 and accompanying text (referring to the Fair Credit Reporting Act and Privacy Act of 1988).

[40] *See infra* notes 69-72 and accompanying text (discussing Whalen v. Roe, 429 U.S. 589 (1977)).

At the federal level, the Freedom of Information Act (FOIA)[41] and the Privacy Act[42] are the most important laws. However, they apply only to federal agencies.[43] The FOIA permits any person to obtain access to records maintained by federal agencies subject to several exceptions. Two of the exceptions provide for some degree of data protection. First, there is no access permitted for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[44] Second, access is denied for "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[45]

Similarly, the Privacy Act, while providing for many of the data protection principles enunciated in the OECD Guidelines and the Directive, applies only to records maintained by federal agencies. The Privacy Act (a) limits disclosure of records without consent of the individual,[46] (b) requires that records be kept of most disclosures,[47] (c) provides for a right of access to[48], and right to rectify, records,[49] and (d) requires that agencies shall (1) maintain records that contain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency,"[50] (2) "collect information to the greatest extent

41 5 U.S.C. § 552 (1994) (originally enacted in 1966 and re-titled in 1986).

42 5 U.S.C. § 552a (1994) (originally enacted in 1974 and re-titled the Computer Matching and Protection Privacy Act of 1988) .

43 An "agency" is defined as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." 5 U.S.C. § 552(f)(1) (Supp. IV 1999). This definition appears in the FOIA, but is specifically referenced by, and therefore applicable to, the Privacy Act. 5 U.S.C. § 552a(a)(1) (1994).

44 5 U.S.C. § 552(b)(6) (1994).

45 5 U.S.C. § 552(b)(7)(C) (1994).

46 5 U.S.C. § 552a(b) (1994).

47 5 U.S.C. § 552a(c) (1994) (requiring an accounting of the "date, nature, and purpose" of a disclosure and to whom such disclosures are made).

48 5 U.S.C. §552a(d)(1) (1994).

49 5 U.S.C. § 552a(d) (2) (B) (1994).

50 5 U.S.C. § 552a(e)(1) (1994).

practicable directly from the subject individual,"[51] (3) inform the individual from whom the information is sought[52] of (i) the authority for the solicitation,[53] (ii) the intended purposes of the information,[54] and (iii) the routine uses which may be made of it,[55] (4) make available "the title and business address of the agency official who is responsible for the system of records,"[56] (5) maintain the accuracy, relevance, timeliness, and completeness of the records "as is reasonably necessary to assure fairness to the individual,"[57] and (6) "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity."[58]

There are several federal laws that rather extensively provide for information privacy. However, they are all limited to specific sectors of business. The first and most important of these laws is the Fair Credit Reporting Act of 1970 (FCRA).[59] The FCRA regulates the collection and disclosure of information maintained by credit reporting companies in great detail.[60] It requires companies to implement "reasonable procedures to assure maximum possible accuracy" of the information maintained,[61] and provides an extensive procedure for individuals who wish to dispute the completeness or accuracy of any information in the file.[62] It also limits disclosure of any credit report.[63]

---

[51] 5 U.S.C. § 552a(e)(2) (1994).
[52] 5 U.S.C. §552a(e)(3) (1994).
[53] 5 U.S.C. §552a(e)(3)(A) (1994).
[54] 5 U.S.C. §552a(e)(3)(B) (1994).
[55] 5 U.S.C. § 552a(e)(3)(c) (1994).
[56] 5 U.S.C. § 552a(e)(4)(F) (1994).
[57] 5 U.S.C. § 552a(e)(5) (1994).
[58] 5 U.S.C. § 552a(e)(10) (1994).
[59] 15 U.S.C. §§ 1681 *et seq*. (1994).
[60] *Id.*
[61] 15 U.S.C. § 1681e(b) (1994).
[62] *See* 15 U.S.C. § 1681i (1994) (providing for reinvestigation by the consumer reporting agency in the case of a reported dispute. If "the reinvestigation does not resolve the dispute, the consumer may file a brief statement setting forth the nature of the dispute." Unless the statement is "frivolous or irrelevant," a note will be made on the consumer report and included with the report will be either a statement itself or "a clear and accurate codification thereof.").
[63] *See* 15 U.S.C. § 1681b (1994) (limiting the exclusive circumstances under which a consumer report may be issued to (1) a response to a court order; (2) upon the request of the consumer; (3) for use in connection with a credit

An example of a very narrow data protection law is the Video Protection Privacy Act of 1988, the so-called "Bork law."[64] This law was quickly passed by Congress in reaction to the release of information regarding the videotape renting habits of then-Supreme Court nominee Robert Bork.[65] This Act defines "personally identifiable information" as that "which identifies a person as having requested or obtained specific video materials or services. . ."[66] It permits disclosure of such information "to any person with the informed, written consent of the consumer given at the time the disclosure is sought."[67] It also permits disclosure of the name and address of a consumer if the consumer has had an "opportunity, in a clear and conspicuous manner, to prohibit such disclosure."[68] This ability to "opt-out" is becoming an important aspect of data protection law.[69]

Finally, there is some caselaw that suggests a constitutionally protected right of information privacy. In *Whalen v. Roe*,[70] a unanimous Supreme Court held that a centralized database, maintained by New York State, containing the names and addresses of all persons obtaining prescriptions for certain drugs did not violate the privacy of those individuals required to register.[71] The Court stated that among the various types of protected privacy interests is that of "avoiding disclosure of personal matters."[72] The Court held, however, that the state's

transaction; (4) when the report's intended use is for employment purposes; (5) in connection with underwriting the consumer's insurance; for "determination of consumer's eligibility for a license" or other governmentally regulated privilege and; other "legitimate business need[s] involving the consumer.").

64 18 U.S.C. § 2710 (1994); *see also* CATE, *supra* note 5, at 86 (stating that the Video Privacy Protection Act of 1988, was adopted because of Congress' disapproval of the disclosure of Judge Robert Bork's list of videos rented by him during his Supreme Court nomination).

65 *See* CATE, *supra* note 5, at 86.

66 18 U.S.C. § 2710(a)(3) (1994).

67 18 U.S.C. § 2710(b)(2)(B) (1994).

68 18 U.S.C. § 2710(b)(2)(D)(i) (1994).

69 *See generally* Federal Trade Commission, *Privacy Online: A Report to Congress* § III(A)(2) (1998) (visited Dec. 19, 2000) <http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair Information Practice Principles>.

70 429 U.S. 589 (1977).

71 *Id.* at 603-04.

72 *Id.* at 599 (citing Olmstead v. United States, 277 U.S. 438, 478 (1928), where Mr. Justice Brandeis stated that "the right to be let alone. . .[is]. . . the right most valued by civilized men"; also citing Griswold v. Connecticut, 381

interest under the circumstances outweighed the individual's interest.[73] It concluded:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[74]

While the Supreme Court has not again specifically addressed this issue, a number of lower courts have, with varying results.[75]

VI. SELF-REGULATION

Data protection in the private sector in the United States is achieved largely by self-regulation.[76] The evolution of these attempts at self-regulation is best observed today on the Internet and the World Wide Web. In the last couple of years, industry has tried to avoid possible legislation in this area by implementing more visible and effective privacy policies.[77]

The Federal Trade Commission has been examining online privacy issues since 1995. In its 1998 report, *Privacy Online: A Report to Congress* (1998 Report),[78] the FTC concluded that while most Web sites collected personal information from consumers, very few provided appropriate notice of their information practices, and fewer still provided comprehensive privacy

U.S. 479, 483 (1965), in which the Court created a First Amendment "penumbra where privacy is protected from governmental intrusion").

[73] *See id.* at 605.

[74] *Id.* at 605-06.

[75] For a further discussion of some of these cases, *see* CATE, *supra* note 5, at 63-64 (discussing the trends decisions of the various federal courts).

[76] *See Safe Harbor Letter from Ambassador Aaron* (last modified Apr. 19, 1999) <http://www.ita.doc.gov/td/ecom/aaron419.html>.

[77] *See generally* Stephen Labaton, *White House and Agency Split on Internet Privacy*, N.Y. TIMES, May 23, 2000, at C1. (discussing the political aspect of the internet privacy regulation and the conflict between private industry and government).

[78] Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) (visited Dec. 19, 2000) <http://www.ftc.gov/reports/privacy3/toc.htm>.

policies.[79]

The FTC, making specific reference to the OECD Guidelines and the Directive, identified the "five core principles of privacy protection"[80] and what it termed "fair information practices:"[81]

1. Notice/Awareness

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them . . . While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;
- identification of the uses to which the data will be put;
- identification of any potential recipients of the data;
- the nature of the data collected and the means by which it is collected if not obvious . . .;
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data . . .

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction. Such

---

[79] *See* Federal Trade Commission, *Privacy Online: A Report to Congress, § VI: Conclusion* (visited Dec. 19, 2000) <http://www.ftc.gov/reports/privacy3/conclu.htm> *(*noting that core principles of fair information practice require that consumers have notice of information practices, that they be given a choice with use and release of information collecting about them, that the be given access to their own personal information, and that appropriate security measures be employed).

[80] Federal Trade Commission, *Privacy Online: A Report to Congress, § III(A) Fair Information Practice Principles* (visited Dec. 19, 2000) <http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair Information Practice Principles> (listing the five core principles as: (1) notice/ awareness; (2) choice/ consent; (3) access/ participation; (4) integrity/ security; and (5) enforcement/ redress).

[81] *Id.*

secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer . . . .

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself—i.e., to view the data in an entity's files—and to contest that data's accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data .

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.

> a. Self-Regulation
>
> To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue. A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.
>
> Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed. Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.
>
> b. Private Remedies
>
> A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation . . . Important questions would need to be addressed in such legislation, *e.g.*, the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages; and the elements of any such cause of action.
>
> c. Government Enforcement
>
> Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers. Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.[82]

In its 1999 report, *Self-Regulation and Privacy Online: A Report to Congress* (1999 Report),[83] the FTC revisited the issue of self-regulation of privacy on the Internet. It noted the rising

---

[82] *Id.*

[83] Federal Trade Commission, *Self-Regulation and Privacy On-Line: A Report to Congress* (1999) (visited Dec. 19, 2000) <http://www.ftc.gov/os/1999/9907/privacy99.pdf> [hereinafter *Self-Regulation and Privacy On-Line*].

public concern about online privacy,[84] and the passage of the Children's Online Privacy Protection Act of 1998 (COPPA).[85] It also discussed in detail two extensive industry studies it commissioned, which showed generally, that while there was still a lot of room for improvement, progress had been made in bringing fair information practices to the World Wide Web.[86]

The FTC also discussed the emergence of online seal programs, such as TRUSTe[87] and BBBOnLine.[88] These programs encourage companies doing business on the Web to adopt privacy policies and join their respective programs. Both TRUSTe and BBBOnLine provide a wealth of information about privacy, as well as sample privacy policy statements.[89]

In its 2000 report, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (2000

[84] *See id*. at § I(B) (noting that as Internet use has increased, so has the concern for consumer privacy).

[85] *See id*. at § III; Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (1999).

[86] *See Self-Regulation and Privacy On-Line, supra* note 83, at § IV(A) (reporting that Professor Mary J. Culnan of the McDonough School of Business at Georgetown University directed the two industry-funded surveys. The first study, the Georgetown Internet Privacy Policy Survey, focused on 361 Web sites drawn from a list of the 7500 busiest servers on the World Wide Web. The second study, Privacy and the Top 100 Web Sites, concentrated on the 100 busiest Web sites, and was commissioned by the Online Privacy Alliance, a coalition of businesses and trade associations whose purpose is to encourage self-regulation. *See* Mary Culnan, *Georgetown Internet Privacy Policy Study* (last modified Aug. 9, 2000) <http://www.msb.edu/faculty/culnanm/gippshome.html>.
While the author of the reports emphasizes that comparisons between the FTC's 1998 Report and these studies cannot accurately be made because of the differing methodologies used in selecting the Web sites and analyzing their privacy policies, the FTC is nonetheless optimistic that progress was made during that year).

[87] *See id.* § IV(C)(1) (defining TRUSTe as an independent, non-profit organization, which has more than 500 licensees representing various industries).

[88] *See id.* at § IV(C)(2) (stating BBBOnLine is a subsidiary of the Council of Better Business Bureaus. BBBOnLine requires its customers to display a privacy policy that conforms with the programs information practices, and in exchange is allowed to post the BBBOnLine seal.).

[89] *See* TRUSTe*, TRUSTe: Building a Web You Can Believe In* (visited Dec. 19, 2000) <http://www.truste.org>; BBBOnline, Inc., *BBBOnline, Inc. – Promoting a Web You Can Believe In* (last modified Dec. 19, 2000) <http://www.bbbonline.com>.

Report),[90] the FTC changed direction and urged Congress to enact legislation that would set forth a basic level of privacy protection.[91] The 2000 Report cited numerous studies that indicated that self-regulation efforts are not keeping pace with the phenomenal growth of online business, and that consumers are not very confident about the quality of protection afforded their personal information.[92]

Specifically, the 2000 Report referenced surveys and studies finding that:

-67% of consumers were "very concerned" and 92% "concerned" about the misuse of their personal information online,[93]

-privacy concerns resulted in lost online retail sales of up to $2.8 billion in 1999 alone,[94]

-privacy concerns may result in potential losses in online sales of up to $18 billion by 2002,[95]

-82% of online households believe that government should regulate the use of personal information online, and 92% do not trust online companies to keep this information confidential.[96]

The FTC stated that progress had been made since its first report in 1998 with regard to privacy disclosures and implementation of fair information practices. It discussed its decision, in 1998,[97] and again in 1999,[98] to give industry self-

[90] Federal Trade Commission, *Privacy On-Line: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (2000) (visited Dec. 20, 2000) <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> [hereinafter *Privacy On-Line*].

[91] *Id.* (reporting three of the five Commissioners joined in the majority report. Commissioner Orson Swindle dissented, issuing a statement in which he stated that a call for legislation was premature, given the continued progress made by industry self-regulation. Commissioner Thomas B. Leary issued a statement, concurring in part and dissenting in part. He stated that the "recommendation is too broad because it suggests the need for across-the-board substantive standards when, in most cases, clear and conspicuous notice alone should be sufficient. The recommendation is too narrow because any legislation should apply to offline commerce a well.").

[92] *See id*. at 2-3.

[93] *See id*. at 2 & n. 12; (citing Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want,* PRIVACY AND AMERICAN BUSINESS, Nov. 1999, at 11).

[94] *See id*. at 2.

[95] *See Privacy On-Line, supra* note 90, at 2.

[96] *See id*.

[97] *See, e.g., id.* at 11.

[98] *See, e.g., id.* at 5.

regulation efforts more time to develop. The FTC concluded, however, that industry efforts alone have not been sufficient.[99]

The FTC conducted two surveys in February and March 2000. One focused on a random sample of 335 of 5,672 Web sites with 39,000 or more unique visitors per month (Random Sample),[100] and the other on 91 of the 100 busiest Web sites (Most Popular Group).[101]

The surveys found that personal identifying information, such as name or e-mail address, were collected by 97% of the Random Sample and 99% of the Most Popular Group.[102] 88% of the sites in the Random Sample and 100% of those in the Most Popular Group posted, at least, one privacy disclosure statement,[103] while 62% and 97%, respectively, posted a unified privacy policy.[104] The FTC acknowledged that these figures showed improvement over similar figures cited in the 1998 Report and 1999 Report.

However, the FTC was not satisfied with the quality of many of the privacy disclosures found on these Web sites. The surveys included a set of content analysis questions which more closely scrutinized how well the privacy disclosure implemented each of the four main principles of fair information practices: Notice, Choice, Access, and Security.[105] The results showed that of the

[99] *See id. at 38.*

[100] *See Privacy On-Line, supra* note 90, at 7-9 (referring to Appendix A of the 2000 Report, which discusses in detail the methodology used in the surveys, and Appendix B of the 200 report, which contains the list of Web sites included in the survey, the survey forms used, the instructions, and the results).

[101] *See id.*

[102] *Id.* at 9 (noting that "when the traffic of all sites surveyed is taken into account, there is a 99% chance that, during a one-month period, a consumer surfing the business sites on the Web will visit a site that collects personal identifying information. . .") .

[103] *Id.* at 10 (noting that a "privacy disclosure" is defined as either a unified privacy policy or a discrete information practice statement, such as "This is a secure order form").

[104] *Id.* at 10-11 (noting "the posting of a privacy policy does not necessarily mean that a site follows any or all fair information practices, as the policy might address only certain practices and not others").

[105] *See Privacy On-Line, supra* note 90, at 4 (describing that in the 2000 Report the FTC modified slightly the "core principles of privacy" it had discussed in the 1998 Report by reducing from five to four the number of principles and by shortening the names of the principles from Notice/Awareness to Notice, Choice/Consent to Choice, Access/Participation to Access, and Integrity/Security to Security. The FTC relegated what had been the fifth core principle, Enforcement/Redress, to being a "critical ingredient in any

sites that collected personal identifying information, only 20% of the Random Sample and 42% of the Most Popular Group implemented, at least in part, all four of the fair information practices.[106] The FTC stated that while there can be some disagreement on how to implement the principles of Access and Security, Notice and Choice should be much less complicated to implement.[107] The survey found, however, that only 41% of the sites in the Random Sample and 60% of those in the Most Popular Group met the basic standards for Notice and Choice.[108]

The 2000 Report discussed in detail the content analysis questions pertaining to each of the fair information practice principles, Notice, Choice, Access and Security.[109] It also discusses Enforcement and the growth of the online privacy seal programs, TRUSTe and BBBOnLine.[110] The surveys found that only 8% of the sites in the Random Sample and 45% of those in the Most Popular Group displayed any type of privacy seal.[111] Furthermore, of the sites that had a privacy seal, only 52% and 56%, respectively, implemented all four of the fair information practice principles, and 63% and 71%, respectively, implemented even the basic Notice and Choice standards.[112]

The FTC cautioned that these numbers might be somewhat misleading since a site was given credit for implementing a principle if it implemented even a part of it.[113] For example, a site received credit for implementing the principle of Access if it permits the ability to review, correct, or delete at least one piece of personal information collected, regardless of how many others

governmental or self-regulatory program," and shortened its name to Enforcement).

106 *See id*. at 12 (noting these figures "indicate[ ] improvement since the release of the Gipps Report - which found that 10%of sites in the random sample posted disclosures addressing at least one element of each of the four fair information practices principles").

107 *See id*. at 13 (describing how the Commission examined data to determine how Web sites are implementing Notice and Choice).

108 *See id*.

109 *See generally id*. at 14-19 (describing the "types of disclosures for which sites were awarded credit for each of the fair information practice principles of Notice, Choice, Access, and Security, and the results for each principal individually").

110 *See Privacy On-Line, supra* note 90, at 20.

111 *See id*. at 20.

112 *See id*.

113 *See id*. at 22.

it may collect with or without this same ability to review, correct, or delete.[114]

The 2000 Report examined the practice of placement of cookies on a consumer's computer by third parties.[115] The surveys found that 57% of the sites in the Random Sample and 78% of the sites in the Most Popular Group allowed such placement.[116] Furthermore, only 22% and 51%, respectively, gave Notice that the third parties might place cookies on the user's hard drive or collect information about them.[117]

The FTC recommended that "Congress enact legislation to ensure adequate protection of consumer privacy online."[118] It recognized that self-regulation would still need to be an important component of any scheme to protect consumer privacy, but urged adoption of legislation that would require compliance with the four fair information practices.[119] It stated that, given the industry's limited success in implementing these practices, along with heightened consumer concerns about privacy, the time is right for legislative action.[120]

The FTC call for legislation has not been well received by the White House or Congress, and it does not appear likely that the passage of any far reaching privacy legislation is imminent.[121] Instead, it appears for now that self-regulation will continue to be the primary mechanism for protection of personal information.[122]

---

114 *See id*. at 23-24.

115 A third party is defined as "any domain other than the site being surveyed." *See Privacy On-Line, supra* note 90, at 21. This practice has become a very common way for advertisers to gather information about consumers.

116 *See id*. (noting the majority of the third-party cookies are from network advertising companies that engage in on-line profiting).

117 *See id*. (noting that the "majority of the Web sites that allow third-party cookies do not disclose that fact to consumers").

118 *Id.* at 36.

119 *See id.* (explaining that the proposed legislation would provide a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites).

120 *See Privacy On-Line, supra* note 90, at 36-37.

121 *See* Labaton, *White House and Agency Split on Internet Privacy*, *supra* note 77 (stating, "[w]hile legislation has been introduced by Democrats in both the House and the Senate, there is no expectation that Congress will act any time soon").

122 *See id.*

VII. SAFE HARBOR PRINCIPLES

A first draft of the proposed Safe Harbor was made public in November 1998.[123] After much public comment and negotiation between the DOC and the European Commission, a second draft was released in April 1999. A cover letter, written by then-Under Secretary and Ambassador David L. Aaron, explained that "[o]rganizations within the safe harbor would have a presumption of adequacy and data transfers from the European Community to them would continue. Organizations could come into the safe harbor by self certifying that they adhere to these privacy principles. The decision to enter the safe harbor is entirely voluntary."[124]

In his letter, Ambassador Aaron outlined the benefits of entering the Safe Harbor:

- All 15 Member States (MS) will be bound by the European Commission's finding of adequacy;
- The understanding will create the presumption that companies within the safe harbor provide adequate data protection and data flows to those companies will continue;
- MS requirements for prior approval of data transfers either will be waived or approval will be automatically granted;
- US companies will have a transition period to implement safe harbor policies;
- Claims against US organizations will for the most part be limited to claims of non-compliance with the principles, European consumers will be expected to exhaust their recourse with the US organization first, and due process will be assured for US organizations that are subject to complaints; and
- Generally, only the European Commission, acting with a committee of Member State representatives (the Article 31 Committee), will be able to interrupt personal data flows from an EU country to a US organization.[125]

---

[123] *See* International Trade Administration, *USDOC Electronic Commerce Task Force: Final Safe Harbor Documents – July 21, 2000* (last modified July 21, 2000) <http://www.ita.doc.gov/td/ecom.menu.html> (noting that draft, as well as all subsequent drafts, are available) [hereinafter *Final Safe Harbor Documents*].

[124] *Safe Harbor Letter from Ambassador Aaron*, *supra* note 76 (presenting the revised International Safe Harbor Principles, from Ambassador David L. Aaron, Under Secretary for International Trade).

[125] *Id.*

A third draft of the Safe Harbor was published in March 2000.[126] A final draft was approved unanimously by the European Union Member States in May 2000 and posted in June 2000.[127] The Safe Harbor agreement includes a statement of Safe Harbor Privacy Principles[128] and a set of fifteen Frequently Asked Questions (FAQs). These documents are referred to, collectively, as "the Principles."[129]

United States organizations that receive personal data from the EU may choose to qualify for the Safe Harbor and its presumption of "adequacy."[130] An organization may choose to adhere to the Principles and join a self-regulatory privacy program, such as TRUSTe or BBBOnLine, or it may choose to develop its own privacy policy in accordance with the Principles.[131] Some organizations may already be subject to statutory, regulatory or administrative rules that bring it in compliance with the Principles. In any case, the organization must self-certify to the DOC its adherence to the Principles.[132]

While an organization may choose to apply the Principles to all of the data it processes, it is obligated, under the Safe Harbor, only to apply the Principles to personal data and personal information[133] received from a European Union country.[134] Furthermore, the Principles need only be applied after the U.S. organization chooses to enter the Safe Harbor.[135]

The Safe Harbor Privacy Principles are:

---

126 *See* United States Department of Commerce, *Draft*, *International Safe Harbor Privacy Principles* (last modified March 17, 2000) <http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm> [hereinafter Redlined Principles]

127 *See Final Safe Harbor Documents, supra* note 123.

128 *See* United States Department of Commerce, *Draft, Safe Harbor Privacy Principles* (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/USPrinciplesJune2000.htm> [hereinafter US Principles].

129 *Id.*

130 *Id.*

131 *See id.*

132 *See id.*

133 "'Personal data' and 'personal information' are defined in the Safe Harbor as "data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form." US Principles, *supra* note 128.

134 *See id.*

135 *See id.*.

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party[136] or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the notice and choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the

136 "It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task[s] on behalf of and under the instructions of the organization. The onward transfer principle, on the other hand, does apply to such disclosures." *Id.* at endnote 1.

organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be

sufficiently rigorous to ensure compliance by organizations.[137]

At the heart of the Safe Harbor are the notice and choice Principles. These require that an organization inform an individual, in clear and conspicuous language, about the purposes for which it collects and uses information about them, the types of third parties to which the information may be disclosed, the choices available to limit such use and disclosure, and how to contact the organization with inquiries or complaints.[138]

The organization must provide the individual with the opportunity to opt-out of having information disclosed to third parties.[139] What this will mean in most cases is that, as long as notice is properly given, the burden will fall on the individual to opt-out. In other words, as long as the individual does not object to the stated uses of the information, the organization will be in compliance with the Principles.

On the Web, users have already become quite familiar with ubiquitous registration forms. Unless someone pays close attention to the various default choices provided on the form, he will likely lose his choice to opt-out of some of the uses of his information. It will be interesting to see how many Web sites will adopt policies banning users from entering the site, or parts of the site, if they don't agree to some minimal (or greater) use of information. Some Web sites have already begun enticing users to disclose personal information by offering to trade it for something of value. For example, an individual may be required to complete a detailed form in order to enter a contest.

If sensitive information is involved, it may be protected from distribution to third parties, unless the individual opts-in, that is, unless the individual takes some affirmative step to have the information distributed.[140] However, there are so many conditions and exceptions that it will be rare for such an opt-in requirement to exist. Only if the sensitive information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized, will there be an "opt-in" requirement.[141] Even then, there are

137 *Id.*
138 *See* US Principles, *supra* note 128.
139 *See id.*
140 *See id.*
141 *See id.*

additional exceptions that limit this choice.[142]

During negotiations, the European Commission had preferred the word "revealing" to "specifying" in the phrase defining sensitive information, that is "personal information *specifying* medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information *specifying* the sex life of individual."[143] (emphasis added) It believed that "specifying" would be too narrow inasmuch as certain information might not technically *specify* a medical condition, for example, but could *reveal* it. There is no doubt that the adoption of "specifying" in the final draft greatly weakens the protection for sensitive data and the applicability of the "opt-in" requirement.

For the vast majority of information collected, an organization will be within the Safe Harbor as long as it adequately provides notice of the intended uses of the information, and provides the individual with the choice not to have his information so used.[144] Whether an individual may agree to certain disclosures or uses of his information despite some reservations about those disclosures or uses, may depend upon how much he wants to enter the organization's Web site or receive whatever it is that the organization is offering. An individual who is interested in protecting his personal information should be better able to, unless the industry standard evolves into one requiring objectionable disclosures or uses merely to gain entrance to the site. If this were to happen, an individual would have to choose between permitting such disclosure or use, and foregoing whatever is being offered by the organization.

Under the onward transfer Principle, an organization must apply the notice and choice Principles in order to disclose information to a third party.[145] However, it may disclose

[142] *See* Directive, *supra* note 1, at art. 8; *see also* United States Department of Commerce, *Draft, Frequently Asked Questions (FAQs) FAQ 1 – Sensitive Data* (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/FAQ1sensitivedataJune2000.htm> (listing six such exceptions).

[143] US Principles, *supra* note 128; *see* Redlined Principles, *supra* note 126 (noting the European Commission's preference of the word "revealing" and the United States Government's concern about that selection).

[144] *See* US Principles, *supra* note 128.

[145] *See id.*

information, without adhering to the notice and choice Principles, to a third party agent performing tasks under its supervision, if it ascertains that the third party subscribes to the Principles or is otherwise subject to the Directive or some other adequacy finding.[146] The organization is relieved of liability for subsequent abuses of the information unless it knew or should have known that the third party would not comply with the Principles.[147]

During negotiations, there were several endnotes addressing issues that were unresolved or problematic to one or both sides.[148] The only remaining endnote in the Safe Harbor Privacy Principles has to do with the notice and choice regarding disclosures to third parties and the related onward transfer of that information.[149] In somewhat recursive fashion, the Principle refers one to the endnote, which exempts certain disclosures from notice and choice, but then states that the onward transfer Principle nonetheless still applies to the exception.[150] This will prove to be a problem unless the language is clarified.

The security Principle requires organizations to "take reasonable precautions to protect [personal information] from loss, misuse, unauthorized access, disclosure, alteration and destruction."[151]

The data integrity Principle requires that personal information be relevant for the purposes for which it is used and prohibits an organization from processing personal information in a way that is incompatible with the purposes for which it was collected.[152] The organization is required to "take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current."[153]

The access Principle provides an individual with the right to amend or delete inaccurate information.[154] There was much discussion about the "reasonableness" of the access required.

146 *See id.*
147 *See id.*
148 *See* Redlined Principles, *supra* note 126 (listing several differences in opinion between the European Commission and the United States on various issues).
149 *See* US Principles, *supra* note 128.
150 *See id.*
151 *See id.*
152 *See id.*
153 *See id.*
154 *See* US Principles, *supra* note 128.

The phrase "reasonable access," which appeared in the first draft, was replaced with "access," but accompanied by the equally vague proviso "except where the burden or expense of providing access would be disproportionate to the risks of the individual's privacy. . ."[155] This language will undoubtedly be the subject of many factual disputes.

The longest FAQ is the one addressing access.[156] It states that while the right of access is not absolute and is subject to the principle of proportionality or reasonableness, organizations should make good faith efforts to provide access.[157] It states, however, that confidential commercial information, such as marketing inferences, do not have to be disclosed.[158]

The FAQ also states that "[t]he access principle does not . . . create any obligation to retain, maintain, reorganize or restructure personal information files."[159] If an organization stores information in a way that cannot identify individual information, there is no requirement to change this structure. There is no requirement to provide access to personal information that is processed solely for research or statistical purposes. There is no requirement to provide access to the database itself, but merely to the identifiable information of the individual. In addition, there are about a dozen situations in which access can be denied.[160]

There was much concern from industry about repetitious or vexatious requests for access. The FAQ provides that an organization may charge a reasonable fee for access and may limit the number of request from one individual to a certain number per given period of time, although access cannot be denied on cost grounds if the individual agrees to pay the costs.[161]

---

155 *Id.*; *see also* United States Department of Commerce, *Draft, International Safe Harbor Privacy Principles* (last modified Apr. 19, 1999) <http://www.ita.doc.gov/td/ecom/shprin.html> (containing the phrase "reasonable access" and providing an explanation of the meaning).

156 *See* United States Department of Commerce, *Draft, Frequently Asked Questions (FAQs) FAQ8: Access* (visited Dec. 20, 2000). <http://www.ita.doc.gov/td/ecom/FAQ8AccessJune2000.htm> [hereinafter *FAQ8*].

157 *Id.*

158 *See id.*

159 *Id.*

160 *See id.*

161 *See FAQ8*, *supra* note 156.

In order to protect itself from fraudulent requests, an organization may require sufficient information to verify the identity of the person making the request.[162] An organization is not required to provide access to personal information that is derived from public records or is otherwise publicly available.[163]

Access will be one of the more difficult issues for business to address. New mechanisms will, in most cases, have to be created to handle the changes. The FAQ states that while responses to requests for access should be made without excessive delay and within a reasonable time period, responses may be made at regular intervals rather than on an individual request basis.[164]

A number of Web sites have already experienced increased expenses in complying with the more rigorous requirements of the Children's Online Privacy Protection Act.[165] In addition to requiring access to information collected from children under 13, COPPA requires extensive notification and verification to and from parents.[166] In response, a number of sites have either stopped collecting information from children or purged their files of any information previously collected.[167]

The enforcement Principle will provide another major challenge for business. It requires a) the establishment of "readily available, and affordable independent resource mechanisms"[168] under which complaints are investigated and resolved; b) verification of the privacy policies adopted by organizations; and c) obligations to remedy noncompliance with the Safe Harbor.[169]

Four of the FAQs deal specifically with enforcement issues. First, the Self-Certification FAQ[170] provides that an organization

---

[162] *See id*

[163] *See id.*

[164] *See id.*

[165] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (Supp. IV 1999).

[166] *See id.* at §§ 6501(1), 6502(b)(1) (defining "child" as a person under the age of thirteen, and giving parents broad rights to view, alter and refuse to allow the use of information about a child gathered by Web sites).

[167] *See* Karen J. Bannan, *Parents Remain Unclear on Online Privacy Law,* N.Y. TIMES, May 12, 2000 (detailing the steps that websites have taken to attempt to comply with COPPA).

[168] US Principles, *supra* note 128.

[169] *See id.*

[170] United States Department of Commerce*, Draft, Frequently Asked*

choosing to self-certify must send a letter, signed by a corporate officer, to the DOC.[171] Included in this letter, must be, at least, a description of its privacy policy, where the policy is available for public viewing, a contact office for the handling of complaints, the name of any privacy program to which the organization belongs, the method of verification, and the independent recourse mechanism that is available for investigation of unresolved complaints.[172] The FAQ also provides that the DOC will maintain a list of all organizations that self-certify, and make this list, along with the self-certification letters, available for public viewing.[173] Organizations that self-certify must state in their published privacy policy statements that they adhere to the Safe Harbor.[174]

Second, the Verification FAQ[175] describes the two basic approaches an organization can take to verify that the attestations and assertions it makes about its safe harbor privacy practices are true and have been implemented. The first approach is one of self-assessment. An organization must demonstrate that its privacy policy conforms to the Safe Harbor and "is accurate, comprehensive, prominently displayed, completely implemented and accessible."[176] The organization must demonstrate that individuals are informed of any in-house or independent complaint mechanisms, and that employees are properly trained regarding privacy policies and appropriately disciplined for violations thereof.[177] In addition, the organization should have internal procedures for periodically conducting objective compliance reviews.[178] A statement verifying such self-assessment should be made at least once a year.[179]

Alternatively, an organization may choose to have an outside

Questions (FAQs) FAQ6 - Self-Certification (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/FAQ6selfcertJune2000.htm>.

171 *See id.*

172 *See id.*

173 *See id.*

174 *See id.*

175 United States Department of Commerce, *Frequently Asked Questions (FAQs) FAQ7 - Verification* (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/FAQ7verifJune2000.htm> [hereinafter *FAQ7*].

176 *Id.*

177 *See id.*

178 *See id.*

179 *See id.*

compliance review.[180] Such a review would have to demonstrate that mechanisms and procedures similar to those described above are effectively in place.[181] A statement verifying successful completion of an outside compliance review also should be obtained at least once a year.[182]

Third, a FAQ on the Role of Data Protection Authorities[183] discusses how organizations may satisfy points (a) and (c) of the enforcement Principle by declaring in its self-certification to the DOC its intention to cooperate with the DPAs in the investigation and resolution of complaints brought under the Safe Harbor and to comply with the DPA's advice.[184] The DPAs will render advice from informal panels that will hear any evidence presented by either side.[185] An organization will have twenty-five days to comply with the advice given by the DPA.[186] Failure to comply may result in referral of the matter to the FTC or other United States federal or state body with authority to take enforcement action.[187]

Fourth, the Dispute Resolution and Enforcement FAQ[188] also addresses points (a) and (c) of the enforcement Principle. It states that organizations may satisfy these requirements by compliance with private sector developed privacy programs, by compliance with legal or regulatory supervisory authorities that handle complaints and dispute resolution, or by commitment to

---

[180] *See FAQ7*, *supra* note 175.

[181] *See id.*

[182] *See id.*

[183] United States Department of Commerce, *Frequently Asked Questions (FAQs) FAQ5 The Role of the Data Protection Authorities* (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/FAQ5DPAsJune2000.htm> [hereinafter *FAQ5*]. Each of the European Union Member States has a Data Protection Authority (DPA) charged with monitoring the provisions adopted pursuant to the Directive.

[184] *See id.*

[185] *See id.*

[186] *See id.*

[187] *See* United States Department of Commerce, *Draft, Frequently Asked Questions (FAQs) FAQ 5 The Role of the Data Protection Authorities* (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/FAQ5DPAsJune2000.htm>.

[188] United States Department of Commerce, *Draft, Frequently Asked Questions, FAQ No 11: Dispute Resolution and Enforcement* (visited Dec. 20, 2000) <http://www.ita.doc.gov/td/ecom/FAQ11EnforcementJune2000.htm> [hereinafter *FAQ No 11*].

cooperate with the DPAs, as discussed above.[189]

Consumers are encouraged to resolve any complaints directly with the organization before pursuing an independent recourse mechanism.[190] If a complaint reaches a dispute resolution body, the goal is to correct any noncompliance and to prevent similar behavior from happening again.[191] A variety of sanctions and remedies are available to the successful complainant, including publicity of the noncompliance, deletion of data, suspension or removal of an organization's privacy seal, compensation for losses, and injunctive orders.[192]

Undoubtedly the major enforcement mechanism of the Safe Harbor is the FTC's agreement to investigate alleged noncompliance under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive trade practices.[193] The FTC has promised to review on a priority basis referrals from privacy self-regulatory programs, like TRUSTe and BBBOnLine, and from EU member countries alleging noncompliance.[194] This would include failures to comply with advice given by a DPA.[195]

The DOC will maintain a list of organizations that have self-certified adherence to the Safe Harbor.[196] It will also maintain a list of those organizations that have persistently failed to comply with the Safe Harbor and are no longer assured of its benefits.[197]

Industry has been lobbying hard to maintain a system of self-regulation. Many organizations have adopted new policies and have implemented new mechanisms to deal with some or all of the issues addressed by the Safe Harbor. Whether or not these changes are proved to be or are perceived to be effective enough will determine just how strong the demand is for new legislation.

---

189 *See id.*
190 *See id.*
191 *See id.*
192 *See id.*
193 15 U.S.C. § 45 (1994).
194 *See FAQ No 11*, *supra* note 188.
195 *See FAQ5*, *supra* note 183 (stating that failure to cooperate with DPAs will be considered actionable under Section 5 of the Federal Trade Commission Act).
196 *See FAQ No 11*, *supra* note 188.
197 *See id.*