Order Code RS20823
February 21, 2001

CRS Report for Congress

The EU-US "Safe Harbor" Agreement on Personal Data Privacy

Patricia A. Wertman
Specialist in International Trade and Finance
Foreign Affairs, Defense, and Trade Division

Summary

The European Union (EU) Data Privacy Directive, which went into effect in October 1998, prevents EU organizations, public and private, from transferring personal data to countries where the legal protections for personal data are not deemed "adequate" by the EU. To prevent the interruption of data transfers, the U.S. Department of Commerce (DOC) negotiated the "Safe Harbor" framework with the EU. U.S. organizations participating in "Safe Harbor" are automatically considered as having met EU privacy rules. "Safe Harbor," however, raises issues that may be reviewed by Congress. These include issues related to extraterritoriality, non-tariff barriers, business costs, and consumer protection. This report will be updated as events require.

Background

On October 24, 1995, the European Union (EU) agreed upon a Directive on Data Privacy.[1] The Directive arose from EU efforts to harmonize its Member's laws with regard to the protection of personal data. Its goal was to facilitate information flows within the EU and, thus, to strengthen the EU's internal market and to foster the development of the information-based economy, generally, and e-commerce and the Internet, specifically. At the same time the Directive seeks to balance these requirements against the need for strong personal privacy protections.

The Data Privacy Directive, which became effective in October 1998, enshrines strict legal protections that are deeply rooted in the belief that the privacy of personal data is a fundamental legal right. Personal information is defined as any information relating to natural persons, whether directly identified or indirectly identifiable.

---

[1] Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the processing of personal data and the free movement of such data. Official text available in the Official Journal of the European Communities, November 23, 1995, No. L. 281, p. 31.

The Directive applies to all organizations, public and private, operating in the EU. It covers the processing of all personal data, whether done automatically or manually. There is no exception for public records, such as telephone directory listings. Only information compiled for private, personal household use is excluded. Under the Directive data may be collected and used only for specified, explicit and legitimate purposes, and only those purposes. Security and accuracy must be guaranteed. Individuals have not only the right to access and the right to correct errors, but also to remedial measures and compensation, if necessary. The transfer of data to third parties may occur only under similarly strict requirements. More stringent rules apply to the processing of sensitive data, including data relating to race; ethnic origin; political, religious, or philosophical beliefs; and health or sex life.

The Directive also requires the creation of "Data Protection Agencies" (DPAs) in each of the 15 EU member states; registration of data bases with these authorities, and, sometimes, prior DPA approval before organizations or firms may begin data processing.

Rationale for the Agreement

The Data Directive prohibits the transfer of personal data to any nation outside the EU that does not meet the EU test of "adequacy" with regard to privacy protections. In the EU view, privacy protections in the United States may fail this test. The Directive, thus, potentially threatens to disrupt or, in some limited cases, even to prevent the transfer of data between the EU and the United States.

The reasons for the dissimilarities in the two regulatory regimes appear to lie in fundamentally different approaches to the issue of privacy. The right to privacy is a fundamental human right recognized both in the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of European Community laws. Thus, the EU has implemented privacy protection by enacting comprehensive legislation. By contrast, the United States has focused on industry sectors, overseeing the collection and use of data through a mix of legislation, regulation, and industry self-regulation, such as the new federal rules applicable to medical records. Moreover, U.S. firms tend to view personal data as a valuable commercial asset rather than as an individual asset. Practically, in the United States, this usually means the customers must "opt out" of customer lists and sales promotions; in Europe, customers generally have to "opt in" to commercial marketing schemes.

To bridge the regulatory difference and ease potential problems, the U.S. Department of Commerce (DOC) negotiated the "Safe Harbor" Framework with the EU. The EU Commission gave its final approval to "Safe Harbor" in July 2000. It became operational on November 1, 2000, when the DOC "Safe Harbor" website [http://www.export.gov/safeharbor/] went on-line. The DOC website provides information to U.S. organizations about participating in the "Safe Harbor" framework. It also makes available an up-to-date on-line list of U.S. organizations that have subscribed to the "safe harbor" framework, thus allowing EU organizations to be sure that data may be transferred to particular U.S. organizations.

Currently a "standstill," a political agreement between the United States and the EU not to enforce the Privacy Directive against U.S. firms, is in effect until mid-2001, when the "Safe Harbor" arrangement will be reassessed.

Basics of the "Safe Harbor" Framework

In addition to the EU Privacy Directive itself, the "Safe Harbor" framework encompasses seven basic principles, fifteen "frequently asked questions" (FAQs), the EU Commission's adequacy decision, an exchange of letters between DOC and the EU Commission, and an exchange of letters between the U.S. Departments of Transportation (DOT) and Federal Trade Commission (FTC) and the EU Commission – all available on the DOC web site. The seven basic principles, in edited and abridged form, are:[2]

- **Notice**: An organization must inform individuals about the purposes for which it collects and uses information, how to contact the organization with inquiries or complaints, and the types of third parties to which it discloses the information.

- **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 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.

  For **sensitive information**, individuals must explicitly **opt in** when personal data is to be transferred to a third party or used for a purpose other than the one for which it was originally collected or subsequently authorized. Sensitive information includes information about medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information regarding the individual's sex life.

- **Onward Transfer**: In transferring information to a third party, organizations must apply the Notice and Choice Principles. Third parties acting as agents must provide the same level of privacy protection either by subscribing to "Safe Harbor," adhering to the Directive or another adequacy finding, or entering into a contract that specifies equivalent privacy protections.

- **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**: Personal information must be relevant for the purposes for which it is to be used. . . . 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 the 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 would disproportionate to the risks to the individual's privacy or where the rights of others would be violated.

- **Enforcement**: Effective privacy protection must include mechanisms for verifying compliance; readily available and affordable independent recourse mechanisms in

---

[2] Full text is available at [http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm] .

cases of non-compliance; and consequences for the organization when the Principles are not followed. Sanctions must be rigorous enough to ensure compliance.

Eligibility and Enforcement

Any organization that receives data from the EU must comply with the Privacy Directive. Nevertheless, joining "Safe Harbor" is voluntary. Participation is open to any U.S. organization that is subject to regulation by the Federal Trade Commission (FTC), which enforces a variety of consumer protection laws, including those related to unfair and deceptive practices, and to U.S. air carriers and ticket agents that are subject to regulation by the Department of Transportation (DOT). To qualify organizations must self-certify annually in a letter to the DOC that they adhere to the safe harbor principles.

Enforcement of the "Safe Harbor" framework is undertaken both by the private sector and by federal and state authorities enforcing unfair and deceptive practices laws. Private sector enforcement has three components: verification, dispute resolution, and remedies. Persistent failure to comply will result in withdrawal of "Safe Harbor" status, a fact that will be listed on the "Safe Harbor" web site, and also, potentially, by regulatory action.

Organizations that do not fall under the jurisdiction of the FTC and the DOT are not eligible for "Safe Harbor." Notably, this includes U.S. financial firms and telecommunications carriers. In particular, the European Union does not consider that the Fair Credit Reporting Act (P.L. 91-508; 15 U.S.C. 1681 et seq.) or the recently enacted Financial Services Modernization Act (P.L. 106-102, popularly known as the Gramm-Leach-Bliley Act) provide adequate privacy protections. As a result, negotiations between the United States and Europe to achieve an agreement covering the financial sector continue. This latter omission has been a source of concern with some critics.

Issues for Congress

"Safe Harbor" is clearly intended to facilitate transatlantic data exchange and, hence, transatlantic commerce, both on-line and off. It, nevertheless, raises a number of policy issues or concerns that may be of interest to Congress[3]:

- **Extraterritoriality**: The EU Privacy Directive deliberately extends EU law beyond EU boundaries, not just to the United States, but to any nation with which EU organizations are likely to exchange personal information. On other issues, the United States has at times extended its laws to firms and activities in other countries. Some observers assert that, by extending EU law to the borderless worldwide web, this goes further.

- **Non-tariff Barrier (NTB)**: Some have suggested that the privacy protection requirements make the conduct of cross-border business, even between related corporate entities, so difficult and costly that they constitute an international trade

---

[3] See also, U.S. Library of Congress. Congressional Research Service. *Electronic Commerce: An Introduction*, by Glenn J. McLoughlin, January 25, 2001, RS20426; and *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith, December 21, 2000, RL30784.

barrier. Additionally, the EU has not negotiated agreements similar to "Safe Harbor" with other non-EU countries. Thus, the Directive, in practice, might operate in a manner that competitively disadvantages U.S. firms both with regard to EU firms and firms in third countries, particularly if enforcement is uneven.

- **Consumer Protection**: In recent years, the privacy issue has achieved heightened importance among consumers, particularly those using the Internet. Consumer advocates in Europe worry that "Safe Harbor" falls short of European data protection laws. Indeed, the European Parliament voted against the agreement because it was viewed as inadequate. Among their concerns was whether EU citizens who felt that their privacy rights had be violated would have the right to sue in U.S. courts. U.S. privacy advocates and civil libertarians, on the other hand, are concerned that U.S. firms will be extending less protection to Americans than Europeans. They also question the effectiveness of such business-backed self-regulatory privacy programs as BBBOnline and TRUSTe.[4] Balancing consumer and business interests in a workable regulatory framework, however, might provide a competitive advantage, building consumer confidence and furthering the development of e-commerce.

- **Relationship to the United States**: The "Safe Harbor" framework might be seen as accommodating international realities. FTC and DOT enforcement of "Safe Harbor" commitments, however, effectively give "Safe Harbor" the force of law. The U.S. Congress did not participate in its formulation, but must contend with private sector concerns regarding its requirements. Moreover, in extending EU law on privacy to U.S. organizations, it potentially alters both the complexity and the "complexion" of the domestic debate with regard to privacy issues. Significantly, the EU privacy directive reportedly played a role in the January 1, 2001 implementation of a new privacy law in Canada.[5]

- **Compliance**: Compliance within the EU itself is uneven. The EU Commission is taking legal action against six states – Denmark, France, Germany, Ireland, Luxembourg, and Netherlands – for failure to comply with the Privacy Directive. Many European firms do not state their privacy policy. Thus, U.S. firms participating in "Safe Harbor" potentially might be subject to greater scrutiny than European firms that are not in compliance.

- **"Free Speech"**: The Data Privacy Directive applies to the transmission of public records, such as, for example, numbers in a public telephone directory. "Safe Harbor" FAQ2 specifically states that the First Amendment rights of journalists are protected; no comparable statement is made regarding the rights of other U.S. citizens.

---

[4] BBBOnline, a wholly owned subsidiary of the Council of Better Business Bureaus, runs a voluntary self-regulatory program intended to promote consumer trust on the Internet. The program includes a "Privacy Seal Program." TRUSTe is an independent, non-profit privacy organization founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium. Its privacy program is based on a branded online seal, or "trustmark."

[5] See Pritchard, Timothy. Canada Strengthens Internet Privacy. *New York Times*, December 23, 2000, p. B2.

- **Encryption**: The privacy of data in the computer age of is often achieved by using encryption technology. Thus, U.S. policy on the export of encryption technology shadows this issue. Even after the July 2000 liberalization allowing exports of any strength encryption product to both government and private sector entities in the member states of the European Union, export of encryption technology remains subject to controls.

Business Concerns and Response

A number of additional issues are likely to be of interest to private businesses or organizations, including:

- **Cost**: The costs of implementation might well be substantial, requiring expensive organizational changes. Data subject to the Directive might have to be maintained and processed separately. A costly series of notices and permissions are required. Affiliates and subsidiaries might be considered "third parties," which could, for example, mean that data derived by a European subsidiary could not be transferred to its U.S. parent. Restrictions apply as long as the data are held, that is, *in perpetuity*. Firms are potentially opened up to private lawsuits by EU nationals.

- **Market Segmentation**: The data privacy directive might cause firms to segregate their European operations, especially their data processing, from those in the United States and elsewhere. This would have a particularly serious impact on e-commerce and the Internet, where the absence of boundaries has been a pre-eminent advantage.[6]

- **Web Diversity**: Some suggest that the worldwide web, where e-commerce makes this a particularly salient issue, is being "reculturalized," that is, as European and other countries increase their on-line presence, the preeminence of U.S. standards and rules is likely to diminish.[7]

Given the variety of issues that "Safe Harbor" generates, as well as the relative newness of the framework, it is perhaps not surprising that only 21 U.S. companies have signed on to "Safe Harbor." The framework has also not been publicly endorsed by the two organizations helping DOC to promote the framework – the Software Information Industry Association (SIIA) and the US Council for International Business (USCIB).[8]

---

[6] On November 20, 2000, a Paris court ordered Yahoo! to block French users from buying Nazi memorabilia on its U.S. sites – a decision that would also extend national law to the Internet. Yahoo! had already blocked sale of such items on its French language portal and is appealing.

[7] This point was made by Michael Erbschloe, vice president of Computer Economics in Carlsbad, CA, who has remarked that "[t]he reculturalization of the Web will be one of the biggest changes in the next few years. As more Europeans get on-line, U.S. companies will have to adhere to local rules and mores. They'll have to create Web sites in different languages and address different tastes. And they'll need to consider privacy as a priority, not as a nuisance." Erbschloe, quoted in Rothfeder, Jeffrey. Privacy War: The Europe-U.S. Struggle Over Consumer Data, p. 2. Available at [(http://www.strategy-business.com/policy/00305/].

[8] Krebs, Brian. U.S. Businesses Slow to Adopt EU Safe Harbor Agreement. Washtech.com, January 5, 2001.