THE EU-U.S. PRIVACY SAFE HARBOR: SMOOTH SAILING OR TROUBLED WATERS?

James M. Assey, Jr. and Demetrios A. Eleftheriou*

"Nobody should underestimate the problem by doubting the political will of the European Union to protect the fundamental human rights of citizens."[1]

"You have zero privacy. Get over it."[2]

In both the United States and Europe, the birth of the Internet and the rapid growth of online services have placed great strains on the ability of individuals to keep information about themselves private.[3] The power and speed of computers and the anonymity of cyberspace makes information collection more detailed, more easily indexed to the individual, more easily processed or "mined," more permanent and, perhaps most importantly, less detectable.[4] As a result, while the value of personal data as a commercial asset has steadily risen, so too has the concern of citizens worried about threats to their personal privacy.[5] While these fears may be common, there exists a great division of opinion over what individuals and governments can do to combat them.

In 1995, the European Union ("EU") adopted sweeping privacy legislation creating strong protections governing the collection and use of personal data, and harmonizing the domestic privacy

* James Assey and Demetrios Eleftheriou are attorneys in the Cable and Internet Practice Group of Willkie Farr & Gallagher's Washington, D.C. office. They can be reached via e-mail at jassey@willkie.com and deleftheriou@willkie.com.

1 Ulf Bruhan, Data Protection in Europe: Looking Ahead, Address Before the Nineteenth International Conference of Privacy Data Protection Commissioners (Sept. 1997), *quoted in* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 46 (1998) [hereinafter SWIRE & LITAN].

2 Deborah Radcliff, *A Cry for Privacy*, COMPUTER WORLD, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO042940,00.html (May 17, 1999) (quoting Scott McNealy, CEO, Sun Microsystems Inc.).

3 At the outset, we stress that our discussion of privacy is limited to informational privacy, or "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others." INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION, *at* http://www.iitf.nist.gov/ipc/privacy.htm (1997) (citing ALAN WESTIN, PRIVACY AND FREEDOM 7 (1968)); *see* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 n.4, 1466 (2000) [hereinafter Froomkin] (describing information privacy as the ability to control the acquisition and release of information about oneself and noting that it differs from the U.S. constitutional formulation of privacy). An essential component of informational privacy is effective "data protection." COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 13 (1992) (discussing data protection as a more precise term than "privacy," as it is "[a] more accurate appellation for the group of policies designed to regulate the collection, storage, use, and transmittal of personal information").

4 Marie Save de Beaurecueil, *Regulating Information Privacy: A Comparative Study of Data Protection Policy in the United States and European Union*, J. OF INTERNET L., Dec. 1999, at 21 [hereinafter Save de Beaurecueil]; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998) [hereinafter Kang]; *see* Patrick Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet the Standard?*, 21 FORDHAM INT'L L.J. 932, 941–42 (1998); SWIRE & LITAN, *supra* note 1, at 6; *see also* Froomkin, *supra* note 3, at 1468-69 (discussing various "privacy-destroying" technologies in our modern information society).

5 Jason Sykes & Glenn R. Simpson, *Some Big Sites Back P3P Plan; Others Wait*, WALL ST. J., Mar. 21, 2001, at B1 (citing a 2001 Wall Street Journal-Harris Interactive poll in which 73% of Americans were either very concerned or somewhat concerned about threats to their personal privacy on the Internet); Toby Lester, *The Reinvention of Privacy*, THE ATLANTIC MONTHLY, Mar. 2001, *available at* http://www.theatlantic.com/issues/2001/03/lester.htm [hereinafter Lester] (citing a 1999 Wall Street Journal-NBC survey in which Americans cited privacy as their number one concern in the 21st Century, ahead of overpopulation, racial tensions and global warming); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1126 (2000) [hereinafter Samuelson] (noting that personal data may be used for internal marketing purposes as well as third-party licensing); *see* Nicole M. Buba, *Waging War Against Identity Theft: Should the United States Borrow From the European Union's Battalion?*, 23 SUFFOLK TRANSNAT'L L. REV. 633, 637 n.21 (2000) [hereinafter Buba] (citing Nov. 1998 Lou Harris Poll stating that 88% of respondents were concerned about threats to their privacy and of those, 55% were very concerned); Kang, *supra* note 4, at 1196–97 (citing 1996 Study finding that 89% of persons polled were either very or somewhat concerned about privacy).

laws of EU Member States.[6] This legislation (the "Directive"), which took effect on October 25, 1998, generally establishes principles of data protection applicable in all fifteen EU Member States.[7] Organizations "processing" personal information within the EU must comply with legislation implementing the Directive in the relevant EU Member States.[8] For affected organizations in Europe, the Directive creates extensive regulatory and substantive obligations, and requires nonconforming organizations to adopt necessary operational changes to their collection, use, processing and dissemination of personal data.[9]

But across the Atlantic, enactment of the Directive also has had a very palpable effect on U.S. organizations that receive personal information from foreign divisions or third parties within EU Member States. Specifically, U.S. multinational and e-commerce organizations objected to provisions in Article 25 of the Directive, which generally bar the transfer of personal data to any non-EU country that does not provide "adequate" privacy protection.[10] Because it was feared that the EU would find U.S. privacy law to be "inadequate," U.S organizations worried that the Directive would create a "data fence" around Europe, and lead to the interruption of data flows between Europe and the United States.[11]

To EU regulators, however, this "third country" transfer prohibition was necessary to prevent circumvention of the Directive's protections through the creation of "data havens" where the very rights created under the Directive could be systematically violated.[12] Processing organizations in data havens may have no legal obligations to protect personal data, and data subjects may have no enforceable rights.[13] In addition, despite the visibility of the prohibition in Article 25, laws restricting the transfer of personal data were not novel and had existed in pre-Directive data privacy laws in certain Member States.[14]

To U.S. businesses, however, the likelihood that

---

6 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 2, 1995 O.J. (L 281) 10 [hereinafter Directive]. The Directive ensures the privacy of individuals' personal data in any type of commercial medium, and is not limited to data collected and transferred online. In particular, the Directive recognizes that individuals have certain rights in their personal information, including: (1) a right to information from subsequent data users about where the personal data is available, the identity of the organization that is processing the data and the purposes for which the data is being used; (2) a right of access to any personal data relating to that individual; (3) a right to correct or rectify any personal data that is inaccurately reported; and (4) a right to opt out of permitting personal data to be used under certain circumstances, such as for direct marketing purposes where no specific reason is provided. *Id.* at art. 14; *see also* Save de Beaurecueil, *supra* note 4, at 24 (discussing the rights of data subjects under the Directive).

7 Directive, *supra* note 6, at art. 4. Under EU law, the Directive requires Member States to pass legislation implementing its provisions. As such, it sets the minimum requirements for such national laws, yet permits some variation between them. *See* SWIRE & LITAN, *supra* note 1, at 25 (noting that the Directive permits Member States to adopt stricter regulations regarding sensitive information and permits them to narrow certain exceptions to the prohibition on the transfer of personal data to countries that lack "adequate" privacy protection). Notably, some EU states (Denmark, France, Germany, Ireland, Luxembourg and the Netherlands) failed to pass implementing legislation by the deadline provided in the Directive. While this failure may preclude governments in these countries from requiring compliance with certain provisions of the Directive, it does not under EU law, preclude individual citizens in these Member States from: (1) invoking provisions of the Directive before their national courts; and (2) seeking compensation before national courts for any damages suffered as a result of the Member State's failure to adopt implementing legislation. Dr. Klaus-Dieter Borchadt, *The ABC of Community Law*, 91-92, *at* http://europa.eu.int/comm/dg10/publications/brochures/docu/abc/txt_en.pdf (2000). Additionally, we note that the European Commission has initiated proceedings before the European Court of Justice in an effort to bring these Member States into compliance. *See* Jonathan Kapstein, *U.S. Firms Not Buying E.U. Privacy Deal*, NAT. L.J., Jan. 29, 2001, at B5.

8 Directive, *supra* note 6, at art. 2 (defining processing to mean "any operation or set of operations which is performed upon personal data, whether or not by automatic means, 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").

9 *Id.* at art. 17.

10 *See id.* at art. 25(1) ("Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection.").

11 Owen D. Kurtin & Beth Simone Noveck, *Spotlight on Privacy: Developments in Data Protection*, J. INTERNET L., Aug. 2000, at 12 [hereinafter Kurtin & Noveck].

12 SWIRE & LITAN, *supra* note 1, at 25–26; *see* Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 158 (1996) [hereinafter Gellman]; Paul M. Schwartz, *European Data Protection Laws and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 472 (1995).

13 *See* SWIRE & LITAN, *supra* note 1, at 25–26.

14 *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1339 (2000) [hereinafter *Rules in Cyberspace*]; SWIRE & LITAN, *supra* note 1, at 25 n.11 (discussing dispute whereby Fiat-France eventually entered into a contract with Fiat-Italy to of-

EU officials would not view the largely self-regulatory approach to privacy protection in the United States as "adequate" left many organizations with the two poor options of either adopting costly changes to their information processing practices or risking the prospect of not being able to receive critical data from entities in EU countries.[15] Thus, despite the existence of limited exceptions to the transfer prohibition,[16] U.S. organizations argued for the creation of an alternative, more flexible means of ensuring that data flows from the EU would not be interrupted.[17]

In light of such concerns, U.S. and EU negotiators embarked on the negotiation of "Safe Harbor Privacy Principles" ("Safe Harbor" or "Principles") as an alternative means of satisfying the adequacy requirement in Article 25.[18] Under this approach, U.S. organizations qualifying for the Safe Harbor would be presumed to provide "adequate" privacy protection as required by the Directive. On March 14, 2000, after almost two years of negotiations, the Department of Commerce announced that it had reached a tentative agreement with the European Commission regarding the Principles.[19] Four months later, the European Commission formally adopted a decision recognizing that the Safe Harbor provides adequate protection for personal data transferred from the EU to the United States.[20] Finally, on November 1, 2000, the U.S. Department of Commerce began accepting Safe Harbor applications and launched a website dedicated to helping U.S. businesses sign up.[21]

Unfortunately, the Safe Harbor that was once trumpeted as "a landmark accord for e-commerce"[22] has, at best, received only a tepid response to date from the U.S. business community.[23] In five and one-half months, only thirty-seven organizations have enrolled in the Safe Har-

---

fer protections of French law to data transferred to the Italian affiliate); Kurtin & Noveck, *supra* note 11, at 13 (discussing the same).

15 *See* SWIRE & LITAN, *supra* note 1, at 42 (noting that despite pre-Directive prohibitions, passage of the Directive has significantly made the anti-transfer rules universal, more visible, more urgent and has put data processors on much fuller notice of their obligations).

16 Article 26(1) permits the transfer of personal data to countries that lack "adequate" privacy protections where: (a) the data subject has given his consent unambiguously; (b) the transfer is necessary to perform certain contracts; (c) the transfer is necessary on important public interest grounds; (d) the transfer is necessary to protect the data subject's vital interests; (e) the transfer is made from a register that is intended to provide information to the public; or (f) the data controller has adduced sufficient guarantees through the addition of appropriate contractual clauses and such clauses have been approved by the relevant national regulator (subject to the objection of other Member States). Directive, *supra* note 6, at art. 26(1). Alternatively, under Article 26(2), a Member State may authorize transfers to a third country lacking adequate protection if such data is protected by "adequate safeguards," which in particular may include appropriate contractual clauses approved by a Member State. *Id.* at art. 26(2). Finally, Article 26(4) of the Directive empowers the European Commission to adopt model contractual clauses containing adequate safeguards that could be used by parties transferring personal data. *Id.* at art. 26(4); *see* THE EUROPEAN COMMISSION, PRELIMINARY DRAFT OF A COMMISSION DECISION UNDER ARTICLE 26(4) OF THE DIRECTIVE 95/46/EC ON STANDARD CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES THAT DO NOT PROVIDE AN ADEQUATE LEVEL OF PROTECTION FOR THE PROCESSING OF PERSONAL DATA, *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/callcom.htm (Sept. 29, 2000) (noting the European Commission's release of a model contract for comment by interested parties). However, reliance on these latter two exceptions may be limited, however, to rare circumstances. *See* SWIRE & LITAN, *supra* note 1, at 33–38.

17 U.S. DEPARTMENT OF COMMERCE, WELCOME TO THE SAFE HARBOR, *at* http://www.export.gov/safeharbor/ (last visited Feb. 28, 2001).

18 Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666, 45,666–86 (July 24, 2000) [hereinafter Safe Harbor Principles]. The Safe Harbor applies only to U.S. organizations receiving personal data from the EU and includes both the seven principles of data protection discussed as well as fifteen Frequently Asked Questions ("FAQs") that supplement these Principles and provide guidance on their interpretation. These documents are also available through the Department of Commerce's website. INTERNATIONAL TRADE ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, ELECTRONIC COMMERCE TASK FORCE, *at* http://www.ita.doc.gov/td/ecom/menu.html (last visited Mar. 8, 2001).

19 *See* Press Release, Department of Commerce, U.S., European Union Agree on "Safe Harbor" for Data Privacy, *at* http://www.usinfo.state.gov/topical/global/ecom/00031501.htm (last visited Mar. 15, 2000).

20 Letter from EU Commission to Robert LaRussa, Undersecretary for Int'l Trade of United States Dep't of Commerce (July 28, 2000) *available at* http://www.useu.be/issues/adequ0728.html (transmitting the European Commission's adequacy finding).

21 *See, e.g.*, U.S. DEPARTMENT OF COMMERCE, WELCOME TO THE SAFE HARBOR, *at* http://www.export.gov/safeharbor/ (last visited Feb. 28, 2001).

22 Press Release, Department of Commerce, Commerce Secretary William M. Daley Hails EU Approval of Safe Harbor Privacy Arrangement, *available at* http://osecnt13.osec.doc.gov/public.nsf/docs/169C6EEE9A01CA64852568F00058DF37 (May 31, 2000).

23 This reluctance may be fueled by a number of factors, including uncertainty over enforcement issues, compliance costs, a reluctance to go first and little penalty for taking a go-slow approach. *See* Tamara Loomis, *EU's Data Privacy Safeguards Get Scant Response in the United States*, N.Y.L.J., Nov. 30, 2000, at 5 [hereinafter Loomis]; *see also* Declan McCullagh, *Safe Harbor is a Lonely Harbor*, WIRED NEWS, *at* http://www.wired.com/news/print/0,1294,41004,00.html (last visited Jan. 5, 2001) (noting the unwillingness of companies and

bor.[24] Of these, only two, Hewlett-Packard and Dun & Bradstreet, are large multinational organizations; the rest are generally either small to medium enterprises with privacy issues arising from business-to-consumer transactions, or self-regulatory organizations who are in the business of providing organizations with privacy compliance services.[25] While others may soon rush to join, the clock may be ticking as EU officials have pledged to review their current forbearance on enforcement in mid-2001.[26] Accordingly, the stage is now set for U.S. organizations receiving personal data from EU entities either to embrace the protections of the Safe Harbor and adopt necessary changes to their information practices, or to prepare for potentially turbulent times ahead as European authorities ready their data embargo orders.

This discussion does not come to save the day but rather it: reviews the competing philosophies of privacy protection that underlie this controversy; examines the provisions of the Safe Harbor and the flexibilities provided therein; and finally, suggests strategies for U.S. organizations seeking to determine whether to enroll in the Safe Harbor.

I. BACKGROUND

A. EU: A Rights-Based Approach to Information Privacy

Over the last thirty years, European governments have responded to concerns about the privacy of personal data through the adoption of comprehensive, "rights-based" data protection statutes.[27] Under such approaches, governments recognize data privacy as a "political right anchored among the panoply of fundamental human rights and the rights attributed to 'data subjects' or citizens."[28] Typically, these laws: (1) apply to both the private and public sectors; (2) affect a wide range of activities including the collection, use and dissemination of personal data; (3) impose affirmative obligations, such as registration, with the appropriate governmental authority; and (4) are generally nonsectoral, applying regardless of the specific type of data.[29]

Beginning in the 1970s, EU nations began discussions regarding data protection and transborder data flow issues that led to the enactment of the first comprehensive data protection laws in Europe.[30] These laws responded to consumer

trade associations to endorse the Safe Harbor).

[24] *See, e.g.*, U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR LIST, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safeărbor+list (last visited Apr. 13, 2001).

[25] *Id.* As of Apr. 13, 2001, the enrolled organizations are: Adar International, Inc.; Audits & Surveys Worldwide; Capital Venue; Crew Tags Int'l; Cybercitizens First; Data Services, Inc.; Decision Analyst, Inc.; The Dun & Bradstreet Corporation; E-lection.com (LDE Inc.); e2 Communications, Inc.; enfoTrust networks; Entertainment Software Rating Board; Genetic Technologies, Inc.; HealthMedia, Inc.; Hewlett Packard; Market Measures Interactive, L.P.; Mediamark Research, Inc.; Naviant Marketing Solutions, Inc.; NOP Automotive, Inc.; Numerical Algorithms Group, Inc.; Oak Technology; Pharmaceutical Product Development, Inc.; Privacy Leaders; Qpass Inc.; Responsys; Software 2010 LLC; SonoSite, Inc.; Strategic Marketing Corporation; TRUSTe; United Information Group (c/o ASW); USERFirst; USERTrust Inc; The USERTRUST Network L.L.C.; Usinternetworking, Inc.; WellMed, Inc.; World Research, Inc. d/b/a/ Survey.com; and WorldChoiceTravel.com, Inc. *Id.*

[26] Safe Harbor Principles, 65 Fed. Reg. at 45,666 ("[W]e understand that the Commission and Member States will use the flexibility of Article 26 and any discretion regarding enforcement to avoid disrupting data flows to U.S. organizations during the implementation phase of the safe harbor *and that the situation will be reviewed in mid-2001.*" (quoting Letter to EC representative John Mogg (EU) from Robert LaRussa, U.S. Department of Commerce) (emphasis added)); *see* Mary Mosquera, *EU May "Make An Example" Of U.S. Privacy Abusers*, INTERNET WK. (Apr. 4, 2001) *available at* http://www.techweb.com/wire/story/TWB20010404S0009 (discussing the possibility that European data authorities may take action against U.S. organizations).

[27] *Rules in Cyberspace, supra* note 14, at 1318; Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 782 (1999) [hereinafter *Electronic Commerce*]. "Rights-based" refers to a system that grants to each citizen a right to consent to the personal processing of his or her personal information, and the concomitant right to access any stored personal data and to have any errors corrected. *Id.*

[28] *Rules in Cyberspace, supra* note 14, at 1330–31.

[29] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32–33 (1997) [hereinafter CATE], *cited in* SWIRE & LITAN, *supra* note 1, at 23.

[30] *See Rules in Cyberspace, supra* note 14, at 1329; COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 13–14 (1992).

fears that the increased use of electronic data processing by governments and large corporations would lead to the creation of centralized national data banks containing their personal information.[31] Changes in technology exacerbated these fears, as the evolution from centralized mainframes to distributed PCs radically increased the number of potential public and private data offenders and furthered the push for broad data protection.[32] In 1970, the German state of Hesse adopted the first data processing regulation due to concerns that sophisticated technologies were increasing the risk that an individual's personal data could be improperly manipulated.[33] Sweden followed in 1973 by passing the first national data protection law.[34] Similarly, in 1978, France enacted the Law Concerning Data Processing, Files and Liberty, which required the processing of data in a manner that would protect privacy and avoid harm to the individual.[35]

During the 1980s, the adoption of binding national laws was complemented by the development of international data protection instruments.[36] In 1980, in an effort to balance data protection with the need to promote strong economic growth in the personal data industry, the Committee of Ministers of the Organization for Economic Cooperation and Development ("OECD") promulgated voluntary guidelines with regard to protecting privacy and transborder data flows ("Guidelines").[37] In another multinational attempt to establish data protection guidelines, the Council of Europe, a post-World War II intergovernmental organization focused on the protection of human rights, promulgated a convention "For the Protection of Individuals with Regard to Automatic Processing of Personal Data" ("European Convention").[38] The European Convention set forth norms of data privacy similar to those set forth in the Guidelines but created binding rules for signatories.[39] However, the Council of Europe largely failed to achieve uniform protection of personal data because of wide variation among the different countries implementing the European Convention and because, like the Guidelines, its implementation was not mandatory.[40]

While the voluntary nature of the Guidelines and the European Convention did not result in the adoption of national data protection laws in all EU Member States, their common aims did lay the groundwork for the adoption of the Directive in 1995.[41] As such, the purpose of the Directive was to harmonize data protection laws throughout the EU in a way that would guarantee a high level of privacy protection to EU citizens and further support the creation of a unified market in Europe.[42]

B. United States: A Market-Based Approach to Information Privacy

In contrast to Europe, the United States has adopted a self-regulatory, "market-based" ap-

---

31 Save de Beaurecueil, *supra* note 4, at 22 (noting that large social welfare systems in the EU gave rise to the need for governments to collect large amounts of information about individuals).

32 *Id.* at 22–23; SWIRE & LITAN, *supra* note 1, at 52–64 (distinguishing between data protection problems arising from mainframe technology and client-server systems).

33 Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 447 (1995). In addition to being only a state law, this law applied only to the public sector. Michael R. Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 71, 77 (1996) [hereinafter Roch].

34 This law established a national Data Protection Board with enforcement powers. Roch, *supra* note 33, at 77.

35 *See* Buba, *supra* note 5, at 650. Not all EU nations followed suit. Indeed, at the time that drafting of the Directive began in 1990, Italy, Greece, Spain and other European countries had not yet enacted national data protection statutes. SWIRE & LITAN, *supra* note 1, at 23.

36 CATE, *supra* note 29, at 34–35.

37 Organisation for Economic Co-operation and Development, Guidelines on Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, 20 I.L.M. 422 (1981), *available at* http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM. The United States agreed to these basic Principles for data protection. However, as mentioned, the Guidelines were voluntary and did not create binding law. Gellman, *supra* note 12, at 152.

38 *See* CATE, *supra* note 29 at 34.

39 Julie Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 467 (2000) [hereinafter Fromholz]; *Rules in Cyberspace*, *supra* note 14, at 1329.

40 *See* Fromholz, *supra* note 39, at 467; Buba, *supra* note 5, at 651–52. The European Convention, although similar to the Guidelines, focused more on the significance of data protection to protect personal privacy. *See* CATE, *supra* note 29, at 34. Although the Guidelines emphasized that the free flow of data is critical to economic development, the European Convention emphasized the need to protect individuals. *See* Joel R. Reidenberg, *The Privacy Obstacle Course Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. 137, 144 (1992).

41 *See* Fromholz, *supra* note 39, at 467; Kurtin & Noveck, *supra* note 11, at 13.

42 SWIRE & LITAN, *supra* note 1, at 24–25; *Rules in Cyberspace*, *supra* note 14, at 1329.

proach to information privacy.[43] Rather than seeking to create broad political rights, such a system relies primarily on industry norms, codes of conduct and the consumer marketplace to protect personal privacy; and secondarily, relies on narrowly targeted protections that apply to specific sectors of the economy or particular groups of individuals.[44] For example, the United States has enacted a patchwork of laws protecting personal information collected online from children under 13,[45] personal information collected by financial institutions,[46] the contents of electronic communications,[47] information regarding the viewing habits of cable subscribers,[48] telephone customer information,[49] video rental records,[50] driver records,[51] school records,[52] medical records[53] and consumer credit information,[54] to name only a few. In other cases, where privacy legislation has not targeted specific groups or types of information, it has generally been focused on checking government prying rather than private incursions.[55]

One explanation for this market-oriented bias supporting privacy protection in the United States has been the importance placed on promoting the free flow of information—a principle firmly rooted in the First Amendment.[56] In addition, the open flow of information not only comports with the U.S. system of self-governance, it also assists in promoting commerce, and providing citizens with significant economic and social benefits.[57] Finally, reliance on a combination of market-based solutions and targeted legislative actions may be the result of a healthy distrust for governmental solutions, and a belief that the market provides a more effective and sensitive means of protecting personal privacy.[58]

Regardless of its origins, the U.S. market-based approach to data protection is not without its opponents. Indeed, critics argue that there are significant obstacles to securing adequate protection of personal information: individuals may be uninformed of their privacy rights, unaware of potential business uses and value resulting from aggregation, unable to detect improper disclosures, and unwilling to accept the high costs that may be associated with bargaining regarding the value of their data.[59] Concerns such as these have prevented EU authorities from concluding that the United States has "adequate" privacy protections and, ultimately, led to the development of the Safe Harbor.

II. HOW TO QUALIFY FOR THE SAFE HARBOR

As previously discussed, the Safe Harbor is designed to permit U.S. organizations to receive

43 *See* Froomkin, *supra* note 3, at 1524; *Electronic Commerce, supra* note 27, at 771–81, 787–89.

44 *Rules in Cyberspace, supra* note 14, at 1332; Buba, *supra* note 5, at 642–49; Save de Beaurecueil, *supra* note 4, at 25–27; *Electronic Commerce, supra* note 27, at 771–87; *see also* Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000) [hereinafter *Principles of Internet Privacy*] (discussing principles that undergird the U.S. government's efforts to protect privacy and craft privacy norms); Froomkin, *supra* note 3, at 1524–28 (criticizing the self-regulatory approach adopted by the United States); Roch, *supra* note 33, at 88.

45 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6502 (Supp. V 1999).

46 Gramm-Leach-Bliley Act of 1999, 12 U.S.C. §§ 1811, 1828b, 1831x (Supp. V 1999)

47 Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701–2709, 2711, 3121–3126 (1994 & Supp. IV 1998).

48 Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994).

49 Telecommunications Act of 1996, 47 U.S.C § 222 (Supp. IV 1998).

50 Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994).

51 Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (1994 & Supp. IV 1998).

52 Family Education and Right to Privacy Act of 1974, 20 U.S.C. § 1232g (1994).

53 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

54 Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681(a)(4) (1994).

55 *See, e.g.*, Privacy Act of 1974, 5. U.S.C. § 552a (1994) (addressing privacy of personal records held by the government); Right to Financial Privacy Act of 1978, 12 U.S.C. § 3402 (1994) (limiting government access to personal records held by a private sector recordkeeper); *see also Principles of Internet Privacy, supra* note 44, at 877 (discussing reasons that the highest protections guard against government intrusions).

56 *See Principles of Internet Privacy, supra* note 44, at 881. Cate argues that U.S. privacy law is based on five broad principles: a history of balancing competing interests, respect for open flows of information, a desire to be free of government intrusions, a requirement of specific harm and a preference for self-help measures. *Id.* at 879–91.

57 *Id.* at 881–84; *see also* Reno v. Condon, 528 U.S. 141, 142 (2000) (noting that personal, identifying information is an item of interstate commerce, and thus, properly subject to regulation under the Commerce Clause).

58 *See Principles of Internet Privacy, supra* note 44, at 890.

59 SWIRE & LITAN, *supra* note 1, at 7–8; *see also* Samuelson, *supra* note 5, at 1132–36 (discussing the appeal of a property-rights approach to personal privacy as a means of combating market failure).

transfers of personal data from entities in EU Member States.[60] Although U.S. companies are not required to participate in the Safe Harbor, those electing not to enroll run the risk that EU authorities will take action to cut off the flow of personal data normally received from EU-based entities.[61]

To qualify for the Safe Harbor and thus receive its presumption of "adequacy," an eligible U.S. organization must: (1) adhere to the Safe Harbor summarized below; and (2) publicly announce its compliance through certification letters filed annually with the Department of Commerce or its designee.[62] Compliance with the Safe Harbor may be accomplished through a variety of methods, among these are joining an industry self-regulatory privacy program (such as TRUSTe or BBBOnline) or developing a self-regulatory privacy policy.[63]

A. Safe Harbor Privacy Principles

All U.S. organizations seeking to enroll in the Safe Harbor must agree to the following seven Principles:

(1) NOTICE: Organizations must provide clear and conspicuous notice to individuals of: (a) their purposes in collecting and using the individual's personal information;[64] (b) how to contact the organization with complaints or inquiries; (c) the types of third parties to which personal information is disclosed; and (d) the choices and means available to individuals to limit use and disclosure of their information.[65] Notice is required when the personal information is collected or as soon thereafter as is practicable.[66] Where such information is disclosed to a third party for the first time or used for a purpose other than that for which it was collected, prior notice of such fact is required.[67]

(2) CHOICE: Organizations must offer individuals a clear, conspicuous, readily available and affordable mechanism to choose ("opt out") whether their personal information may be: "(a) disclosed to third parties; or (b) used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual."[68] In contrast, organizations must receive affirmative and explicit consent from individuals ("opt in") before any of their sensitive information may be: (a) disclosed to third parties; and/or (b) used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual.[69]

(3) ACCESS: Organizations must permit individuals to access their personal information and must permit them 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 or where the rights of other persons would be violated.[70]

(4) ONWARD TRANSFER: Where a third party

60 Information for Certification Under FAQ 6 of the Safe Harbor Privacy Principles, 66 Fed. Reg. 3983 (Jan. 17, 2001) *available at* http://www.export.gov/safeharbor/SafeHarborHistoricalDocuments.htm.

61 Information for Certification Under FAQ 6 of the Safe Harbor Privacy Principles, 65 Fed. Reg. 66,690 (Nov. 7, 2000) *available at* http://www.export.gov/safeharbor/SafeHarborHistoricalDocuments.htm.

62 *Id.*

63 U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR OVERVIEW, *at* http://www.export.gov/safeharbor/SafeHarborInfo.htm (last visited Feb. 21, 2001).

64 Under the Safe Harbor, "personal information" and "personal data" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the EU and recorded in any form. Safe Harbor Principles, 65 Fed. Reg. at 45,667; *see* SWIRE & LITAN, *supra* note 1, at 26 (noting that inclusion of "identifiable" means that the Directive applies not only to names but also to any information from which a person can be identified).

65 Safe Harbor Principles, 65 Fed. Reg. at 45,667.

66 *Id.*

67 *Id.*

68 *Id.* "An individual should be able to exercise [an] 'opt out' (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization." *Id.* at 45,674. Organizations are not required to provide notice and choice to individuals where disclosure is made to a third party acting as an agent to perform tasks on behalf and under the instructions of another party. Nevertheless, the principle of "onward transfer" discussed below does apply to such disclosures. *Id.* at 45,667.

69 *Id.* at 45,668. Sensitive information includes personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or the sex life of the individual. In addition, any information received from a third party should be treated as sensitive where such third party treats and identifies it as sensitive. *Id.*

70 *Id.* Requests for access are subject to the principle of proportionality or reasonableness. The sensitivity of the data and the expense and burden of providing access are important (but not controlling) factors in determining whether providing access is reasonable. In certain limited circumstances, organizations may deny or limit an individual's access to personal information, but, if so, must provide individuals with specific reasons for such denial or limitation.

acts as an agent of the organization, disclosure of personal information to such third party is permitted without providing notice and choice to the individual if the organization first: "(a) ascertains that the third party subscribes to the [P]rinciples, or is subject to the Directive or another adequacy finding; or (b) enters into a written agreement with such third party requiring . . . at least the same level of privacy protection as required by the relevant [P]rinciples."[71] Compliance with the Principle of onward transfer will immunize an organization from liability arising from the third party's improper processing of such information *unless* the organization knew or should have known that the third party would process the information improperly, and has not taken reasonable steps to prevent or stop such processing.[72]

(5) SECURITY: "Organizations creating, maintaining, using or disseminating personal information must take reasonable steps to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction."[73]

(6) DATA INTEGRITY: Organizations "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."[74] To ensure data integrity, organizations "should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current."[75]

(7) ENFORCEMENT: Organizations must provide enforcement mechanisms that, at a minimum, include: (a) "readily available and affordable independent recourse mechanisms through 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";[76] (b) follow-up procedures to verify that an organization's stated "privacy practices are in fact true and that these practices have been implemented as presented";[77] and (c) obligations to remedy problems arising out of an organization's failure to comply with the Principles (where it has announced its adherence to the Principles) and the possibility of sufficiently rigorous sanctions for noncompliance.[78] Complaints of noncompliance with the Principles referred to the Federal Trade Commission ("FTC") by self-regulatory organizations (e.g., TRUSTe, BBBOnline) and EU nations

Organizations may charge a reasonable fee for providing individuals with access to their personal information. *Id.* at 45,670–72.

71 *Id.* at 45,668.

72 *Id.*

73 *Id.*

74 *Id.*

75 *Id.*

76 *Id.* Consumers should be encouraged to raise complaints directly with the organization before proceeding to independent recourse mechanisms. *Id.* at 45,673. In addition, recourse mechanisms should explain dispute resolution procedures and contain notice of the mechanism's privacy practices in conformity with the Safe Harbor. *Id.*

77 *Id.* at 45,668. Organizations may meet verification requirements either through self-assessment or outside compliance reviews. *Id.* at 45,670. Those choosing self-assessment must annually create and keep on file a statement signed by a corporate officer or other authorized representative that is available to individuals upon request, or to independent bodies or agencies responsible for investigating complaints or unfair practices. *Id.* Such a statement must indicate that an organization's published privacy policy regarding personal information collected from the EU: (a) is accurate, comprehensive, prominently displayed, completely implemented and accessible; (b) conforms to the Safe Harbor; and (c) informs individuals of available in-house or independent mechanisms for pursuing complaints. Additionally, the organization must indicate that it has in place procedures to train employees in implementing its privacy policy and to conduct periodic compliance reviews. *Id.* Those organizations choosing outside compliance review must ensure that such review demonstrates that: (a) the organization's privacy policy conforms to the Safe Harbor and is being complied with; and (b) individuals are informed of available complaint mechanisms. They also must annually obtain and keep on file a statement, signed by the reviewer or a corporate officer or other authorized representative that is available to individuals upon request in the context of an investigation or complaint about compliance. *Id.*

78 *Id.* at 45,668. Organizations may satisfy the requirements of (a) and (c) by: (1) committing to cooperate with European Data Protection Authorities ("DPAs"); (2) complying with legal or regulatory authorities that provide for handling of individual complaints and dispute resolution; (3) complying with private programs incorporating the Principles into their rules and including effective enforcement mechanisms as described in the enforcement principle; or (4) complying with any other private sector mechanism developed that satisfies the requirements of the enforcement principle. *Id.* at 45,673. Organizations choosing to satisfy (a) and (c) through cooperation with the DPAs must state in their certification to the Department of Commerce (see below) that they will: (1) comply with the enforcement principle through cooperation with the DPAs; (2) cooperate with the DPAs in the investigation and resolution of complaints brought under the Safe Harbor; and (3) comply with advice given by the DPAs, including taking certain remedial and compensatory measures; and (4) provide the DPAs with written confirmation that such action has been taken. Any advice provided to an organization by the DPAs must be complied with within twenty-five days. A failure either to comply with the Principles or to cooperate with the DPAs shall be actionable under Section 5 of the Federal Trade Commission ("FTC") Act or similar statute. *Id.* at 45,669.

will be reviewed by the FTC, on a priority basis, to determine whether Section 5 of the Federal Trade Commission Act has been violated.[79] Organizations that persistently fail to comply with the Principles will lose the benefits of the Safe Harbor.[80]

Generally, organizations seeking Safe Harbor protection must apply the foregoing Principles to all personal data transferred from the EU to the United States.[81] However, adherence to the Principles may be limited:

> (a) [t]o the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization;[82] or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.[83]

B. Annual Certification Required

In addition to conforming their information practices to the foregoing Principles, organizations seeking the benefits of the Safe Harbor must publicly announce this fact in certification letters filed annually with the Department of Commerce or its designee.[84] The Department of Commerce maintains on its website a public list of certified organizations and their self-certification letters.[85]

At a minimum, these certification letters must be signed by a corporate officer on behalf of the organization joining the Safe Harbor and must include:

(1) the name of the organization, mailing address, e-mail address, telephone and fax numbers;[86]

(2) a description of the activities of the organization with respect to personal information received from the EU;[87]

(3) a description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public; (b) its effective date of implementation; (c) a contact office for the handling of complaints, access requests and any other issues arising under the Safe Harbor; (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices, and violations of laws or regulations governing privacy (most likely the FTC); (e) the names of any privacy programs in which the organization is a member (e.g., TRUSTe, BBBOnline); (f) the method of verification; and (g) the independent recourse mechanism that is available to investigate unresolved complaints.[88]

When joining the Safe Harbor, if an organization wishes to include human resources information transferred from the EU for use in the context of an employment relationship, its certification letter also must include a declaration of its intent in this regard and a declaration of its commitment to cooperate with EU authorities as necessary.[89] Moreover, organizations wishing to comply with the enforcement principle through cooperation with Data Protection Authorities ("DPAs") must include in their certification letter

---

79 *Id.* at 45,673; 15 U.S.C. § 45 (Supp. IV 1998).

80 Safe Harbor Principles, 65 Fed. Reg. at 45,674.

81 *Id.* at 45,667. The transfer of financial services information is the subject of ongoing negotiations between the EU and United States (and thus does not fall within the protections of the Safe Harbor rules). Until such negotiations conclude, however, U.S. companies are permitted to receive such information. Additionally, Safe Harbor protections will only apply to human resources personal information transferred from the EU for use in the context of an employment relationship if the organization indicates this intention in its certification to the Department of Commerce, and conforms to certain procedures and policies described in the FAQs. *Id.*

82 Where exceptions to the Principles will be applied on a regular basis, organizations must indicate such fact in their privacy policies. *Id.*

83 *Id.* at 45,668–69. Further exceptions allow: (a) the gathering of personal information for publication, broadcast or other forms of public communication, as well as information found in previously published material disseminated from media archives (FAQ #2); and (b) the processing of information by investment bankers or auditors without an individual's knowledge, but only to the extent and for the period necessary to meet statutory or public interest requirements or where application of the Principles would prejudice the legitimate interests of the organization (FAQ #4). *Id.*

84 *Id.* at 45,670. Safe Harbor benefits are assured from the date on which an organization files its certification letter with the Department of Commerce. *Id.* at 45,667.

85 U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR LIST, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safeărbor+list (last visited Feb. 22, 2001).

86 THE UNITED STATES MISSION TO THE EUROPEAN UNION, FREQUENTLY ASKED QUESTIONS, SELF-CERTIFICATION, *at* http://www.useu.be/ISSUES/faqs0721.html (last visited Feb. 22, 2001).

87 Safe Harbor Principles, 65 Fed. Reg. at 45,669.

88 *Id.* at 45,669–70.

89 *Id.* at 45,670. Specific guidance is provided in FAQ #9 concerning application of the Principles to the transfer of human resources data from the EU to the United States. *Id.* at 45,672.

the statements outlined above.[90]

Finally, in circumstances where an organization will cease to exist as a legal entity due to a merger or takeover, the organization is required to provide notice to the Department of Commerce (or its designee) in advance of such action indicating whether the resulting entity will: (1) continue to be bound by the Safe Harbor by operation of law; or (2) elect to self-certify its adherence to the Safe Harbor or put in place other safeguards, such as a written agreement that will ensure such adherence.[91] Where neither option is satisfied, all data acquired by the U.S. organization under the Safe Harbor must be promptly deleted.[92]

III. CONSIDERING WHETHER TO JOIN THE SAFE HARBOR

Understanding the requirements of the Safe Harbor is only half the battle. The other half is determining whether enrollment in the Safe Harbor is the best way for a particular U.S. organization to ensure that its receipt of personal information from EU entities will be lawful and uninterrupted. Because, as noted, the current standstill on actions by EU authorities to prohibit data transfers is subject to review this summer,[93] U.S. organizations may soon have to face difficult decisions regarding how (or if) their information practices must be changed. Such changes require a thorough assessment of current data practices, as well as careful consideration of the time required to implement such changes and the impact that these changes may have on other aspects of the organization's operations.

To assist in this endeavor, we briefly describe some of the key inquiries that organizations should consider.

A. Assess the Availability of the Safe Harbor

First, an organization must determine whether it qualifies to enroll in the Safe Harbor. At present, only the FTC and the Department of Transportation have agreed to enforce violations of the Safe Harbor. Therefore, organizations in sectors of the economy not subject to the jurisdiction of these agencies (e.g., financial services and telecommunications sectors) are not, currently, eligible for Safe Harbor protections.[94]

B. Conduct a Privacy Audit

Second, having determined that it can enroll in the Safe Harbor, an organization should carry out a careful and thorough review of its current information practices. Attention should focus not only on current practices, but also on potential future plans to collect, store, use or disseminate personal data. Such a review is critical because before an organization can assess its potential liabilities and determine if Safe Harbor protection is necessary, it must thoroughly understand its data collection, storage, use and sharing practices.

1. Select a Privacy Team

Issues related to collection, storage, use and sharing of personal data can arise throughout the organization's structure. Accordingly, a compre-

---

90 *See supra* note 77.

91 THE UNITED STATES MISSION TO THE EUROPEAN UNION, FREQUENTLY ASKED QUESTIONS, SELF-CERTIFICATION, *at* http://www.useu.be/ISSUES/faqs0721.html (last visited Feb. 22, 2001).

92 *Id.*

93 *See supra* note 26.

94 As described by the European Commission:

> The FTC covers commerce in general, but some sectors are excluded from its jurisdiction (financial services, transport, telecommunications, etc.). These sectors can also be covered by the 'safe harbor' to the extent that other public bodies with similar powers to the FTC undertake to pursue companies in sectors under their jurisdiction for non-compliance with the Principles. For the time being, only the U.S. Department of Transportation has chosen to come forward with the necessary information to allow the European Commission to recognise it as a government enforcement body in addition to the FTC. This will allow airlines to join the 'safe harbor.' The European Commission expects to be able to recognise other U.S. government enforcement bodies in due course.

EUROPEAN COMMISSION, HOW WILL THE "SAFE HARBOR" ARRANGEMENT FOR PERSONAL DATA TRANSFERS TO THE U.S. WORK?, *available at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/datatransf.htm (July 27, 2000); *see* Terry Lane, *FCC Help Sought Enforcing Privacy Safe Harbor for Telecom*, COMM. DAILY, Jan. 8, 2001, at 4 (noting efforts by the FTC to enlist the Federal Communications Commission's assistance in agreeing to enforce Safe Harbor violations against common carriers). Though common carriers could not seek protection for data transfers not subject to the FTC's enforcement authority, they may be able to seek protection for other data transfers not directly related to a company's common carrier operations (e.g., collection through a website in violation of a posted privacy policy). Terry Lane, *FCC Help Sought Enforcing Privacy Safe Harbor for Telecom*, COMM. DAILY, Jan. 8, 2001, at 4.

hensive review of information practices requires input from all departments, including the international, information services, marketing, finance, public relations, legal, administrative, governmental affairs, employee training and communications departments. Because this process will take time and cut across multiple areas, an organization must ensure that it devotes sufficient resources to this effort.

The review process should be managed by a dedicated senior employee to ensure that timetables are set, deadlines are met and members of the team in different areas of the organization have a common point of contact.[95] An organization may conduct this review internally with assistance from outside counsel or with the assistance of a private consulting firm.[96]

2. *Ask the Right Questions*

An organization should strive to develop a complete picture of the personal data it collects, processes and disseminates. Accordingly, these inquiries must be carried out in each area of the organization that deals with personal information (e.g., human resources, marketing, sales, Internet assets), and must consider both online and offline practices. Some of the key inquiries should include:

- What kinds of personal data are collected?
- How is personal data collected?
- How does the organization use personal data?
- How long does the organization retain such data?
- Does the organization disclose or will it in the future disclose personal data to third parties?
- What is the purpose for collecting or disclosing personal data?
- What are the security measures safeguarding personal data?
- Which employees or other persons have access to personal data?
- Does the organization collect more personal data than is reasonably necessary for the purpose collected?
- What types of notice, choice, access and rights of redress does the organization currently provide to those individuals from whom it collects personal data?

C. Assess Potential Liability for Failure to Comply With the Directive

Third, after clearly summarizing its current and anticipated future information practices, an organization must carefully evaluate whether such practices might be subject to the transfer prohibition under Article 25 of the Directive.[97] An organization should decide whether its data practices fall within the scope of the Directive by assessing whether any part of the organization's data practices are within the broad definitions of "personal data" and "processing,"[98] and, if so, whether they fit within one of the exceptions to the transfer prohibition in Article 26(1).[99]

In particular, the Directive explicitly does not apply to the processing of personal data in governmental activities where Member States have retained substantial sovereignty for processing operations regarding public security, defense, state security and state activities regarding criminal law,[100] and for processing of personal data "by a natural person in the course of a purely personal or household activity."[101]

---

95 It is estimated that by 2005, most midsize and large firms will create positions for chief privacy officers ("CPOs"). *Hot Job Track: Privacy, Chief Privacy Officer*, U.S. NEWS ONLINE, *available at* http://www.usnews.com/usnews/issue/001106/nycu/jobs.privacy.htm (Nov. 6, 2000). In addition to data privacy monitoring and compliance, CPOs would have to constantly conform the organization's privacy policy to adapt to organizational changes. Companies with CPOs include IBM, Delta Airlines, Microsoft, American Express and Mutual of Omaha. *Id.*; *see* Lester, *supra* note 5 (discussing the increasing prevalence of CPOs).

96 A number of private consulting firms (e.g., PriceWaterhouseCoopers, IBM) market specific privacy consulting services. *See, e.g.*, Patrick Sullivan, *Privacy and Corporate Compliance, at* http://www.pwcglobal.com/extweb/newcojou.nsf/DocIDManagement/1B32FCD6C379A808852566280068A33B (2001); IBM, PRIVACY WORKSHOP, *at* http://www.ibm.com/services/e-business/priwkshop.html (last visited Feb. 20, 2001).

97 Directive, *supra* note 6, at 21.

98 *See supra* notes 8 and 64.

99 *See supra* note 16.

100 SWIRE & LITAN, *supra* note 1, at 26–27 (citing Directive, *supra* note 6, at art. 3(2)).

101 *Id.* at 27 (quoting Directive, *supra* note 6, at art. 3(2)). A separate and unresolved question involves whether website activities could qualify as data transfers. While the Safe Harbor documents explicitly state that the Safe Harbor discussions "have not resolved nor prejudged the questions of jurisdiction or applicable law with respect to websites," the Directive calls upon Member States to apply their national law where "the controller is not established on Community

D. Assess Relative Costs and Benefits of Safe Harbor Protection

Next, after having determined that certain data practices would expose an organization to potential liability under the Directive, an organization should consider whether the relative benefits of the Safe Harbor outweigh the costs of enrollment.

1. Safe Harbor Benefits

Participating in the Safe Harbor can provide organizations with a number of benefits. First and foremost, it affords a measure of predictability and certainty for U.S. organizations and their trading partners whose businesses depend on the transfer of personal data across the Atlantic.[102] Enrollment ensures speedy transfers of personal data as prior approval by DPAs will either be automatic or not required.[103] Second, entrance results in lighter administrative burdens as the organizations will not have to provide protections on a case-by-case basis and will not have to seek approvals in each Member State, but rather, may rely on the fact that all fifteen Member States will recognize the Safe Harbor as providing adequate protections.[104] Finally, given rising consumer concern over personal privacy issues, enrollment in the Safe Harbor can also be seen as good business. By increasing employee and customer confidence in its privacy practices, an organization may generate substantial goodwill, favorable press and the enhancement of its brand.

2. Safe Harbor Costs

Unfortunately, the benefits of the Safe Harbor are not experienced without some cost. Participation may necessitate significant changes to an organization's information practices, requiring technical fixes and employee education. Additionally, while the Safe Harbor requires that the foregoing changes be implemented only to the extent necessary to protect personal data received from EU citizens, organizations may, as a practical and public relations matter, wish to extend such added protections to the personal data of all persons. Unless they implement such uniform information practices, organizations would face, for example, the unhappy prospect of maintaining different information processing mechanisms for different individuals in different countries, and also might invite criticism and complaints from certain customers who feel that their personal information receives less protection than that of EU citizens.[105] An organization either directly or indirectly bears the costs of implementation of an enforcement mechanism to investigate and resolve customer complaints, and to verify that its promised information practices live up to the requirements of the Safe Harbor. Moreover, an organization may face significant liabilities for its failure to fulfill its obligations. Specifically, it could face negative publicity campaigns, requirements to delete data or provide compensation for losses incurred, "delisting" where there is a persistent failure to comply, and potential liability for misrepresentations made to the public[106] and to the government in its certification letters.[107]

3. Alternative Means of Compliance

As an alternative, an organization also should consider the relative costs and benefits of altering its data practices to obtain unambiguous consent

territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." Safe Harbor Principles, 65 Fed. Reg. at 45,666; Directive, *supra* note 6, at art. 4(1)(c).

102 Jeff Rohlmeier & William Yue, *The Safe Harbor Privacy Framework*, EXPORT AM., Jan. 2001, at 20, 23 [hereinafter Rohlmeier & Yue]. The Safe Harbor's choice of an enforcement mechanism also can be seen as reducing risk and uncertainty as organizations (other than those choosing to cooperate with DPAs) may ensure that enforcement actions will occur in the United States. Safe Harbor Principles, 65 Fed. Reg. at 45,667.

103 Rohlmeier & Yue, *supra* note 102, at 23. Where personal data is transferred from the EU to the United States only for processing purposes, the EU organization is required under the Directive to enter into a contract with the U.S. party (so-called Article 17 contracts). However, because the Safe Harbor provides adequate protection, those contracts with Safe Harbor participants will not require prior authorization by Member States or such authorization will be granted automatically. Safe Harbor Principles, 65 Fed. Reg. at 45,673.

104 Safe Harbor Principles, 65 Fed. Reg. at 45,667.

105 *See The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearings Before the Subcomm. On Commerce, Trade, and Consumer Protection*, 107th Cong., *at* http://www.house.gov/commerce/hearings/03082001-49reidenberg104/htm (2001) (testimony of Prof. Joel Reidenberg) [hereinafter Reidenberg Testimony].

106 *See, e.g.*, 15 U.S.C. §§ 41–58 (1994 & Supp. 1999).

107 18 U.S.C. § 1001 (1994 & Supp. 1999); *see* Safe Harbor Principles, 65 Fed. Reg. at 45,673–74.

from the individual or otherwise find a way to fit within the Article 26(1) exceptions that would make Safe Harbor enrollment unnecessary.[108] For example, an organization may attempt to satisfy the "adequacy" requirement in Article 25 in other ways by providing other "adequate safeguards"—such as entering into contracts on a case-by-case basis that would provide sufficient privacy protections.[109] Should the European Commission subsequently adopt model contractual clauses governing the transfer of personal data, transfers could be carried out under such terms.[110]

IV. IMPLEMENTATION

Once an organization decides to enroll in the Safe Harbor, it must, as noted, register with the Department of Commerce and must change its information practices to reflect the Principles. Because it may face significant liabilities due to its failure to abide by these Principles, an organization should devote the necessary resources to ensure that any changes required of its data practices are properly implemented.

A. Regulatory Compliance: Safe Harbor Workbook

To assist organizations that wish to participate in the Safe Harbor, the Department of Commerce has developed a "Safe Harbor Workbook" available online through the Safe Harbor website.[111] The Workbook generally discusses the EU Directive and Safe Harbor framework in order to assist an organization in determining what changes, if any, are required in its information practices. In addition, the Safe Harbor website contains certification documents that enable an organization to enroll electronically in the Safe Harbor by providing the requisite information.[112] Also, aids provided by the government, outside counsel and private organizations such as TRUSTe offer EU Safe Harbor privacy seal programs that may assist organizations in signing up for the Safe Harbor and implementing any necessary changes to their data practices.[113]

B. Operational Compliance: Changes to Existing Privacy Policy

An organization also must ensure that it implements the necessary alterations to its information practices and that its revised policies conform to the Principles. These changes may be global in nature or may focus only on personal data received from EU countries. In any case, the organization must be sure that its practices conform to its stated policies.

C. Operational Compliance: Employee Training and Periodic Review

All employees and affiliates should undergo comprehensive training regarding procedures for the collection, storage, use and dissemination of personal data. In addition, because organizations will have to submit annual certifications regarding their compliance with Safe Harbor, monitoring

---

108 *See* Directive, *supra* note 6, at art. 26(1).

109 *See* Directive, *supra* note 6, at art. 26(2). One advantage of such an approach would be to avoid FTC jurisdiction. *See* Loomis, *supra* note 23, at 6. Such contractual provisions would by subject to the approval of the DPA in the Member State from which the data is being transferred subject to the objection of DPAs in other Member States. Directive, *supra* note 6, at art. 26(3).

110 Directive, *supra* note 6, at art. 26(4). A European Commission committee has recently given its preliminary approval of a "Draft Model Contract." *See* THE EUROPEAN COMMISSION, DRAFT COMMISSION DECISION PURSUANT TO ARTICLE 26(4) OF THE DIRECTIVE 95/46/EC ON STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES (VERSION OF 19 JANUARY 2001), *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clauses.htm (last visited Mar. 22, 2001). However, in the United States these model clauses have come under severe attack. Glenn R. Simpson, *U.S. Officials Criticize Rules On EU Privacy: Financial Companies Object To Europe's Strict View Of Web-Data Standards*, WALL ST. J., at B7 (discussing the Bush Administration's View that the EU model contractual clauses "impose unduly burdensome requirements that are incompatible with real-world operations."); *see U.S. Asks for Hold on EC's Consideration Of Standard Contracts for Data Transfers*, BNA DAILY REP. FOR EXECUTIVES, Mar. 28, 2001, *at* A17; *The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearings Before the Subcomm. On Commerce, Trade, and Consumer Protection*, 107th Cong., *at* http://www.house.gov/commerce/hearings/03082001-49/Winer103/htm (2001) (testimony of Jonathan Winer) [hereinafter Winer Testimony] (commenting on the shortcomings of the proposed model contracts).

111 U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR WORKBOOK, *at* http://www.export.gov/safeharbor/SafeHarborWorkbook.htm (last visited Feb. 19, 2001).

112 U.S. DEPARTMENT OF COMMERCE, CERTIFYING AN ORGANIZATION'S ADHERENCE TO THE SAFE HARBOR, *at* http://web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?openform (last visited Feb. 19, 2001).

113 TRUSTE, THE TRUSTE EU SAFE HARBOR PRIVACY PROGRAM, *at* http://www.truste.com/webpublishers/pub_eu.html (last visited Feb. 19, 2001).

and periodic review of data practices will be an essential part of a program of compliance.

V. CONCLUSION

Ultimately, the success of the Safe Harbor will depend on the willingness of U.S. organizations to enroll. The Department of Commerce has tried to encourage such action by stressing the Safe Harbor's benefits and by working with private trade associations to help businesses make an informed choice as to their options.[114] Of late, however, the Safe Harbor's critics have grown louder, arguing that compliance with the existing Safe Harbor rules would be costly, unworkable and unfair given the failure of Member State governments to aggressively enforce data privacy violations by European organizations.[115]

Despite these often-valid criticisms, it is important to remember that the Safe Harbor represents a (and not the only) means of ensuring that U.S. organizations dependent on transfers of personal data can participate in European markets despite the wide differences between the European and U.S. approach to data protection.[116] For some U.S. organizations, the Safe Harbor may provide a means of reducing compliance burdens and providing greater legal certainty. For others, such as organizations involved in data processing activities within an EU Member State (and thus directly subject to its data protection laws), the Safe Harbor may be of little benefit. The important point, however, is that U.S. organizations must avoid using the current controversy surrounding the Safe Harbor as an excuse to do nothing. Instead, they should carefully review their information practices so as to better understand their potential exposure to liability and choose the most appropriate means of compliance. Such a process may be difficult and may require painful changes to current operations, but it ultimately will reap substantial dividends for U.S. organizations and help to ensure smooth sailing through the global marketplace.

---

114 Margaret Johnston, *Commerce Department Tries to Boost 'Safe Harbor' Adoption*, COMPUTERWORLD, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55924,00.html (Jan. 5, 2001); Rohlmeier & Yue, *supra* note 102, at 23.

115 *See* Reidenberg Testimony, *supra* note 105; Winer Testimony, *supra* note 110; Patrick Thibodeau, *Key U.S. Lawmaker Calls for Review of Europe's Privacy Laws*, COMPUTER WORLD, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58406,00.html (Mar. 8, 2001); Madeline Bennett, *Sites are Flouting Privacy Rules*, IT WK., *at* http://www.zednet.co.uk/news/2001/ns-20692.html (Feb. 2, 2001).

116 Other means of bridging this divide may be on the horizon. In the online world, privacy enhancing technologies such as the Platform for Privacy Preferences ("P3P") may one day offer a superior means of ensuring that individual privacy preferences are respected. *See* Glen Simpson, *The Battle over Web Privacy*, WALL ST. J., Mar. 21, 2001, at B1 (discussing Microsoft's efforts to incorporate P3P technology into its Web browser).