



Safe Harbor Overview

The European Commission's Directive on Data Protection went into effect in October 1998, and would prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions.

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor -- approved by the EU in 2000 -- is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor will assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Directive.

SAFE HARBOR BENEFITS

The safe harbor provides a number of important benefits to U.S. and EU firms. Benefits for U.S. organizations participating in the safe harbor will include:

- All 27 Member States of the European Union will be bound by the European Commission's finding of adequacy
- Companies participating in the safe harbor will be deemed adequate and data flows to those companies will continue;
- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and
- Claims brought by European citizens against U.S. companies will be heard in the U.S. subject to limited exceptions.

The safe harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive, which should particularly benefit small and medium enterprises.

An EU organization can ensure that it is sending information to a U.S. organization participating in the safe harbor by viewing the public list of safe harbor organizations posted on this website. This list contains the names of all U.S. companies that have self-certified to the safe harbor framework. This list will be regularly updated, so that it is clear who is assured of safe harbor benefits.

HOW DOES AN ORGANIZATION JOIN?

The decision by U.S. organizations to enter the safe harbor is entirely voluntary. Organizations that decide to participate in the safe harbor must comply with the safe harbor's requirements and publicly declare that they do so. To be assured of safe harbor benefits, an organization needs to self-certify annually to the Department of Commerce in writing that it agrees to adhere to the safe harbor's requirements, which includes elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the safe harbor. The Department of Commerce will maintain a list of all organizations that file self-certification letters and make both the list and the self-certification letters publicly available.

To qualify for the safe harbor, an organization can (1) join a self-regulatory privacy program that adheres to the safe harbor's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the safe harbor.

WHAT DO THE SAFE HARBOR PRINCIPLES REQUIRE?

Organizations must comply with the seven safe harbor principles. The principles require the following:

Notice

Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can 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 for limiting its use and disclosure.

Choice

Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

Onward Transfer (Transfers to Third Parties)

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(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter 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.

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.

Security

Organizations must take reasonable precautions to protect personal information 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.

Enforcement

In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply

with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

To provide further guidance, the Department of Commerce has issued a set of frequently asked questions and answers (FAQs) that clarify and supplement the safe harbor principles.

HOW AND WHERE WILL THE SAFE HARBOR BE ENFORCED?

In general, enforcement of the safe harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's safe harbor commitments the force of law vis a vis that organization.

Private Sector Enforcement

As part of their safe harbor obligations, organizations are required to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings of non-compliance and deletion of data in certain circumstances. They may also include suspension from membership in a privacy program (and thus effectively suspension from the safe harbor) and injunctive orders.

The dispute resolution, verification, and remedy requirements can be satisfied in different ways. For example, an organization could comply with a private sector developed privacy seal program that incorporates and satisfies the safe harbor principles. If the seal program, however, only provides for dispute resolution and remedies but not verification, then the organization would have to satisfy the verification requirement in an alternative way.

Organizations can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities or by committing to cooperate with data protection authorities located in Europe.

Government Enforcement

Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or the states may provide overarching government enforcement of the safe harbor principles. Where a company relies in whole or in part on self-regulation in complying with the safe harbor principles, its failure to comply with such self regulation must be actionable under federal or state law prohibiting unfair and deceptive acts or it is not eligible to join the safe harbor. At present, U.S. organizations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation with respect to air carriers and ticket agents may participate in the safe harbor. The Federal Trade Commission and the Department of Transportation with respect to air carriers and ticket agents have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the safe harbor framework but then fail to live up to their statements.

Under the Federal Trade Commission Act, for example, a company's failure to abide by commitments to implement the safe harbor principles might be considered deceptive and actionable by the Federal Trade Commission. This is the case even where an organization adhering to the safe harbor principles relies entirely on self-regulation to provide the enforcement required by the safe harbor enforcement principle. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to \$12,000 per day for violations.

Failure to Comply with the Safe Harbor Requirements: If an organization persistently fails to comply with the safe harbor requirements, it is no longer entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

The Department of Commerce will indicate on the public list it maintains of organizations self certifying adherence to the safe harbor requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

Contact Us

1-800-USA Trade

- [Find a Local U.S. Office](#)
- [Find an Overseas Office](#)

Safe Harbor Workbook

This Safe Harbor workbook is designed to aid U.S. businesses assess their privacy policies and practices with respect to complying with the Safe Harbor privacy framework. Because implementation of the Safe Harbor will require you to consider your organization's specific needs, practices, and objectives, this guide does not constitute legal advice and is not intended to substitute for the services of legal counsel or other qualified professionals. The information in this publication is provided on an "as is" basis, and no warranty of the suitability of the advice offered for your organization is made by this publication.

INTRODUCTION: PRIVACY AND THE SAFE HARBOR FRAMEWORK

Today's information technologies allow information to be collected, compiled, analyzed, and delivered globally more quickly and inexpensively than ever before. Where it was once difficult, time-consuming, and expensive to obtain, compile, and analyze information, it is now often available with a few simple clicks of a computer mouse. Increased access to information facilitates personal and political expression as well as commerce, education, and health care. Consumers benefit from the increased access to information. Organizations benefit through reduced costs and client-focused advertising.

The advent of global communications and information flows also raises new challenges and opportunities for building processes to effectively protect privacy. Multinational organizations may centralize all human resources data in one location from their constituent affiliates around the world for record keeping, benefits, and payroll purposes; credit card organizations may do the same with bankcard information for billing purposes and account management. Citizens of one country may easily visit web sites in other countries, transferring personal information across borders as they visit. Laws, which generally are limited by nations' borders, may have little effect in a medium without borders.

Many nations share concerns about the impact of the expansion of electronic networks on information privacy. Indeed, converging technologies and mobile communications heighten the risk and the opportunity for accessing content, i.e., music downloads, text messaging, bill paying, and a host of other services now available on one's mobile phone. Recognizing the importance information and communications technologies play in the global economy and the need to transfer data across national boundaries, The United States and the European Union (EU)¹ address these concerns, but in markedly different ways. The European Commission proposes legislation, implements policy and enforces the Treaties. It has investigative powers and can take legal action against Member States or companies that violate Treaties or rules. The Commission manages the EC budget and represents the Union in trade negotiations. The terms of the EU Directive on Data Protection requires the Commission to determine the "adequacy" of data protection in third countries and to prohibit personal data flows to countries with privacy regimes that are not deemed "adequate." Organizations wishing to receive personally identifiable information from the European Union would have to provide "adequate" privacy protection.

The implications for countries such as the United States, which receive a significant number of data transfers EU Member States and, in 2002, had approximately \$379 billion in trade with the EU, are serious. Data transfers are the lifeblood of many organizations and the underpinnings for all of electronic commerce. Multinational organizations routinely share among their different offices a vast array of personal information. This information can be as simple as personnel telephone directories to more sensitive information such as

personnel records, insurance information needed to process medical claims, credit card billing information, or patient information essential for conducting pharmaceutical research on new drugs.

Accordingly, the United States initiated a high-level informal dialogue, led by the U.S. Department of Commerce's International Trade Administration and the European Commission Directorate for Internal Market, with the goals of ensuring the free flow of data and effective protection of personal data. These discussions led to the development of a "Safe Harbor" framework based on principles that reflect the U.S. approach to privacy and, at the same time, meet the European Directive's "adequacy" requirements. These principles were deemed "adequate" by the European Commission in July 2000. The Safe Harbor became effective on November 1, 2000.

This workbook provides further guidance on how U.S. organizations can comply with the Safe Harbor privacy principles. This is for information only and creates no legally binding effects.

SECTION I: PRIVACY IN THE UNITED STATES AND THE EUROPEAN UNION

Introduction

Objectives

At the end of this section, you should be able to

- Understand the impact of differing national law, and
- Know the differences in approaches to privacy in the U.S. and Europe.

Many fear that privacy concerns can stunt the growth of electronic commerce. Without confidence that data provided on-line will be protected and used responsibly, users will not take full advantage of the benefits that electronic commerce offers. No amount of marketing, attractive pricing or convenience will spur on-line users to conduct business on-line if they believe that doing so will unduly compromise the privacy of their personal information.

The United States, the E.U. and its member states are committed to making privacy protections available to their citizens without unnecessarily impeding the free flow of information. The United States has largely adopted a self-regulatory approach to the development of privacy protections in the private sector, addressing specific privacy concerns in the law as needed. The concern is that privacy issues differ across industry sectors, and that "a one size fits all" legislative approach would lack the necessary precision to avoid interfering with the benefits that result from the free flow of information. Nonetheless, the United States does address specific privacy concerns in the law as needed, particularly where sensitive information is involved or there have been cases of abuses. In Europe, however, privacy laws tend to be comprehensive, applying to every industry and closely regulating what data is collected and how it is used.

U.S. Approach to Privacy

In the United States, the importance of protecting the privacy of individuals' personal information is a priority for the federal government and consumers. Consumers repeatedly cite fears that their personal information will be misused as a reason for not doing business online. In this way, moves to bolster on-line privacy protect consumer interests and fuel the broader growth of on-line communications, innovation, and business. Self-regulatory initiatives are an effective approach to putting meaningful privacy protections in place. In certain highly sensitive areas, however, legislative solutions are appropriate. These sensitive areas include financial and medical records, genetic information, Social Security numbers, and information involving children.

A self-regulatory initiative could involve a number of companies in the same line of business deciding that they will follow certain rules in handling information about their customers. These companies might also decide to display a seal that shows that they follow the rules. If one of the members of this "self-regulatory regime" breaks the rules, the company's membership and permission to display the seal will be revoked. Companies across industries -- and especially in Internet-related fields -- are increasingly hiring privacy

experts and making the protection of consumer information a priority. The continuing introduction of new technologies designed to protect the privacy of personal information will have a profound effect on empowering consumers to control how their personal information is used. The federal government continues in its mission to be a model citizen of cyberspace in its information practices. The goal is for the government to serve as an example for private companies, as well as state and local governments.

The United States has supported legislative solutions in certain sensitive areas. In 1999, Congress passed and President signed into law the Financial Modernization Act which included significant new privacy protections for financial information. In addition, the Administration has issued rules guaranteeing the privacy of medical information under the Health Insurance Portability and Accountability Act of 1996. In 1998, the Administration worked with Congress to pass the Children's Online Privacy Protection Act (COPPA). COPPA requires commercial web sites that target children under the age of 13 to obtain verifiable parental consent before they gather information from children under age thirteen.

The European Approach

While the United States and EU generally agree on the underlying fair information principles, they employ different means to achieve this goal. The EU's approach to privacy grows out of Europe's history and legal traditions. In Europe, protection of information privacy is viewed as a fundamental, human right. Europe also has a tradition of prospective, comprehensive lawmaking that seeks to guard against future harms, particularly where social issues are concerned.

The EU began examining the impact of technology on society over a fifteen years ago; the inquiry culminated in the adoption of a directive in July 1995 specifically addressing privacy issues. The European Community's Directive on Data Protection took effect in October 1998. Member States were required to bring into force laws, regulations, and administrative provisions to comply with the Directive by its effective date.

The European Union Directive on Data Protection

A quick review of the Directive's basic terms makes clear that, consistent with European tradition, the Directive takes a regulatory and comprehensive approach to privacy issues. It has two basic objectives: first, to protect individuals with respect to the "processing" of personal information; and second, to ensure the free movement of personal information within the EU through the coordination of national laws (Article 1).

Personal information is defined as information relating to an identified or identifiable natural person. 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 (Article 2).

The scope of the Directive is very broad. It applies to all processing of data, on-line and off-line, manual as well as automatic, and all organizations holding personal data. It excludes from its reach only data used "in the course of purely personal or household activity" (Article 3). The Directive establishes strict guidelines for the processing of personal information. "Processing" includes any operations involving personal information, except perhaps its mere transmission (Article 2). For example, copying information or putting it in a file is viewed as "processing." The substantive aspects of the Directive's privacy protections are based on the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the Organization for Economic Cooperation and Development (OECD) in 1981.

Data Quality. The Directive requires that all personal information must be processed fairly and lawfully, so that, for example, a person whose personal information is at issue knows that it is being collected and used and must be informed of the proposed uses. Furthermore, the use of personal information must be limited to the purpose first identified and to other compatible uses, and no more information may be collected than is required to satisfy the purpose for which it is collected. In other words, the theory is that if a person provides information to obtain telephone service, that information should not be used to target that person for information about vacation trips, nor should information relevant to a customer's interests in vacation trips be required to get, for instance, telephone service. Information must also be kept accurate and up to date (Article 6).

Legitimate Data Processing. The Directive sets forth rules for "legitimate" data processing. Most basically, this requires obtaining the consent of the data subject before information is processed unless specific

exemptions apply (Article 7). In addition, certain information must be provided to data subjects when their personal information is processed (Article 10), such as whether they have rights to see the data, to correct any information that is inaccurate, or to know who will receive the data (Article 12).

Sensitive Data. "Sensitive" data, such as that pertaining to racial or ethnic origins, political or religious beliefs, or health or sex life, may not be processed at all unless such processing comes within limited exceptions, for example if the individual gives explicit consent (Article 8).

Security. The Directive requires that "appropriate technical and organizational measures to protect data" against destruction, loss, alteration, or unauthorized disclosure or access be taken (Article 17).

Data Controllers. The Directive requires those processing data to fulfill very specific requirements. Specifically, they must appoint a "data controller" responsible for all data processing, who must register with government authorities (Article 19) and notify them before processing any data (Article 18). Notification must at a minimum include: the purpose of the processing; a description of the data subjects; the recipients or categories of recipients to whom the data might be disclosed; proposed transfers to third countries; and a general description that would allow a preliminary assessment of whether requirements for security of processing have been met (Article 19).

Government Data Protection Authorities. The Directive also mandates a government authority to oversee data processing activities. Each Member State must establish an independent public authority to supervise the protection of personal data. These "Data Protection Commissions" must have the power to: (1) investigate data processing activities and monitor application of the Directive; and (2) intervene in the processing and to order the blocking, erasure, or destruction of data as well as to ban its processing. They must also be authorized to hear and resolve complaints from data subjects and must issue regular public reports on their activities (Article 28).

Transfers of Data Outside the EU. Most importantly from the U.S. perspective, the Directive requires that Member States enact laws prohibiting the transfer of personal data to countries outside the European Union that fail to ensure an "adequate level of [privacy] protection" (Article 25). Where the level of protection is deemed inadequate, Member States are required to take measures to prevent any transfer of data to the third country. Member States and their Data Protection Commissions must inform each other when they believe that a third country does not ensure an adequate level of protection.

SECTION II: OVERVIEW OF THE SAFE HARBOR FRAMEWORK

Objectives

At the end of this session, you should be able to:

- Describe the Safe Harbor arrangement and its benefits;
- Determine what organizations may join the Safe Harbor; and
- Understand how the arrangement will be enforced.

Introduction

The Safe Harbor framework was developed by the U.S. Department of Commerce, in consultation with the European Commission, industry and non-governmental organizations to provide U.S. organizations with a streamlined means of satisfying the "adequacy" requirement under the European Directive on Data Protection. U.S. organizations wishing to legally receive personal information from European organizations legally either must join the safe harbor, satisfy one of the Directive's other exceptions, or seek an "adequacy" determination. For example, personal data that is necessary to complete a contract between an individual and the company may be transferred without an "adequacy" determination, and data importing companies may receive such data if they enter into contracts with data exporting companies that bind the data importer to provide "adequate" privacy protection (See Article 26).

Description of the Safe Harbor Framework

The Safe Harbor framework is set forth in a set of seven privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision, the exchange of letters between the Department and the European Commission, and letters from the Department of Transportation and Federal Trade Commission on their enforcement powers. Understanding the Safe Harbor requires familiarity with all of these documents. The Safe Harbor can apply to all personal information transferred from the European Union - whether collected on or off-line and whether it is within the scope of the Directive. Decisions by U.S. organizations to enter the Safe Harbor are entirely voluntary.

A "flexible implementation period", a political agreement by the EU to use discretion regarding enforcement to avoid disrupting data flows to U.S. organizations during the implementation period, remains in effect. A joint Department of Commerce and European Commission review of the implementation of the Safe Harbor was completed in January 2002. During this review, the Commission and Department officials discussed a range of implementation issues. In particular, they: 1) verified that all of the elements required by the framework are in place; 2) discussed the "visible compliance" of current safe harborites to the Safe Harbor privacy principles and Frequently Asked Questions; 3) discussed the progress of the Department's outreach and education plan; and 4) reviewed the alternative dispute resolution mechanisms named by current harborites.

Both sides were pleased to see that membership has grown significantly in recent months, but efforts need to continue to explain the advantages of joining the Safe Harbor. In addition, the importance of future cooperation between the U.S. and the EU in order to ensure continued data-flows was emphasized. Furthermore, the Commission reaffirmed its commitment to inform the Department if it becomes aware of any actions that may interrupt data flows to the U.S. and stated that it sees no reason to expect any change in policy regarding the "flexible implementation period".

Benefits of Implementing the Safe Harbor Framework

The Safe Harbor provides predictability and continuity for those EU organizations that send personal information to the United States and U.S. organizations that receive personal information from the EU. All 15 Member States are bound by the European Commission's finding of adequacy. The Safe Harbor either eliminates the need for prior approval to begin data transfers or provides for automatic approvals. It provides for a flexible privacy regime more congenial to the U.S. approach to privacy and, for the most part, enforcement will be conducted in the United States (as opposed to Europe). The Safe Harbor privacy principles offer a simpler and more efficient means of complying with the adequacy requirements of the Directive, which should particularly benefit small and medium enterprises.

In addition to the specific benefits that flow from joining the Safe Harbor, developing a privacy policy can be a good business decision for U.S. organizations. By developing a well-thought out, carefully implemented privacy policy, and a policy that is compliant with the Safe Harbor, if your organization receives personally identifiable information from the EU, such a policy will, increase its customers' confidence. A privacy policy should be seen as a critical piece of any overall business strategy, particularly an international business strategy, as well as a critical piece of its electronic commerce strategy.

For example, by providing customers with choice about how your organization uses their personal information, you can reduce the possibility that you will lose sales because your customers are concerned about use of their data.

What Organizations May Join the Safe Harbor

Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. The Federal Trade Commission and the Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the Safe Harbor framework but then fail to live up to their statements. Please note that certain sectors are not subject to the jurisdiction of either the FTC or the DoT, and thus may not be eligible for Safe Harbor. Organizations that are telecommunications common carriers, meat packers, banks, insurance companies, credit unions or not-for-profits may not be eligible for Safe Harbor. If you are considering joining Safe Harbor, but are not certain whether your organization falls

within the jurisdiction of either the FTC or the DoT, it is recommended that you contact those agencies for further guidance.

What Organizations Should Join the Safe Harbor

Organizations that receive personally identifiable information from EU Member States are required to demonstrate that they provide "adequate" privacy protections. Organizations that receive personally identifiable information and have not identified either another basis for demonstrating "adequacy" or a relevant exception in the Directive should consider joining the Safe Harbor as one means of meeting the Directive's "adequacy" requirements. Though not necessary to comply with U.S. law, companies that wish to demonstrate to their customers that they provide a high level of privacy protection may also consider joining the Safe Harbor, recognizing that the Safe Harbor is only applicable to transfers of personally identifiable data from the European Union to the United States.

How Do Organizations Join the Safe Harbor

Organizations that decide to participate in the Safe Harbor must comply with the Safe Harbor's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization needs to reaffirm its self-certification annually to the Department of Commerce, indicating that it continues to adhere to the Safe Harbor's requirements, and of course, it must continue to abide by the Safe Harbor requirements. As set forth in FAQ 6, it also required that the organization state in its published privacy policy statement that it adheres to the Safe Harbor privacy principles.

The Department of Commerce maintains a list of all organizations that register through the website or through a letter. An EU organization can ensure that it is sending information to a U.S. organization participating in the Safe Harbor by viewing the public list of Safe Harbor organizations posted on the Department of Commerce's website (<http://export.gov/safeharbor>). This list became operational in November 2000. The list is updated regularly, so that it is clear who is in the Safe Harbor.

How and Where will the Safe Harbor be Enforced

In general, enforcement of the Safe Harbor takes place in the United States in accordance with U.S. law and relies, to a great degree, on enforcement by the private sector. The Safe Harbor private sector enforcement has three components: verification, dispute resolution, and remedies. Organizations are required to have procedures for verifying compliance; to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes; either independent or self-assessment; and to remedy problems arising out of a failure to comply with the principles. Provision is also made for U.S. organizations to cooperate with European Data Protection Authorities to satisfy the dispute resolution and remedy requirements or where human resources data is involved. (See introductory paragraph of the principles for further guidance).

Private sector self regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive trade practices statutes. The effect of these statutes is to give an organization's Safe Harbor commitments the force of law vis-a-vis that organization.

Depending on the industry sector, the Federal Trade Commission or the Department of Transportation provide overarching government enforcement of the Safe Harbor principles. Where an organization relies in whole or in part on self regulation in complying with the safe harbor principles, its failure to comply with such self regulation must be actionable under federal or state law prohibiting unfair and deceptive acts or it is not eligible to join the safe harbor. (Note: It is possible that an annex to the Safe Harbor principles will contain a list of additional U.S. governmental enforcement agencies recognized by the European Commission. It is possible that this list will expand as more agencies declare their willingness to enforce the Safe Harbor).

Failure to Comply with the Safe Harbor Requirements

If a U.S. Safe Harbor organization persistently fails to comply with the Safe Harbor requirements, it is no longer entitled to benefit from the Safe Harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its

claim to comply is no longer credible. In these cases, the U.S. Safe Harbor organization must promptly notify the Department of Commerce [by letter or by email] of such facts. The Safe Harbor list will indicate that there has been a persistent failure to comply and the communication from the enforcement body will be made public 30 days after the Department of Commerce receives the notification.

The list maintained by the Department of Commerce will indicate any notifications the Department receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of Safe Harbor benefits.

Determining what your privacy policy should contain

In order for a privacy policy to be compliant with the Safe Harbor, the policy must address the seven privacy principles and any relevant points that are covered in the frequently asked questions (FAQs) and reflect the organization's actual and anticipated information handling practices. For instance, FAQ 6 requires that you state that you are in compliance with the Safe Harbor privacy principles. Please note that important exceptions are contained in the introductory paragraphs of the principles (as well as in other Safe Harbor documents) and your organization needs to take these into account as well. It is important to write a policy that is clear, concise, and easy to understand.

Safe Harbor Principles

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.

Notice is a key element of any privacy policy. In order for consumers to make informed decisions about what information they provide, they must understand what data is being collected, for what purposes the data is being collected, how that data is used, how to contact the organization with inquiries or complaints, the types of third parties to which the information may be disclosed, the choices and means the organization offers individuals for limiting its use and disclosure, and how it is secured. By providing notice to customers about your data collection practices, you enable consumers to make informed decisions about their on-line activities. **Note that for a third party which is acting as an agent, notice and choice do not need to be provided.**

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. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

Choice ensures that consumers have choices regarding the collection of their personal data. For example, individuals who do not wish that their data be used as described in the privacy policy can choose not to have their data shared, have complimentary goods and services marketed to them, have their data sold to third parties or used in other ways. By providing customers the option of choice, you can also reduce the possibilities that you will lose sales because your customers are concerned about the use of their data. **An organization must offer individuals the opportunity to opt out of two situations: if an organization discloses personal information to third parties, even for the same purpose for which it was originally collected or subsequently authorized; or where the information may be used by the collecting organization for a purpose which is "incompatible" with the purpose for which it was originally collected or subsequently authorized by the individual.**

Safe Harbor Sensitive Information Principle: 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.

For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

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 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.

This principle is intended to assure that there is as little "leak-out" of data from Safe Harbor protections as possible. In certain circumstances, if you know someone is doing wrong, such as misusing property for which you are responsible, or misbehaving in a situation for which you have responsibility and you don't stop them, you bear some responsibility for the consequences. This principle provides some on-going responsibility for data transferred pursuant to the Safe Harbor. In Europe, this responsibility would be provided by data protection laws. Since omnibus data protection laws do not exist in the United States, we have adopted this principle.

This concept is neither new nor novel in the U.S. legal system. An employer's responsibility to provide a workplace free from hazardous situations, including careless or reckless employees, is one example. An employer's responsibility to provide a workplace free from a hostile atmosphere of sexual harassment is another example. Senior officers of organizations can be held personally responsible for the acts of lower-level employees for certain violations of the laws. What is novel is the application of this concept to the personal information relating to individuals.

A Safe Harbor participant will not be deemed to violate the principles if a transferee misuses data, provided the Safe Harbor transferor has satisfied the requirements of the principle.

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.

The principle of security applies to how your organization stores, processes, maintains and protects customer information. Organizations should take steps to secure personally identifiable information. It does little good to have a strict privacy policy if personal data is available to any employee or if your computer systems and paper files are not secured.

Organizations must take more care to protect sensitive information, as it is defined in the principles.

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.

The data integrity principle minimizes the risk that personal information would be misused or abused because the organization is collecting only relevant information, there is less opportunity to misuse and abuse personal information. You also avoid the risk that decisions will be based upon erroneously or inappropriate information.

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. See FAQ 8

Customers are not only concerned about what data is being collected about them, they are also concerned that this information is correct and timely. Providing access to the data that you have collected about an

individual allows that person to check the stored information and ensure that it is up-to-date and correct, and that the organization is doing what it says it is doing about collecting and retaining data.

Allowing customers to access and correct information collected about them can greatly increase customer's confidence by assuring users that they will only receive further information about other goods and services that are of interest to them (if your organization re-markets goods and services either internally or through sale of information to third parties) or that their goods will be delivered promptly and properly. At the same time, your organization benefits from having accurate customer information.

The question of how and to what extent a customer should have access to their data requires a nuanced response. The obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. The sensitivity of the data is also important in considering whether access should be provided. See FAQ 8 for additional information about when access must be provided.

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. (See FAQ 11 for additional information about enforcement required under the Safe Harbor.)

The Safe Harbor private sector enforcement has three components: verification, dispute resolution, and remedy. Organizations are required to have procedures for verifying compliance, either independent or self-assessment, to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes, and to remedy problems arising out of a failure to comply with the principles.

Verification

To meet the second requirement of the enforcement principle, verification, an organization may use a self-assessment or an outside/third-party assessment program

Self -Assessment. Under the self-assessment approach, verification would indicate that an organization's published safe harbor privacy policy is accurate, comprehensive, prominently displayed, completely implemented, accessible and conforms to the Safe Harbor principles. It would also need to indicate that appropriate employee training is in place and that internal procedures for periodically conducting objective reviews of compliance are in place. A statement verifying the self- assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year.

Outside Assessment. Where the organization has chosen outside compliance review, the review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor privacy principles, that it is being complied with and that customers are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys," or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year.

The method of verification should be included in the privacy statement. For additional guidance on verification see FAQ 7.

Dispute Resolution Mechanism

By providing a means of redress, organizations assure consumers that they are committed to resolving any privacy concerns that they may have. Organizations should clearly state how consumers who feel that their

privacy may have been violated based on the Safe Harbor privacy principles should contact the organization and what steps the organization will take to resolve such issues.

Selecting a dispute resolution mechanism

A third-party dispute resolution mechanism assures your customers that your organization is complying with its stated policies. While programs vary, organizations such as BBBOnLine, the Direct Marketing Association, the Privacy Council and the Entertainment Software Rating Board have indicated that they have developed privacy programs that allow companies to comply with the Safe Harbor privacy principle on enforcement. Other programs such as an outside arbitration and mediation service (e.g. JAMS or the American Arbitration Association) may also be used, so long as every complaint is heard in compliance with the enforcement principle and FAQ 11. (Note: Organizations self-certifying to the Safe Harbor are responsible for ensuring that they have chosen a dispute resolution provider that will satisfy the requirements of the framework. The Department of Commerce does not certify programs in order to serve as dispute resolution mechanisms under Safe Harbor. Therefore, the Department of Commerce cannot guarantee that a particular program will meet all Safe Harbor requirements, including those under FAQ 11).

Alternatively, organizations may choose to cooperate with the European Data Protection Authorities. In this instance an organization must comply with procedures outlined in FAQ 5. In the instance of human resources data, the organization must agree to cooperate with the data protection authority for handling complaints. Moreover, this option is necessary in situations where a transfer is to a business that is not regulated. Additional guidance is provided in FAQ 9 for the handling of human resources data.

Please note that organizations who choose to utilize the European Data Protection Authorities for dispute resolution will be required to pay an annual fee of US \$50 in order to cover the operating costs of the Data Protection Authorities' panel. This fee is payable to the United States Council for International Business (c/o Mr. Paul Cronin, U.S. Council for International Business (USCIB); 1212 Avenue of the Americas; New York, NY 10036), which has agreed to act as trusted third party for this purpose.

Please see FAQ 5 for more details regarding the role of the Data Protection Authorities. Should you need further information on how to carry out the payment, please contact Mr. Paul Cronin, USCIB, at 212-354-4480, or pcronin@uscib.org. If, on the other hand, you require more information on how the cooperation/compliance with the EU DPAs works, you can contact the Secretariat of the Data Protection Panel at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/.

Characteristics of effective dispute resolution mechanisms

Whatever type of service is selected, it must meet certain basic criteria. The Safe Harbor privacy principles identify the following as necessary elements for any effective dispute mechanisms: readily available and affordable independent recourse mechanisms by which individual's complaints and disputes are investigated and resolved by reference to the principles; damages awarded where the applicable law or private sector initiatives so provide; obligations to remedy problems arising out of failure to comply with the principles; sanctions that are sufficiently rigorous to ensure compliance by organizations; and notification of persistent failures of Safe Harbor organizations to comply with their rulings to governmental body with applicable jurisdiction or to the courts, as appropriate, and the Department of Commerce.

Evaluating a dispute resolution mechanism

When evaluating a third-party service, keep your own business processes in mind. Make sure that the services offered provide your customers the assurance that they seek and your organization the support it needs without impeding your regular operations. As with any service, take care to clarify the services that will be provided to you, spell out the terms of use of any icons or graphics that identify your organization as a subscriber, and understand what your obligations are before entering into any binding arrangement.

Once an organization has selected an appropriate dispute resolution mechanism, this information should be made readily available to the consumer through the privacy policy. For additional requirements pertaining to dispute resolution, see FAQ 11.

Remedies and Sanctions

The dispute resolution body that is chosen must provide sufficiently rigorous sanctions to ensure compliance by organizations. The remedies should be such that noncompliance is reversed or corrected and future processing is in conformity with the safe harbor principles. Sanctions should include both publicity for non-compliance and deletion in certain instances. In instances of persistent failure to comply the dispute resolution body must have the ability to notify such failures to a governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce.

Review of FAQs

In addition to the principles there are 15 FAQs. It is important to review these 15 FAQs to see if any of the sector specific FAQs apply to your organization. For example, FAQ 2 provides an explanation of the exceptions for journalists, FAQ 14 provides additional guidance for handling information dealing with pharmaceuticals and medicals products, and FAQ 15 provides additional guidance on how publicly available information should be handled. Familiarize yourself with the contents of these FAQs generally and make sure your policies conform with these as well.

Safe Harbor List Procedures

- To be included on the Safe Harbor list, organizations must notify the Department of Commerce that they adhere to the Safe Harbor privacy principles developed by the Department of Commerce in coordination with the European Commission. The principles provide guidance for U.S. organizations on how to provide "adequate protection" for personal data from Europe as required by the European Union's Directive on Data Protection.
- An organization's request to be put on the Safe Harbor list, and its appearance on this list pursuant to that request, constitute a representation that it adheres to a privacy policy that meets the Safe Harbor privacy principles.
- Observance of the Safe Harbor Principles and subscription to the list are entirely voluntary. An organization's absence from the list does not mean that it does not provide effective protection for personal data or that it does not qualify for the benefits of the Safe Harbor.
- In order to keep this list current, a notification will be effective for a period of twelve months. Therefore, organizations need to notify the Department of Commerce every twelve months to reaffirm their continued adherence to the Safe Harbor Principles.
- Organizations should notify the Department of Commerce either by email or letter if their representation to the Department is no longer valid. Failure by an organization to so notify the Department could constitute a misrepresentation of its adherence to the Safe Harbor privacy principles and failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).
- An organization may withdraw from the list at any time by notifying the Department of Commerce in writing or by email. Withdrawal from the list terminates the organization's representation of adherence to the Safe Harbor Principles, but this does not relieve the organization of its obligations with respect to personal information received prior to the termination.
- If a relevant self-regulatory or government enforcement body finds an organization has engaged in a persistent failure to comply with the principles, then the organization is no longer entitled to the benefits of the Safe Harbor.
- To be included in the Safe Harbor List, organizations may either send a letter signed by a corporate officer to the Department of Commerce, which includes all the information required or have a corporate officer register on the Safe Harbor website (<http://export.gov/safeharbor/>). Complete the self-certification application, keep a copy for your records, and submit the form to the Department of Commerce's Safe Harbor Team. **IMPORTANT: Verify that all the information required in FAQ 6 is included in the submission.**
- In maintaining the list, the Department of Commerce does not assess and makes no representation as to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.

Last updated on June 8, 2007.

Information Required for Safe Harbor Certification

To expedite the certification process, please compile the following information before you go online to certify your organization's participation.

1. Organization Information:

- Name
- Address
- City
- State
- Zip
- Phone
- Fax
- Website (Optional)

2. Organization Contact Information (for the handling of complaints, access requests, and any other issues arising under the safe harbor):

- Contact Office
- Contact Name (Optional)
- Contact Title (Optional)
- Contact Phone
- Contact Fax
- Contact Email

3. Corporate Officer who is certifying the organization's adherence to the safe harbor framework:

- Corporate Officer Name
- Corporate Officer Title
- Corporate Officer Phone
- Corporate Officer Fax
- Corporate Officer Email

4. Description of the activities of the organization with respect to personal information received from the EU.

5. Description of the organization's privacy policy for personal information:

- Effective date of your organization's privacy policy
- Location of your organization's privacy policy
- 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 (and that is listed in the Annex to the Principles): (Federal Trade Commission or Department of Transportation)
- Information on any privacy programs relevant to the safe harbor in which the organization is a member
- Method of your organization's verification (e.g., In-house, Third Party. (See [FAQ 7](#))
- Independent recourse mechanism(s) available to investigate unresolved complaints (e.g., private sector developed privacy program that incorporates the Safe Harbor Principles, legal or regulatory supervisory authorities that provide for the handling of individual complaints and dispute resolution, or EU data protection authorities. (See [FAQ 11](#))
- Data Covered by the safe harbor (e.g., off-line, on-line, manually processed data, human resources data)

6. Additional Information Required

- EU Countries that you receive information from: (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Spain, Sweden, United Kingdom)
- Industry Sector - you can select up to 3 sectors ([View Safe Harbor Industry Sectors](#))
- Level of organization sales (this information will not be posted on the website)

- Number of employees (this information will not be posted on the website)

Safe Harbor Enforcement Overview

Federal and State "Unfair and Deceptive Practices" Authority and Privacy

This memorandum outlines the authority of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act (15 U.S.C. §§ 41-58, as amended) to take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments to do so. It also addresses the exceptions to that authority and the ability of other federal and state agencies to take action where the FTC does not have authority.(1)

FTC Authority over Unfair or Deceptive Practices

Section 5 of the Federal Trade Commission Act declares "unfair or deceptive acts or practices in or affecting commerce" to be illegal. 15 U.S.C. § 45(a)(1). Section 5 confers on the FTC the plenary power to prevent such acts and practices. 15 U.S.C. § 45(a)(2). Accordingly, the FTC may, upon conducting a formal hearing, issue a "cease and desist" order to stop the offending conduct. 15 U.S.C. § 45(b). If it would be in the public interest to do so, the FTC can also seek a temporary restraining order or temporary or permanent injunction in U.S. district court. 15 U.S.C. § 53(b). In cases where there is a widespread pattern of unfair or deceptive acts or practices, or where it has already issued cease and desist orders on the matter, the FTC may promulgate an administrative rule prescribing the acts or practices involved. 15 U.S.C. § 57a.

Anyone who does not comply with an FTC order is subject to a civil penalty of up to \$11,000, with each day of a continuing violation constituting a separate violation.(2) 15 U.S.C. § 45(l). Likewise, anyone who knowingly violates an FTC rule is liable for \$11,000 for each violation. 15 U.S.C. § 45(m). Enforcement actions can be brought by either the Department of Justice, or if it declines by the FTC. 15 U.S.C. § 56.

FTC Authority and Privacy

In exercising its Section 5 authority, the FTC takes the position that misrepresenting why information is being collected from consumers or how the information will be used constitutes a deceptive practice.(3) For example, in 1998, the FTC filed a complaint against GeoCities for disclosing information it had collected on its Web site to third parties for purposes of solicitation, and without prior permission, despite its representations to the contrary.(4) The FTC staff has also asserted that the collection of personal information from children, and sale and disclosure of that information, without the parents' consent is likely to be an unfair practice.(5)

In a letter to Director General John Mogg of the European Commission, FTC Chairman Pitofsky noted the limitations on the FTC's authority to protect privacy where there has not been a misrepresentation (or no representation at all) as to how the information collected will be used. FTC Chairman Pitofsky letter to John Mogg (September 23, 1998). However, companies that want to avail themselves of the proposed "safe harbor" will have to certify that they will protect the information they collect in accordance with prescribed guidelines. Consequently, where a company certifies that it will safeguard the privacy of information and then fails to do so, such action would be a misrepresentation and a "deceptive practice" within the meaning of Section 5.

As the FTC's jurisdiction extends to unfair or deceptive acts or practices "in or affecting commerce," the FTC will not have jurisdiction over the collection and use of personal information for noncommercial purposes, charitable fund-raising for example. See Pitofsky letter, p. 3. However, the use of personal information in any commercial transaction will satisfy this jurisdictional predicate. Thus, for example, the sale by an employer of personal information on its employees to a direct marketer would bring the transaction within the purview of Section 5.

Section 5 Exceptions

Section 5 establishes exceptions to the FTC's authority over unfair or deceptive acts or practices with respect to:

- financial institutions, including banks, savings and loans, and credit unions;
- telecommunications and interstate transportation common carriers;
- air carriers; and
- packers and stockyard operators.

See 15 U.S.C. § 45(a)(2). We discuss each exception, and the regulatory authority that takes its place, below.

State "Unfair and Deceptive Practices" Authority

According to an analysis prepared by FTC staff, "All fifty states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws more or less like the Federal Trade Commission Act ("FTCA") to prevent unfair or deceptive trade practices." FTC fact sheet, reprinted in Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, *59 Tul. L. Rev. 427 (1984)*. In all cases, an enforcement agency has the authority "to conduct investigations through the use of subpoenas or civil investigative demands, obtain assurances of voluntary compliance, to issue cease and desist orders or obtain court injunctions preventing the use of unfair, unconscionable or deceptive trade practices." *Id.* In 46 jurisdictions, the law allows private actions for actual, double, treble, or punitive damages and, in some cases, recovery of costs and attorney's fees. *Id.*

Florida's Deceptive and Unfair Trade Practices Act, for example, authorizes the attorney general to investigate and file civil actions against "unfair methods of competition, unfair, unconscionable or deceptive trade practices," including false or misleading advertising, misleading franchise or business opportunities, fraudulent telemarketing, and pyramid schemes. See also N.Y. General Business Law § 349 (prohibiting unfair acts and deceptive practices carried out in the course of business).

A survey conducted this year by the National Association of Attorneys General (NAAG) confirms these findings. Of forty-three states that responded, all have "mini-FTC" statutes or other statutes that provide comparable protection. Also according to the NAAG survey, 39 states indicated they would have the authority to hear complaints by non-residents. With respect to consumer privacy, in particular, 37 out of forty-one states that responded indicated that they would respond to complaints alleging that a company within their jurisdiction was not adhering to its self-declared privacy policy.

1. We do not discuss here all the various Federal statutes that address privacy in specific contexts or state statutes and common law that might apply. Statutes at the federal level that regulate the commercial collection and use of personal information include the Cable Communications Policy Act (47 U.S.C. § 551), the Driver's Privacy Protection Act (18 U.S.C. § 2721), the Electronic Communications Privacy Act (18 U.S.C. § 2701 *et seq.*), the Electronic Funds Transfer Act (15 U.S.C. §§ 1693, 1693m), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), the Right to Financial Privacy Act (12 U.S.C. § 3401 *et seq.*), the Telephone Consumer Protection Act (47 U.S.C. § 227), and the Video Privacy Protection Act (18 U.S.C. § 2710), among others. Many states have analogous legislation in these areas. See, e.g., Mass. Gen. Laws ch. 167B, § 16 (prohibiting financial institutions from disclosing customer's financial records to a third party without either

the customer's consent or legal process), N.Y. Pub. Health Law § 17 (limiting use and disclosure of medical or mental health records and giving patients the right of access thereto).

2. In such an action, the United States district court can also order injunctive and equitable relief appropriate to enforcing the FTC order. 15 U.S.C. § 45(l)

3. "Deceptive practice" is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion.

4. See www.ftc.gov/opa/1998/9808/geocitie.htm.

5. See staff letter to Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. In addition, the Children's Online Privacy Protection Act of 1998 confers on the FTC specific legal authority to regulate the collection of personal information from children by website and online service operators. See 15 U.S.C. §§ 6501-6506. In particular, the act requires online operators to give notice and to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. *Id.*, § 6502(b). The act also gives parents a right of access and to refuse permission for the continued use of the information. *Id.*

6. On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act (Pub. L. 106-102, codified at 15 U.S.C. § 6801 *et seq.*) into law. The Act limits the disclosure by financial institutions of personal information about their customers. The Act requires financial institutions to, *inter alia*, notify all customers of their privacy policies and practices with respect to the sharing of personal information with affiliates and non-affiliates. The Act authorizes the FTC, the Federal banking authorities and other authorities to promulgate regulations to implement the privacy protections required by the statute. The agencies have issued proposed regulations for this purpose.

7. By its terms, this exception does not apply to the securities sector. Therefore, brokers, dealers and others in the securities industry are subject to the concurrent jurisdiction of the Securities and Exchange Commission and the FTC with respect to unfair or deceptive acts and practices.

8. The exception in Section 5 originally referred to the Federal Home Loan Bank Board which was abolished in August 1989 by the Financial Institutions Reform, Recovery and Enforcement Act of 1989. Its functions were transferred to the Office of Thrift Supervision and to the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, and the Housing Finance Board.

9. While removing financial institutions from the FTC's jurisdiction, Section 5 also stipulates that whenever the FTC issues a rule on unfair or deceptive acts and practices, the financial regulatory Boards should adopt parallel regulations within 60 days. See 15 U.S.C. § 57a(f)(1).

10. "The business of insurance, and every person engaged therein, shall be subject to the laws of the several States which relate to the regulation or taxation of such business." 15 U.S.C. § 1012(a).

11. The FTC has exercised jurisdiction over insurance companies in different contexts. In one case, the FTC took action against a firm for deceptive advertising in a state in which it was not licensed to do business. The FTC's jurisdiction was upheld on the basis that there was no effective state regulation because the firm was effectively beyond the reach of the state. See *FTC v. Travelers Health Association*, 362 U.S. 293 (1960).

As for the states, seventeen have adopted the model "Insurance Information and Privacy Protection Act" prepared by the National Association of Insurance Commissioners (NAIC). The Act includes provisions for notice, use and disclosure, and access. Also, almost all states have adopted the NAIC's model "Unfair Insurance Practices Act," which specifically targets unfair trade practices in the insurance industry.

12. The term "customer proprietary network information" means information that relates to "the quantity, technical configuration, type, destination, and amount of use of a telecommunications service" by a customer and telephone billing information. 47 U.S.C. § 222(f)(1). However, the term does not include subscriber list information. *Id.*

13. The legislation does not expressly define "personally identifiable information."

14. This authority encompasses the right to redress for privacy violations under both section 222 of the Communications Act or, with respect to cable subscribers, under section 551 of the Cable Act amendment to the Act. See also 47 U.S.C. § 551(f)(3) (civil action in federal district court is a nonexclusive remedy, offered "in addition to any other lawful remedy available to a cable subscriber.")

15. However, the absence of direct damage to a complainant is not grounds to dismiss a complaint. 47 U.S.C. § 208(a).

16. We understand there are efforts underway within the industry to address the privacy issue. Industry representatives have discussed the proposed safe harbor principles and their possible application to air carriers. The discussion has included a proposal to adopt an industry privacy policy with participating firms expressly subjecting themselves to DOT authority.

Privacy and FAQ Letter

July 17, 2000

Mr. John Mogg
Director DG Internal Market
European Commission
Office C 107-6/72
Rue de la Loi, 200
1049 Brussels
BELGIUM

Dear Mr. Mogg:

I am pleased to provide you with several documents: 1) the "Safe Harbor Privacy Principles," issued by the U.S. Department of Commerce on July 21, 2000; 2) Frequently Asked Questions (FAQs) that supplement the Safe Harbor Principles; 3) an overview on how organizations' safe harbor commitments will be enforced in the United States; 4) a memorandum on damages available to individuals; 5) the July 14, 2000 letter from the Federal Trade Commission; and 6) the July 14, 2000 letter from the U.S. Department of Transportation.

The Department is providing these documents under its authority to foster, promote, and develop international commerce. Both the Safe Harbor Principles and the FAQs ("the Principles") are intended to serve as authoritative guidance to U.S. companies and other organizations receiving personal data from the European Union and wishing to establish a predictable basis for the continuation of such transfers. The enforcement overview and other supporting documents are intended to explain how U.S. enforcement mechanisms, based either on law and regulation or self-regulation, will satisfy the requirements of the Enforcement Principle and ensure that an organization's commitment to adhere to the Principles will be effectively enforced. The safe harbor documents of course need to be read against the U.S. legal system and its well known features, such as class actions and contingency fees, which allow consumers even with novel claims relatively ready and inexpensive access to the courts and damages where justified.

Organizations can be assured of the benefits of the safe harbor by self-certifying that they adhere to the Principles. The Department of Commerce will arrange for a list to be maintained of all organizations that self-certify their adherence to the Principles. Both the list and the notifications submitted by organizations containing information with regard to their implementation of the Principles will be made publicly available as will any proper and final adverse determination made by a U.S. enforcement body and notified to the Department of Commerce (or its designee) that a safe harbor organization has persistently failed to comply with the Principles. Where in complying with the Principles, an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.

On the basis of these documents, our expectation is that the European Commission will determine that this safe harbor framework provides adequate protection for the purposes of Article 25.1 of the Data Protection Directive and data transfers from the European Union would continue to organizations that participate in the

safe harbor. As a result, adherence to the Principles on these terms will reduce the uncertainty about the impact of the "adequacy" standard on personal data transfers to such organizations from EU Member States.

On the basis of our dialogue, we 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. This will give U.S. organizations an opportunity to decide whether to enter the safe harbor and (if necessary) to update their information practices. We will encourage U.S. organizations to enter the safe harbor as soon as possible to enhance privacy protection and because participation in the safe harbor provides greater certainty that data flows will continue without interruption.

During the dialogue, you sought assurances that where the United States enacted privacy legislation providing greater privacy protection than the safe harbor, such protection should be applied to safe harbor data too, in cases where the law applied with respect to U.S. citizens only, but was silent on its applicability with respect to non-U.S. citizens. You noted that the EU Directive on Data Protection applies to all personal information processed in Europe, regardless of the individuals' citizenship or residency. I would like to confirm that we agree that privacy legislation should not apply differently on the basis of nationality, as provided for in paragraph 19(e) of the OECD guidelines and paragraph 70 of the explanatory memorandum and to assure you that if such legislation were proposed in Congress, we would work within the legislative process to avoid any such effects. We will also continue our efforts, in line with our general commitment to regulatory co-operation in the context of the Transatlantic Economic Partnership, to keep you informed of legislative and other developments in the United States in the field of privacy protection of which we are aware, with particular attention to any such developments that may create allowable exceptions to the Principles. Of course, you can raise any concerns about these issues under the review arrangements provided for.

Similarly, on a number of occasions I raised with you the concerns of U.S. industry about the possible effects of the safe harbor as regards jurisdiction and applicable law. I would like to confirm that it is the U.S. intention that participation in the safe harbor does not change the *status quo ante* for any organization with respect to jurisdiction, applicable law and liability in the European Union. Moreover, our discussions with respect to the safe harbor have not resolved nor prejudged the questions of jurisdiction or applicable law with respect to websites. All existing rules, principles, conventions and treaties relating to international conflicts of law continue to apply and are not prejudged in any way by the safe harbor arrangement.

Finally, the Department of Commerce will notify the Commission in advance of any proposed FAQs or revisions to existing ones.

Sincerely,

Robert S. LaRussa, Acting