

**DEPARTMENT OF COMMERCE****International Trade Administration****Issuance of Safe Harbor Principles and Transmission to European Commission**

**AGENCY:** International Trade Administration, Department of Commerce.

**ACTION:** Notice of publication.

**SUMMARY:** The U.S. Department of Commerce, under its authority to foster, promote, and develop international commerce, is formally issuing the Safe Harbor Privacy Principles and transmitting them to the European Commission. Upon receipt of the Principles, the Commission is expected to issue an "adequacy determination" for the safe harbor arrangement. In addition to being published in the **Federal Register**, these documents can be found on the International Trade Administration's website ([www.ita.doc.gov/ecom](http://www.ita.doc.gov/ecom)).

**Background**

The Principles, which include a set of Frequently Asked Questions (FAQs) that supplement the Safe Harbor Privacy Principles, are intended to serve as authoritative guidance to U.S. companies and other organizations receiving personal data from the European Union. Upon receipt of the Principles, the Commission is expected to issue an "adequacy determination" for the safe harbor arrangement. Organizations receiving personal data transfers from the EU and complying with the Principles will be considered to meet the "adequacy" requirements of the European Union's Directive on Data Protection.

**FURTHER INFORMATION:** Further information will be provided about the effective dates of operation of the safe harbor, after the European Commission has provided its "adequacy determination."

Dated: July 19, 2000.

**Rebecca J. Richards,**  
*International Trade Specialist, International Trade Administration/Trade Development.*  
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 cooperation 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 prejudiced 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

**Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000**

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place

only to non-EU countries that provide an "adequate" level of 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. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self-regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self-regulatory privacy policies provided that they conform 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. (See the annex for the list of U.S. statutory bodies recognized by the

EU.) In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for safe harbor benefits. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth in the Frequently Asked Question on Self-Certification.

Adherence to these Principles may be limited: (a) To the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection law where possible.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these Principles to personal information in manually processed filing systems. Organizations wishing to benefit from the safe harbor for receiving information in manually processed filing systems from the EU must apply the Principles to any such information transferred after they enter the safe harbor. An organization that wishes to extend safe harbor benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department of Commerce (or its designee) and conform to the requirements set forth in the Frequently Asked Question on Self-Certification.

Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

*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.<sup>1</sup>

*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<sup>1</sup> 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.

<sup>1</sup> It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

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

**Onward Transfer:** To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

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

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

**Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that

information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

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

#### **Annex**

##### *List of U.S. Statutory Bodies Recognized by the European Union*

The European Union recognizes the following U.S. government bodies as being empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals in case of non-compliance with the Principles implemented in accordance with the FAQs:

- The Federal Trade Commission on the basis of its authority under Section 5 of the Federal Trade Commission Act
- The Department of Transportation on the basis of its authority under Title 49 U.S.C. 41712.

#### **Frequently Asked Questions (FAQs)**

##### *FAQ 1—Sensitive Data*

**Q:** Must an organization always provide explicit (opt in) choice with respect to sensitive data?

**A:** No, such choice is not required where the processing is: (1) In the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide

medical care or diagnosis; (4) carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (5) necessary to carry out the organization's obligations in the field of employment law; or (6) related to data that are manifestly made public by the individual.

##### *FAQ 2—Journalistic Exceptions*

**Q:** Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, do the Safe Harbor Principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?

**A:** Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles.

##### *FAQ 3—Secondary Liability*

**Q:** Are Internet service providers (ISPs), telecommunications carriers, or other organizations liable under the Safe Harbor Principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate their terms?

**A:** No. As is the case with the Directive itself, the safe harbor does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

##### *FAQ 4—Investment Banking and Audits*

**Q:** The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. Under what circumstances is this permitted by the Notice, Choice, and Access Principles?

A: Investment bankers or auditors may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

*FAQ 5—The Role of the Data Protection Authorities*

Q: How will companies that commit to cooperate with European Union Data Protection Authorities (DPAs) make those commitments and how will they be implemented?

A: Under the safe harbor, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Safe Harbor Principles. More specifically as set out in the Enforcement Principle, they must provide (a) recourse for individuals to whom the data relate, (b) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a) and (c) of the Enforcement Principle if it adheres to the requirements of this FAQ for cooperating with the DPAs.

An organization may commit to cooperate with the DPAs by declaring in its safe harbor certification to the Department of Commerce (see FAQ 6 on self-certification) that the organization:

1. Elects to satisfy the requirement in points (a) and (c) of the Safe Harbor Enforcement Principle by committing to cooperate with the DPAs;

2. Will cooperate with the DPAs in the investigation and resolution of complaints brought under the safe harbor; and

3. Will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written

confirmation that such action has been taken.

The cooperation of the DPAs will be provided in the form of information and advice in the following way:

—The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will *inter alia* help ensure a harmonised and coherent approach.

—The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the safe harbor. This advice will be designed to ensure that the Safe Harbor Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.

—The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for safe harbor purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.

—Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.

—The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.

—The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the Federal Trade Commission or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been

seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce (or its designee) so that the list of safe harbor participants can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Safe Harbor Principles, will be actionable as a deceptive practice under section 5 of the FTC Act or other similar statute.

Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed \$500 and will be less for smaller companies.

The option of co-operating with the DPAs will be available to organizations joining the safe harbor during a three-year period. The DPAs will reconsider this arrangement before the end of that period if the number of U.S. organizations choosing this option proves to be excessive.

*FAQ 6—Self-Certification*

Q: How does an organization self-certify that it adheres to the Safe Harbor Principles?

A: Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:

1. Name of organization, mailing address, email address, telephone and fax numbers;

2. Description of the activities of the organization with respect to personal information received from the EU; and

3. Description of the organization's privacy policy for such personal information, including:

a. Where the privacy policy is available for viewing by the public,

b. Its effective date of implementation,

c. A contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor,

d. The specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and

violations of laws or regulations governing privacy (and that is listed in the annex to the Principles),

e. Name of any privacy programs in which the organization is a member,

f. Method of verification (e.g. in-house, third party) \*, and

g. The independent recourse mechanism that is available to investigate unresolved complaints.

Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ 9 and FAQ 5 as applicable and that it will comply with the advice given by such authorities.

The Department (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of safe harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. Such self-certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and safe harbor benefits will no longer be assured. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self-certify for the safe harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.

The undertaking to adhere to the Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the safe harbor. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the safe harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (1) continue to be bound by the Safe Harbor Principles by the operation of law

governing the takeover or merger or (2) elect to self-certify its adherence to the Safe Harbor Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Safe Harbor Principles. Where neither (1) nor (2) applies, any data that has been acquired under the safe harbor must be promptly deleted.

An organization does not need to subject all personal information to the Safe Harbor Principles, but it must subject to the Safe Harbor Principles all personal data received from the EU after it joins the safe harbor.

Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 U.S.C. 1001).

#### FAQ 7—Verification

**Q:** How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?

**A:** To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews.

Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. 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 and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

Organizations should retain their records on the implementation of their safe harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.

Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles, that it is being complied with and that individuals 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 and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

#### FAQ 8: Access

##### Access Principle

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 legitimate rights of persons other than the individual would be violated.

1. **Q:** Is the right of access absolute?

1. **A:** No. Under the Safe Harbor Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, 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. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the

\* See FAQ 7 on verification.

information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

2. Q: What is confidential commercial information and may organizations deny access in order to safeguard it?

2. A: Confidential commercial information (as that term is used in the Federal Rules of Civil Procedure on discovery) is information which an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. The particular computer program an organization uses, such as a modeling program, or the details of that program may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information. Organizations may deny or limit access to the extent that granting it would reveal its own confidential commercial information as defined above, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another where such information is subject to a contractual obligation of confidentiality in circumstances where such an obligation of confidentiality would normally be undertaken or imposed.

3. Q: In providing access, may an organization disclose to individuals personal information about them derived from its data bases or is access to the data base itself required?

3. A: Access can be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

4. Q: Does an organization have to restructure its data bases to be able to provide access?

4. A: Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

5. Q: These replies make clear that access may be denied in certain circumstances. In what other circumstances may an organization deny individuals access to their personal information?

5. A: Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition,

where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

a. Interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial;

b. Interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial;

c. Disclosure of personal information pertaining to other individual(s) where such references cannot be redacted;

d. Breaching a legal or other professional privilege or obligation;

e. Breaching the necessary confidentiality of future or ongoing negotiations, such as those involving the acquisition of publicly quoted companies;

f. Prejudicing employee security investigations or grievance proceedings;

g. Prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations; or

h. Prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management; or

i. Other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

An organization which claims an exception has the burden of demonstrating its applicability (as is normally the case). As noted above, the reasons for denying or limiting access and a contact point for further inquiries should be given to individuals.

6. Q: Can an organization charge a fee to cover the cost of providing access?

6. A: Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

Organizations that are in the business of selling publicly available information may thus charge the organization's customary fee in responding to requests for access. Individuals may alternatively seek access to their information from the organization that originally compiled the data.

Access may not be refused on cost grounds if the individual offers to pay the costs.

7. *Q:* Is an organization required to provide access to personal information derived from public records?

7. *A:* To clarify first, public records are those records kept by government agencies or entities at any level that are open to consultation by the public in general. It is not necessary to apply the Access Principle to such information as long as it is not combined with other personal information, apart from when small amounts of non-public record information are used for indexing or organizing public record information. However, any conditions for consultation established by the relevant jurisdiction are to be respected. Where public record information is combined with other non-public record information (other than as specifically noted above), however, an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

8. *Q:* Does the Access Principle have to be applied to publicly available personal information?

8. *A:* As with public record information (see Q7), it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information.

9. *Q:* How can an organization protect itself against repetitious or vexatious requests for access?

9. *A:* An organization does not have to respond to such requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

10. *Q:* How can an organization protect itself against fraudulent requests for access?

10. *A:* An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

11. *Q:* Is there a time within which responses must be provided to access requests?

11. *A:* Yes, organizations should respond without excessive delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, a data controller who provides information to

data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.

#### *FAQ 9—Human Resources*

1. *Q:* Is the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the safe harbor?

1. *A:* Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the safe harbor, the transfer enjoys the benefits of the safe harbor. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

2. *Q:* How do the Notice and Choice Principles apply to such information?

2. *A:* A U.S. organization that has received employee information from the EU under the safe harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms

when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

3. *Q:* How does the Access Principle apply?

3. *A:* The FAQs on access provide guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The safe harbor requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

4. *Q:* How will enforcement be handled for employee data under the Safe Harbor Principles?

4. *A:* In so far as information is used only in the context of the employment relationship, primary responsibility for the data vis-a-vis the employee remains with the company in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employee works. This also includes cases where the alleged mishandling of their personal information has taken place in the United States, is the responsibility of the U.S. organization that has received the information from the employer and not of the employer and thus involves an alleged breach of the Safe Harbor Principles, rather than of national laws implementing the Directive. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A U.S. organization participating in the safe harbor that uses EU human resources data transferred from the Europe Union in the context of the employment relationship and that wishes such transfers to be covered by the safe harbor must therefore commit to cooperate in investigations by and to comply with the advice of competent

EU authorities in such cases. The DPAs that have agreed to cooperate in this way will notify the European Commission and the Department of Commerce. If a U.S. organization participating in the safe harbor wishes to transfer human resources data from a Member State where the DPA has not so agreed, the provisions of FAQ 5 will apply.

#### FAQ 10—Article 17 Contracts

**Q:** When data is transferred from the EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the safe harbor?

**A:** Yes. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, *i.e.* the person or body who determines the purposes and means of processing, who retains full responsibility for the data vis-a-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-a-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles).

Because adequate protection is provided by safe harbor participants, contracts with safe harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the safe harbor or otherwise not providing adequate protection.

#### FAQ No 11: Dispute Resolution and Enforcement

**Q:** How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organization's persistent failure to comply with the Principles be handled?

**A:** The Enforcement Principle sets out the requirements for safe harbor enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of

which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organizations may satisfy the requirements through the following: (1) Compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirement set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

**Recourse Mechanisms.** Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record. As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in

conformity with the Safe Harbor Principles.<sup>1</sup> They should also co-operate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

**Remedies and Sanctions.** The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.<sup>2</sup> Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee).

**FTC Action.** The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason[s] to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result

<sup>1</sup> Dispute resolution bodies are not required to conform with the enforcement principle. They may also derogate from the Principles where they encounter conflicting obligations or explicit authorizations in the performance of their specific tasks.

<sup>2</sup> Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used or disclosed information in blatant contravention of the Principles.

in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of Commerce of any such actions it takes. The Department of Commerce encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Safe Harbor Principles.

**Persistent Failure to Comply.** If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization that has self-certified to the Department of Commerce (or its designee) 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 Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce (or its designee) of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. 1001).

The Department (or its designee) will indicate on the public list it maintains of organizations self-certifying adherence to the Safe Harbor Principles any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a self-regulatory body, or from a government body, but only after first providing thirty (30) days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the public list maintained by the Department of Commerce (or its designee) 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.

#### FAQ 12—Choice—Timing of Opt Out

**Q:** Does the Choice Principle permit an individual to exercise choice only at the beginning of a relationship or at any time?

**A:** Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" (or

choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

#### FAQ 13—Travel Information

**Q:** When can airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, be transferred to organizations located outside the EU?

**A:** Such information may be transferred in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (1) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (2) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the safe harbor provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Directive. Since the safe harbor includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be

included in transfers to safe harbor participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may *inter alia* impose special conditions for the handling of sensitive data.

#### FAQ 14—Pharmaceutical and Medical Products

**1. Q:** If personal data are collected in the EU and transferred to the United States for pharmaceutical research and/or other purposes, do Member State laws or the Safe Harbor Principles apply?

**1. A:** Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Safe Harbor Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

**2. Q:** Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the safe harbor, may the organization use the data for a new scientific research activity?

**2. A:** Yes, if appropriate notice and choice have been provided in the first instance. Such a notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

**3. Q:** What happens to an individual's data if a participant decides voluntarily or at the request of the sponsor to withdraw from the clinical trial?

**3. A:** Participants may decide or be asked to withdraw from a clinical trial at any time. Any data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was

made clear to the participant in the notice at the time he or she agreed to participate.

4. *Q:* Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Are similar transfers allowed to parties other than regulators, such as company locations and other researchers?

4. *A:* Yes, consistent with the Principles of Notice and Choice.

5. *Q:* To ensure objectivity in many clinical trials, participants, and often investigators, as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Will participants in such clinical trials (referred to as "blinded" studies) have access to the data on their treatment during the trial?

5. *A:* No, such access does not have to be provided to a participant if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring company.

6. *Q:* Does a pharmaceutical or medical device firm have to apply the Safe Harbor Principles with respect to notice, choice, onward transfer, and access in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices (e.g. a pacemaker)?

6. *A:* No, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers, to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

7. *Q:* Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies

sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he/she can identify the research subject under special circumstances (e.g. if follow-up medical attention is required). Does a transfer from the EU to the United States of data coded in this way constitute a transfer of personal data that is subject to the Safe Harbor Principles?

7. *A:* No. This would not constitute a transfer of personal data that would be subject to the Principles.

#### *FAQ 15—Public Record and Publicly Available Information*

*Q:* Is it necessary to apply the Notice, Choice and Onward Transfer Principles to public record information or publicly available information?

*A:* It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.

Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the safe harbor.

#### **Safe Harbor Enforcement Overview**

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

July 19, 2000.

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.<sup>3</sup>

<sup>3</sup> We do not discuss here all the various Federal statutes that address privacy in specific contexts or

#### *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.<sup>4</sup> 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.<sup>5</sup> For example, in 1998, the FTC filed a complaint against

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).

<sup>4</sup> 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).

<sup>5</sup> "Deceptive practice" is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion.

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.<sup>6</sup> 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.<sup>7</sup>

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.

#### Financial Institutions<sup>8</sup>

The first exception applies to "banks, savings and loan institutions described in section 18(f)(3) [15 U.S.C. 57a(f)(3)]" and "Federal credit unions described in section 18(f)(4) [15 U.S.C. 57a(f)(4)]."<sup>9</sup> These financial institutions are instead subject to regulations issued by the Federal Reserve Board, the Office of Thrift Supervision,<sup>10</sup> and the National Credit Union Administration Board, respectively. See 15 U.S.C. 57a(f). These regulatory agencies are directed to prescribe the regulations necessary to prevent unfair and deceptive practices by these financial institutions<sup>11</sup> and to establish a separate division to handle consumer complaints. 15 U.S.C. 57a(f)(1). Finally, authority for enforcement derives from section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), for banks and savings and loans, and sections 120 and 206 of the Federal Credit Union Act, for Federal credit unions. 15 U.S.C. 57a(f)(2)-(4).

Although the insurance industry is not specifically included in the list of exceptions in Section 5, the McCarran-Ferguson Act (15 U.S.C. 1011 *et seq.*)

<sup>8</sup> 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.

<sup>9</sup> 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.

<sup>10</sup> 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.

<sup>11</sup> 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).

generally leaves the regulation of the business of insurance to the individual states.<sup>12</sup> Furthermore, pursuant to section 2(b) of the McCarran-Ferguson Act, no federal law will invalidate, impair, or supersede state regulation "unless such Act specifically relates to the business of insurance." 15 U.S.C. 1012(b). However, the provisions of the FTC Act apply to the insurance industry "to the extent that such business is not regulated by State law." *Id.* It should also be noted that McCarran-Ferguson defers to the states only with respect to "the business of insurance." Therefore, the FTC retains residual authority over unfair or deceptive practices by insurance companies when they are not engaged in the business of insurance. This could include, for example, when insurers sell personal information about their policy holders to direct marketers of non-insurance products.<sup>13</sup>

#### Common Carriers

The second section 5 exception extends to those common carriers that are "subject to the Acts to regulate commerce." 15 U.S.C. 45(a)(2). In this case, the "Acts to regulate commerce" refer to subtitle IV of Title 49 of the United States Code and to the Communications Act of 1934 (47 U.S.C. 151 *et seq.*) (the Communications Act). See 15 U.S.C. 44.

49 U.S.C. subtitle IV (Interstate Transportation) covers rail carriers, motor carriers, water carriers, brokers, freight forwarders, and pipeline carriers. 49 U.S.C. 10101 *et seq.* These various common carriers are subject to regulation by the Surface Transportation Board, an independent agency within the Department of Transportation. 49 U.S.C. 10501, 13501, and 15301. In each instance, the carrier is prohibited from disclosing information about the nature, destination, and other aspects of its cargo that might be used to the shipper's detriment. See 49 U.S.C. 11904, 14908,

<sup>12</sup> "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).

<sup>13</sup> 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.

<sup>6</sup> See [www.ftc.gov/opa/1998/9808/geocitie.htm](http://www.ftc.gov/opa/1998/9808/geocitie.htm).

<sup>7</sup> See staff letter to Center for Media Education, [www.ftc.gov/os/1997/9707/cenmed.htm](http://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.*

and 16103. We note that these provisions refer to information regarding the shipper's cargo and thus do not appear to extend to personal information about the shipper that is unrelated to the shipment in question.

As for the Communications Act, it provides for the regulation of "interstate and foreign commerce in communication by wire and radio" by the Federal Communications Commission (FCC). See 47 U.S.C. 151 and 152. In addition to common carrier telecommunications companies, the Communications Act also applies to companies such as television and radio broadcasters and cable service providers which are not common carriers. As such, these latter companies do not qualify for the exception under section 5 of the FTC Act. Thus, the FTC has jurisdiction to investigate these companies for unfair and deceptive practices, while the FCC has concurrent jurisdiction to enforce its independent authority in this area as described below.

Under the Communications Act, "every telecommunications carrier," including local exchange carriers, has a duty to protect the privacy of customer proprietary information.<sup>14</sup> 47 U.S.C. 222(a). In addition to this general privacy-protection authority, the Communications Act was amended by the Cable Communications Policy Act of 1984 (the Cable Act), 47 U.S.C. 521 *et seq.*, to mandate specifically that cable operators protect the privacy of "personally identifiable information" on cable subscribers. 47 U.S.C. 551.<sup>15</sup> The Cable Act restricts the collection of personal information by cable operators and requires the cable operator to notify the subscriber of the nature of the information collected and how that information will be used. The Cable Act gives subscribers the right of access to the information about them and requires cable operators to destroy that information when it's no longer needed.

The Communications Act empowers the FCC to enforce these two privacy provisions, either at its own initiation or in response to an outside complaint.<sup>16</sup>

<sup>14</sup> 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.*

<sup>15</sup> The legislation does not expressly define "personally identifiable information."

<sup>16</sup> 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

47 U.S.C. 205, 403; *id.* 208. If the FCC determines that a telecommunications carrier (including a cable operator) has violated the privacy provisions of section 222 or section 551, there are three basic actions it may take. First, after a hearing and determination of violation, the Commission may order the carrier to pay monetary damages.<sup>17</sup> 47 U.S.C. 209. Alternatively, the FCC may order the carrier to cease and desist from the offending practice or omission. 47 U.S.C. 205(a). Finally, the Commission may also order an offending carrier to "conform to and observe [any] regulation or practice" that the FCC may prescribe. *Id.*

Private persons who believe a telecommunications carrier or cable operator has violated the relevant provisions of the Communications Act or the Cable Act may either file a complaint with the FCC or take their claims to a federal district court. 47 U.S.C. 207. A complainant who prevails in a federal court action against a telecommunications carrier for failure to protect customer proprietary information under the broader section 222 of the Communications Act may be awarded actual damages and attorneys' fees. 47 U.S.C. 206. A complainant who files suit claiming a privacy violation under the cable-specific section 551 of the Cable Act may, in addition to actual damages and attorneys' fees, also be awarded punitive damages and reasonable litigation costs. 47 U.S.C. 551(f).

The FCC has adopted detailed rules to implement section 222. See 47 CFR 64.2001–2009. The rules set out specific safeguards to protect against unauthorized access to customer proprietary network information. The regulations require telecommunications carriers to:

- Develop and implement software systems that "flag" a customer's notice/approval status when the customer's service record first comes on-screen;
- Maintain an electronic "audit trail" to track access to a customer's account, including when a customer's record is opened, by whom, and for what purpose;
- Train their personnel on the authorized use of customer proprietary network information, with appropriate disciplinary processes in place;
- Establish a supervisory review process to ensure compliance when conducting outbound marketing; and

nonexclusive remedy, offered "in addition to any other lawful remedy available to a cable subscriber.")

<sup>17</sup> However, the absence of direct damage to a complainant is not grounds to dismiss a complaint. 47 U.S.C. 208(a).

- Certify to the FCC, on an annual basis, how they are complying with these regulations.

#### Air Carriers

U.S. and foreign air carriers that are subject to Federal Aviation Act of 1958 are also exempt from section 5 of the FTC Act. See 15 U.S.C. 45(a)(2). This includes anyone who provides interstate or foreign transportation of goods or passengers, or who transports mail, by aircraft. See 49 U.S.C. 40102. Air carriers are subject to the authority of the Department of Transportation. In this regard, the Secretary of Transportation is authorized to take action "preventing unfair, deceptive, predatory, or anticompetitive practices in air transportation." 49 U.S.C. 40101(a)(9). The Secretary of Transportation can investigate whether a U.S. or foreign air carrier, or a ticket agent, has engaged in an unfair or deceptive practice if it is in the public interest. 49 U.S.C. 41712. After a hearing, the Secretary of Transportation can issue an order to stop the illegal practice. *Id.* To our knowledge, the Secretary of Transportation has not exercised this authority to address the issue of protecting the privacy of personal information about airline customers.<sup>18</sup>

There are two provisions protecting the privacy of personal information that apply to air carriers in specific contexts. First, the Federal Aviation Act protects the privacy of pilot applicants. See 49 U.S.C. 44936(f). While allowing air carriers to obtain an applicant's employment records, the Act gives the applicant the right to notice that the records have been requested, to give consent to the request, to correct inaccuracies, and to have the records divulged only to those involved in the hiring decision. Second, DOT regulations require passenger manifest information collected for government use in the event of an aviation disaster to "be kept confidential and released only to the U.S. Department of State, the National Transportation Board (upon the NTSB's request), and the U.S. Department of Transportation." 14 CFR part 243, 243.9(c) (as added by 63 FR 8258).

<sup>18</sup> 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.

## Packers and Stockyards

With regard to the Packers and Stockyards Act of 1921 (7 U.S.C. 181 *et seq.*), the Act makes it unlawful for "any packer with respect to livestock, meats, meat food products, or livestock products in unmanufactured form, or for any live poultry dealer with respect to live poultry, to engage in or use any unfair, unjustly discriminatory, or deceptive practice or device." 7 U.S.C. 192(a); *see also* 7 U.S.C. 213(a) (prohibiting "any unfair, unjustly discriminatory, or deceptive practice or device" in connection with livestock). The Secretary of Agriculture has the primary responsibility to enforce these provisions, while the FTC retains jurisdiction over retail transactions and those involving the poultry industry. 7 U.S.C. 227(b)(2).

It is not clear whether the Secretary of Agriculture will interpret the failure by a packer or stockyard operator to protect personal privacy in accordance with stated policy to be a "deceptive" practice under the Packers and Stockyards Act. However, the Section 5 exception applies to persons, partnerships, or corporations only "insofar as they are subject to the Packers and Stockyards Act." Therefore, if personal privacy is not an issue within the purview of the Packers and Stockyards Act, then the exception in Section 5 may very well not apply and packers and stockyard operators would be subject to the authority of the FTC in that regard.

*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.

**Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law**

July 19, 2000.

This responds to the request by the European Commission for clarification of U.S. law with respect to (a) claims for damages for breaches of privacy, (b) "explicit authorizations" in U.S. law for the use of personal information in a manner inconsistent with the safe harbor principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbor principles.

*A. Damages for Breaches of Privacy*

Failure to comply with the safe harbor principles could give rise to a number of private claims depending on the relevant circumstances. In particular, safe harbor organizations could be held liable for misrepresentation for failing to adhere to their stated privacy policies. Private causes of action for damages for breaches of privacy are also available under common law. Many federal and state statutes on privacy also provide for the recovery of damages by private individuals for violations.

**The Right To Recover Damages for Invasion of Personal Privacy is Well Established Under U.S. Common Law**

Use of personal information in a manner inconsistent with the safe harbor principles can give rise to legal

liability under a number of different legal theories. For example, both the transferring data controller and the individuals affected could sue the safe harbor organization which fails to honor its safe harbor commitments for misrepresentation. According to the Restatement of the Law, Second, Torts<sup>19</sup>:

One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it, is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation.

Restatement, § 525. A misrepresentation is "fraudulent" if it is made with the knowledge or in the belief that it is false. *Id.*, § 526. As a general rule, the maker of a fraudulent misrepresentation is potentially liable to everyone who he intends or expects to rely on that misrepresentation for any pecuniary loss they might suffer as a result. *Id.*, § 531. Furthermore, a party who makes a fraudulent misrepresentation to another could be liable to a third-party if the tortfeasor intends or expects that his misrepresentation would be repeated to and acted upon by the third-party. *Id.*, § 533.

In the context of the safe harbor, the relevant representation is the organization's public declaration that it will adhere to the safe harbor principles. Having made such a commitment, a conscious failure to abide by the principles could be grounds for a cause of action for misrepresentation by those who relied on the misrepresentation. Because the commitment to adhere to the principles is made to the public at large, the individuals who are the subjects of that information as well as the data controller in Europe that transfers personal information to the U.S. organization could all have causes of action against the U.S. organization for misrepresentation.<sup>20</sup> Moreover, the U.S. organization remains liable to them for the "continuing misrepresentation" for as long as they rely on the misrepresentation to their detriment. Restatement, § 535.

Those who rely on a fraudulent misrepresentation have a right to recover damages. According to the Restatement:

<sup>19</sup> Second Restatement of the Law—Torts; American Law Institute (1997).

<sup>20</sup> This might be the case, for example, where the individuals relied on the U.S. organization's safe harbor commitments in giving their consent to the data controller to transfer their personal information to the United States.

The recipient of a fraudulent misrepresentation is entitled to recover as damages in an action of deceit against the maker the pecuniary loss to him of which the misrepresentation is a legal cause.

Restatement, § 549. Allowable damages include actual out-of-pocket loss as well as the lost "benefit of the bargain" in a commercial transaction. *Id.*; see, e.g., *Boling v. Tennessee State Bank*, 890 S.W.2d 32 (1994) (bank liable to borrowers for \$14,825 in compensatory damages for disclosing borrowers' personal information and business plans to bank president who had a conflicting interest).

Whereas fraudulent misrepresentation requires either actual knowledge or at least the belief that the representation is false, liability can also attach for negligent misrepresentation. According to the Restatement, whoever makes a false statement in the course of his business, profession, or employment, or in any pecuniary transaction can be held liable "if he fails to exercise reasonable care or competence in obtaining or communicating the information." Restatement, § 552(1). In contrast with fraudulent misrepresentations, damages for negligent misrepresentation are limited to out-of-pocket loss. *Id.*, § 552B(1).

In a recent case, for example, the Superior Court of Connecticut held that a failure by an electric utility to disclose its reporting of customer payment information to national credit agencies sustained a cause of action for misrepresentation. See *Brouillard v. United Illuminating Co.*, 1999 Conn. Super. LEXIS 1754. In that case, the plaintiff was denied credit because the defendant reported payments not received within thirty days of the billing date as "late". The plaintiff alleged that he had not been informed of this policy when he opened a residential electric service account with the defendant. The court specifically held that "a claim for negligent misrepresentation may be based on the defendant's failure to speak when he has a duty to do so." This case also shows that "scienter" or fraudulent intent is not a necessary element in a cause of action for negligent misrepresentation. Thus, a U.S. organization which negligently fails to fully disclose how it will use personal information received under the safe harbor could be held liable for misrepresentation.

Insofar as a violation of the safe harbor principles entailed a misuse of personal information, it could also support a claim by the data subject for the common law tort of invasion of privacy. American law has long recognized causes of action relating to

invasions of privacy. In a 1905 case,<sup>21</sup> the Georgia Supreme Court found a right to privacy rooted in natural law and common law precepts in holding for a private citizen whose photograph had been used by a life insurance company, without his consent or knowledge, to illustrate a commercial advertisement. Articulating now-familiar themes in American privacy jurisprudence, the court found that the usage of the photograph was "malicious," "false," and tended to "bring plaintiff into ridicule before the world."<sup>22</sup> The foundations of the Pavesich decision have prevailed with minor variations to become the bedrock of American law on this topic. State courts have consistently upheld causes of action in the realm of invasion of privacy, and at least 48 states now judicially recognize some such cause of action.<sup>23</sup> Moreover, at least twelve states have constitutional provisions safeguarding their citizens' right to be free from intrusive actions,<sup>24</sup> which in some cases could extend to protect against intrusion by non-governmental entities. See, e.g., *Hill v. NCAA*, 865 P.2d 633 (Ca. 1994); see also S. Ginder, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 S.D. L. Rev. 1153 (1997) ("Some state constitutions include privacy protections which surpass privacy protections in the U.S. Constitution. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have broader privacy protection.")

The Second Restatement of Torts provides an authoritative overview of the law in this area. Reflecting common judicial practice, the Restatement explains that the "right to privacy" encompasses four distinct causes of action in tort under that umbrella. See Restatement, § 652A. First, a cause of action for "intrusion upon seclusion" may lie against a defendant who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.<sup>25</sup> Second, an

"appropriation" case may exist when one takes the name or likeness of another for his own use or benefit.<sup>26</sup> Third, the "publication of private facts" is actionable when the matter publicized is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public.<sup>27</sup> Lastly, an action for "false light publicity" is appropriate when the defendant knowingly or recklessly places another before the public in a false light that would be highly offensive to a reasonable person.<sup>28</sup>

In the context of the safe harbor framework, "intrusion upon seclusion" could encompass the unauthorized collection of personal information whereas the unauthorized use of personal information for commercial purposes could give rise to a claim of appropriation. Similarly, the disclosure of personal information that is inaccurate would give rise to a tort of "false light publicity" if the information meets the standard of being highly offensive to a reasonable person. Finally, the invasion of privacy that results from the publication or disclosure of sensitive personal information could give rise to a cause of action for "publication of private facts." (See examples of illustrative cases below.)

On the issue of damages, invasions of privacy give the injured party the right to recover damages for:

- (a) The harm to his interest in privacy resulting from the invasion;
- (b) His mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and
- (c) Special damage of which the invasion is a legal cause.

Restatement, § 652H. Given the general applicability of tort law and the multiplicity of causes of action covering different aspects of privacy interests, monetary damages are likely to be available to those who suffer invasion of their privacy interests as a result of a failure to adhere to the safe harbor principles.

Indeed, state courts are replete with cases alleging invasion of privacy in analogous situations. *Ex Parte AmSouth Bancorporation et al.*, 717 So. 2d 357, for example, involved a class action that alleged the defendant "exploited the trust depositors placed in the Bank, by sharing confidential information regarding Bank depositors and their accounts" to enable a bank affiliate to sell mutual funds and other

<sup>21</sup> *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905)

<sup>22</sup> *Id.*, at 69.

<sup>23</sup> An electronic search of the Westlaw database found 2703 reported cases of civil actions in state courts that pertained to "privacy" since 1995. We have previously provided the results of this search to the Commission.

<sup>24</sup> See, e.g., Alaska Constitution, Art. 1 Sec. 22; Arizona, Art. 2, Sec. 8; California, Art. 1, Sec. 1; Florida, Art. 1, Sec. 23; Hawaii, Art. 1, Sec. 5; Illinois, Art. 1, Sec. 6; Louisiana, Art. 1, Sec. 5; Montana, Art. 2, Sec. 10; New York, Art. 1, Sec. 12; Pennsylvania, Art. 1, Sec. 1; South Carolina, Art. 1, Sec. 10; and Washington, Art. 1, Sec. 7.

<sup>25</sup> *Id.*, at Chapter 28, Section 652B.

<sup>26</sup> *Id.*, at Chapter 28, Section 652C.

<sup>27</sup> *Id.*, at Chapter 28, Section 652D.

<sup>28</sup> *Id.*, at Chapter 28, Section 652E.

investments. Damages are often awarded in such cases. In *Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580 (D.C.App. 1985), an appellate court reversed a lower court judgement to hold that the use of photographs of the plaintiff "before" and "after" plastic surgery in a presentation in a department store constituted an invasion of privacy through the publication of private facts. In *Candebat v. Flanagan*, 487 So.2d 207 (Miss. 1986), the defendant insurance company used an accident in which plaintiff's wife was seriously injured in an advertising campaign. Plaintiff sued for invasion of privacy. The court held that plaintiff could recover damages for emotional distress and appropriation of identity. Actions for misappropriation can be maintained even if the plaintiff is not personally famous. See, e.g., *Staruski v. Continental Telephone Co.*, 154 Vt. 568 (1990) (defendant derived commercial benefit in using employee's name and photograph in newspaper advertisement). In *Pulla v. Amoco Oil Co.*, 882 F.Supp. 836 (S.D Iowa 1995), an employer intruded on plaintiff employee's seclusion by having another employee investigate his credit card records in order to verify his sick day absences. The court upheld a jury award of \$2 in actual damages and \$500,000 in punitive damages. Another employer was held liable for publishing a story in the company newspaper about an employee who was terminated for allegedly falsifying his employment records. See *Zinda v. Louisiana-Pacific Corp.*, 140 Wis.2d 277 (Wis.App. 1987). The story invaded the plaintiff's privacy by publication of a private matter because the newspaper circulated in the community. Finally, a college which tested students for HIV after telling them the blood test was for rubella only was held liable for intrusion upon seclusion. See *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060 (Colo.App. 1998). (For other reported cases, see Restatement, § 652H, Appendix.)

The United States is often criticized for being overly litigious, but this also means that individuals actually can, and do, pursue legal recourse when they believe they have been wronged. Many aspects of the U.S. judicial system make it easy for plaintiffs to bring suit, either individually or as a class. The legal bar, comparatively larger than in most other countries, makes professional representation readily available. Plaintiffs' counsel representing individuals in private claims will typically work on a contingency fee basis, allowing even poor or indigent plaintiffs to seek redress. This brings up an important factor—in the United States, each side typically bears its own

lawyers' fees and other costs. This contrasts with the prevailing rule in Europe wherein the losing party has to reimburse the other side for costs. Without debating the relative merits of the two systems, the U.S. rule is less likely to deter legitimate claims by individuals who would not be able to pay the costs on both sides if they should lose.

Individuals can sue for redress even if their claims are relatively small. Most, if not all U.S. jurisdictions, have small claims courts which provide simplified and less costly procedures for disputes below the statutory limits.<sup>29</sup> The potential for punitive damages also offers a financial reward for individuals who might have suffered little direct injury to bring suit against reprehensible misconduct. Finally, individuals who have been injured in the same way can marshal their resources as well as their claims to bring a class-action lawsuit.

A good example of the ability of individuals to bring suit to obtain redress is the pending litigation against Amazon.com for invasion of privacy. Amazon.com, the large online retailer, is the target of a class action, in which the plaintiffs allege that they were not told about, and did not consent to, the collection of personal information about them when they used a software program owned by Amazon called "Alexa." In that case, plaintiffs have alleged violations of the Computer Fraud and Abuse Act in unlawful access to their stored communications and of the Electronic Communications Privacy Act for unlawful interception of their electronic and wire communications. They also claim an invasion of privacy under common law. This stems from a complaint filed by an Internet security expert in December. The suit seeks damages of \$1,000 per class member, plus attorneys' fees and profits earned as a result of violations of laws. Given that the number of class members could be in the millions, damages could total billions of dollars. The FTC is also investigating the charges.

Federal and State Privacy Legislation Often Provides Private Causes of Action for Money Damages

In addition to giving rise to civil liability under tort law, noncompliance with the safe harbor principles could also violate one or another of the hundreds of federal and state privacy laws. Many of these laws, which address both government and private-sector handling of personal information, allow individuals to sue for damages when violations occur. For example:

*Electronic Communications Privacy Act of 1986.* The ECPA prohibits the unauthorized interception of cellular telephone calls and computer-to-computer transmissions. Violations can result in civil liability of not less than \$100 for each day of violation. The protection of the ECPA also extends to unauthorized access or disclosure of stored electronic communications. Violators are liable for damages suffered or forfeiture of profits generated by a violation.

*Telecommunications Act of 1996.* Under section 702, customer proprietary network information (CPNI) may not be used for any purpose other than to provide telecommunications services. Service subscribers can either submit a complaint to the Federal Communications Commission or file suit in federal district court to recover damages and attorneys' fees.

*Consumer Credit Reporting Reform Act of 1996.* The 1996 Act amended the Fair Credit Reporting Act of 1970 (FCRA) to require improved notice and right of access for credit reporting subjects. The Reform Act also imposed new restrictions on resellers of consumer credit reports. Consumers can recover damages and attorneys' fees for violations.

State laws also protect personal privacy in a broad range of situations. Areas where the states have taken action include bank records, cable television subscriptions, credit reports, employment records, government records, genetic information and medical records, insurance records, school records, electronic communications, and video rentals.<sup>30</sup>

#### B. Explicit Legal Authorizations

The safe harbor principles contain an exception where statute, regulation or case law create "conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further by such authorization." Clearly, where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law. As for explicit authorizations, while the safe harbor principles are intended to bridge the differences between the U.S. and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected

<sup>29</sup> We had previously provided the Commission with information on small-claims actions.

<sup>30</sup> A recent electronic search of the Westlaw database yielded 994 reported states cases that related to damages and invasion of privacy.

lawmakers. The limited exception from strict adherence to the safe harbor principles seeks to strike a balance to accommodate the legitimate interests on each side.

The exception is limited to cases where there is an *explicit* authorization. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorize the particular conduct by safe harbor organizations.<sup>31</sup> In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorization *conflicts* with adherence to the safe harbor principles. Even then, the exception “is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization.” By way of illustration, where the law simply authorizes a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorizes the company to provide personal information to government agencies without the individual’s consent, this would constitute an “explicit authorization” to act in a manner that conflicts with the safe harbor principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorization to disclose the information without notice and consent). For example, a statute which authorizes doctors to provide their patients’ medical records to health officials without the patients’ prior consent might permit an exception from the notice and choice principles. This authorization would not permit a doctor to provide the same medical records to health maintenance organizations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorized by the law and therefore beyond the scope of the exception.<sup>32</sup> The legal authority in question can be a “stand alone” authorization to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which

proscribes the collection, use, or disclosure of personal information.

#### Telecommunications Act of 1996

In most cases, the authorized uses are either consistent with the requirements of the Directive and the principles, or would be permitted by one of the other allowed exceptions. For example, section 702 of the Telecommunications Act (codified at 47 U.S.C. § 222) imposes a duty on telecommunications carriers to maintain the confidentiality of personal information that they obtain in the course of providing their services to their customers. This provision specifically allows telecommunications carriers to:

- Use customer information to provide telecommunications service, including the publication of subscriber directories;
- Provide customer information to others at the written request of the customer; and
- Provide customer information in aggregate form.

See 47 U.S.C. § 222(c)(1)–(3). The Act also allows telecommunications carriers an exception to use customer information:

- To initiate, render, bill, and collect for their services;
- To protect against fraudulent, abusive or illegal conduct; and
- To provide telemarketing, referral or administrative services during a call initiated by the customer.<sup>33</sup>

*Id.*, § 222(d)(1)–(3). Finally, telecommunications carriers are required to provide subscriber list information, which can only include the names, addresses, telephone numbers and line of business for commercial customers to publishers of telephone directories. *Id.*, § 222(e).

The exception for “explicit authorizations” might come into play when telecommunications carriers use CPNI to prevent fraud or other unlawful conduct. Even here, such actions could qualify as being in the “public interest” and allowed by the principles for that reason.

#### Department of Health and Human Services Proposed Rules

The Department of Health and Human Services (HHS) has proposed rules regarding standards for the privacy of

individually identifiable health information. See 64 FR 59,918 (Nov. 3, 1999) (to be codified at 45 CFR parts 160–164). The rules would implement the privacy requirements of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191. The proposed rules generally would prohibit covered entities (*i.e.* health plans, health care clearinghouses, and health providers that transmit health information in electronic format) from using or disclosing protected health information without individual authorization. See proposed 45 CFR § 164.506. The proposed rules would require disclosure of protected health information for only two purposes: (1) To permit individuals to inspect and copy health information about themselves, *see id.* at § 164.514; and (2) to enforce the rules, *see id.* at § 164.522.

The proposed rules would permit use or disclosure of protected health information, without specific authorization by the individual, in limited circumstances. These include for example oversight of the health care system, law enforcement, and emergencies. See *id.* at § 164.510. The proposed rules set out in detail the limits on these uses and disclosures. Moreover, permitted uses and disclosures of protected health information would be limited to the minimum amount of information necessary. See *id.* at § 164.506.

The permissive uses explicitly authorized by the proposed regulations are generally consistent with the safe harbor principles or are otherwise allowed by another exception. For example, law enforcement and judicial administration are permitted, as is medical research. Other uses, such as oversight of the health care system, public health function, and government health data systems, serve the public interest. Disclosures to process health care payments and premiums are necessary to the provision of health care. Uses in emergencies, to consult with next-of-kin regarding treatment where the patient’s consent “cannot practicably or reasonably be obtained,” or to determine the identity or cause of death of the deceased protect the vital interests of the data subject and others. Uses for the management of active duty military and other special classes of individuals aid the proper execution of the military mission or similar exigent situations; and in any event, such uses will have little if any application to consumers in general.

This leaves only the use of personal information by health care facilities to produce patient directories. While such use might not rise to the level of a

<sup>31</sup> As a point of clarification, the relevant legal authority will *not* have to specifically reference the safe harbor principles.

<sup>32</sup> Similarly, the doctor in this example could not rely on the statutory authority to override the individual’s exercise of the opt-out from direct marketing provided by FAQ 12. The scope of any exception for “explicit authorizations” is necessarily limited to the scope of the authorization under relevant law.

<sup>33</sup> The scope of this exception is very limited. By its terms, the telecommunications carrier can use CPNI only *during* a call initiated by the customer. Furthermore, we have been advised by the FCC that the telecommunications carrier may not use CPNI to market services beyond the scope of the customer’s inquiry. Finally, since the customer must approve the use of CPNI for this purpose, this provision is not really an “exception” at all.

“vital” interest, the directories do benefit patients and their friends and relations. Also, the scope of this authorized use is inherently limited. Therefore, reliance on the exception in the principles for uses “explicitly authorized” by law for this purpose presents minimal risk to the privacy of patients.

#### Fair Credit Reporting Act

The European Commission has expressed the concern that the “explicit authorizations” exception would “effectively create an adequacy finding” for the Fair Credit Reporting Act (FCRA). This would not be the case. In the absence of a specific adequacy finding for the FCRA, those U.S. organizations that would otherwise rely on such a finding, would have to promise to adhere to the safe harbor principles in all respects. This means that where FCRA requirements exceed the level of protection embodied in the principles, the U.S. organizations need only to obey the FCRA. Conversely, where the FCRA might fall short, then those organizations would need to bring their information practices into conformity with the principles. The exception would not alter this basic assessment. By its terms, the exception applies only where the relevant law explicitly authorizes conduct that would be inconsistent with the safe harbor principles. The exception would not extend to where FCRA requirements merely do not meet the safe harbor principles.<sup>34</sup>

In other words, we do not intend the exception to mean that whatever is not required is therefore “explicitly authorized.” Furthermore, the exception applies only when what is explicitly authorized by U.S. law *conflicts* with the requirements of the safe harbor principles. The relevant law must meet both of these elements before non-adherence with the principles would be permitted.

Section 604 of the FCRA, for example, explicitly authorizes consumer reporting agencies to issue consumer reports in various enumerated situations. See FCRA, § 604. If in so doing, section 604 authorizes credit reporting agencies to act in conflict with the safe harbor principles, then the credit reporting agencies would need to rely on the exception (unless, of course, some other exception applied). Credit reporting agencies must obey court

orders and grand jury subpoenas, and use of credit reports by government licensing, social and child support enforcement agencies serves a public purpose. *Id.*, § 604(a)(1), (3)(D), and (4). Consequently, the credit reporting agency would not need to rely on the “explicit authorization” exception for these purposes. Where it acts in accordance with written instructions by the consumer, the consumer reporting agency would be fully in compliance with the safe harbor principles. *Id.*, § 604(a)(2). Likewise, consumer reports can be procured for employment purposes only with the consumer’s written authorization (*id.*, §§ 604(a)(3)(B) and (b)(2)(A)(ii)) and for credit or insurance transactions that are not initiated by the consumer only if the consumer had not opted out from such solicitations (*id.*, § 604(c)(1)(B)). Also, FCRA prohibits credit reporting agencies from providing medical information for employment purposes without the consent of the consumer. *Id.*, § 604(g). Such uses comport with the notice and choice principles. Other purposes authorized by section 604 entail transactions involving the consumer and would be permitted by the principles for that reason. See *id.*, § 604(a)(3)(A) and (F).

The remaining use “authorized” by section 604 relates to secondary credit markets. *Id.*, § 604(a)(3)(E). There is no conflict between use of consumer reports for this purpose and the safe harbor principles *per se*. It is true that the FCRA does not require credit reporting agencies, for example, to give notice and consent to consumers when they issue reports for this purpose. However, we reiterate the point that the absence of a requirement does not connote an “explicit authorization” to act in a manner other than as required. Similarly, section 608 allows credit reporting agencies to provide some personal information to government agencies. This “authorization” would not justify a credit reporting agency ignoring its commitments to adhere to the safe harbor principles. This contrasts with our other examples where exceptions from affirmative notice and choice requirements operate to explicitly authorize uses of personal information without notice and choice.

#### Conclusion

A distinct pattern emerges even from our limited review of these statutes:

- The “explicit authorization” in the law generally permits the use or disclosure of personal information without the individual’s prior consent; thus, the exception would be limited to the notice and choice principles.

- In most cases, the exceptions authorized by the law are narrowly drawn to apply in specific situations for specific purposes. In all cases, the law otherwise prohibits the unauthorized use or disclosure of personal information that does not fall within these limits.

- In most cases, reflecting their legislative character, the authorized use or disclosure serves a public interest.

- In almost all cases, the authorized uses are either fully consistent with the safe harbor principles or fall into one of the other allowed exceptions.

In conclusion, the exception for “explicit authorizations” in the law will, by its nature, likely be rather limited in scope.

#### C. Mergers and Takeovers

The Article 29 Working Party expressed concern over situations where an organization within the safe harbor is taken over by, or merged with, a firm which has not made a commitment to follow the safe harbor principles. The Working Party, however, appears to have assumed that the surviving firm would not be bound to apply the safe harbor principles to personal information held by the firm that is taken over, but that is not necessarily the case under U.S. law. The general rule in the United States as to mergers and takeovers is that a company which acquires the outstanding stock of another corporation generally assumes the obligations and liabilities of the acquired firm. See 15 *Fletcher Cyclopedia of the Law of Private Corporations* § 7117 (1990); see also Model Bus. Corp. Act § 11.06(3) (1979) (“the surviving corporation has all liabilities of each corporation party to the merger”). In other words, the surviving firm in a merger or takeover of a safe harbor organization by this method would be bound by the latter’s safe harbor commitments.

Moreover, even if the merger or takeover were effectuated through the acquisition of assets, the liabilities of the acquired enterprise could nevertheless bind the acquiring firm in certain circumstances. 15 *Fletcher*, § 7122. Even where liabilities did not survive the merger, however, it is worth noting that they also would not survive a merger where the data were transferred from Europe pursuant to a contract—the only viable alternative to the safe harbor for data transfers to the United States. In addition, the safe harbor documents as revised now require any safe harbor organization to notify the Department of Commerce of any takeover and permit data to continue to be transferred to the

<sup>34</sup> Our discussion here should not be taken as an admission that the FCRA does not provide “adequate” protection. Any assessment of the FCRA must consider the protection provided by the statute in its entirety and not focus only on the exceptions as we do here.

successor organization only if the successor organization joins the safe harbor. See FAQ 6. Indeed, the United States has now revised the safe harbor framework to require U.S. organizations in this situation to delete information they have received under the safe harbor framework if their safe harbor commitments will not continue or other suitable safeguards are not put in place.

July 14, 2000.

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

Dear Mr. Mogg:

I understand a number of questions have arisen with regard to my letter to you of March 29, 2000. To clarify our authority on those areas where questions have arisen, I am sending this letter, which, for future ease of reference, adds to and recapitulates some of the text of previous correspondence.

In your visits to our offices and in your correspondence, you have raised several questions about the United States Federal Trade Commission's authority in the online privacy area. I thought it would be useful to summarize my prior responses and to provide additional information about the agency's jurisdiction over consumer privacy issues raised in your most recent letter. Specifically, you ask whether: (1) The FTC has jurisdiction over transfers of employment-related data if done in violation of the U.S. safe harbor principles; (2) the FTC has jurisdiction over non-profit privacy "seal" programs; (3) the FTC Act applies equally to the offline as well as online world; and (4) what happens when the FTC's jurisdiction overlaps with other law enforcement agencies.

#### *FTC Act Application to Privacy*

The Federal Trade Commission's legal authority in this area is found in Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits "unfair or deceptive acts or practices" in or affecting commerce.<sup>35</sup> A deceptive practice is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion. A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition.<sup>36</sup>

Certain information collection practices are likely to violate the FTC Act. For example, if a web site falsely claims to comply with a stated privacy policy or a set of self-regulatory guidelines, Section 5 of the FTC Act provides a legal basis for challenging such a misrepresentation as deceptive. Indeed, we have successfully enforced the law to establish this principle.<sup>37</sup> In addition,

<sup>35</sup> 15 U.S.C. 45. The Fair Credit Reporting Act would also apply to Internet data collection and sales that meet the statutory definitions of "consumer report" and "consumer reporting agency."

<sup>36</sup> 15 U.S.C. 45(n).

<sup>37</sup> See *GeoCities*, Docket No. C-3849 (Final Order Feb. 12, 1999) (available at [www.ftc.gov/os/1999/](http://www.ftc.gov/os/1999/)

the Commission has taken the position it may challenge particularly egregious privacy practices as unfair under Section 5 if such practices involve children, or the use of highly sensitive information, such as financial records<sup>38</sup> and medical records. The Federal Trade Commission has and will continue to pursue such law enforcement actions through our active monitoring and investigative efforts, and through referrals we receive from self-regulatory organizations and others, including European Union member states.

#### **Backstop Self-Regulation**

The FTC will give priority to referrals of non-compliance with self-regulatory guidelines received from organizations such as BBOnline and TRUSTe.<sup>39</sup> This approach would be consistent with our longstanding relationship with the National Advertising Review Board (NARB) of the Better Business Bureau, which refers advertising complaints to the FTC. The National Advertising Division (NAD) of NARB resolves complaints, through an adjudicative process, concerning national advertising. When a party refuses to comply with an NAD decision, a referral is made to the FTC. FTC staff reviews the challenged advertising on a priority basis to determine if it violates the FTC Act, and often is successful in stopping the challenged conduct or convincing the party to return to the NARB process.

Similarly, the FTC will give priority to referrals of non-compliance with safe harbor principles from EU member states. As with referrals from U.S. self-regulatory organizations, our staff will consider any information bearing upon whether the conduct complained of violates Section 5 of the FTC Act. This commitment can also be found in the safe harbor principles under the Frequently Asked Question (FAQ 11) on enforcement.

#### **GeoCities: The FTC's First Online Privacy Case**

The Federal Trade Commission's first Internet privacy case, *GeoCities*, was based

[9902/9823015d%26o.htm](http://www.ftc.gov/opa/1999/9905/younginvestor.htm)); *Liberty Financial Cos.*, Docket No. C-3891 (Final Order Aug. 12, 1999) (available at [www.ftc.gov/opa/1999/9905/younginvestor.htm](http://www.ftc.gov/opa/1999/9905/younginvestor.htm)). See also Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Part 312 (available at [www.ftc.gov/opa/1999/9910/childfinal.htm](http://www.ftc.gov/opa/1999/9910/childfinal.htm)). The COPPA Rule, which became effective last month, requires operators of Web sites directed to children under 13, or who knowingly collect personal information from children under 13, to implement the fair information practice standards enunciated in the Rule.

<sup>38</sup> See *FTC v. Touch Tone, Inc.*, Civil Action No. 99-WM-783 (D.Co.) (filed April 21, 1999) at [www.ftc.gov/opa/1999/9904/touchtone.htm](http://www.ftc.gov/opa/1999/9904/touchtone.htm). Staff Opinion Letter, July 17, 1997, issued in response to a petition filed by the Center for Media Education, at [www.ftc.gov/os/1997/9707/cenmed.htm](http://www.ftc.gov/os/1997/9707/cenmed.htm).

<sup>39</sup> Indeed, the FTC recently filed a complaint in federal district court against a TRUSTe sealholder, Toysmart.com, seeking injunctive and declaratory relief to prevent the sale of confidential, personal customer information collected on the company Web site in violation of its own privacy policy. The FTC learned of this possible law violation directly from TRUSTe. *FTC v. Toysmart.com, LLC*, Civil Action No. 00-11341-RGS (D.Ma.) (filed July 11, 2000) (available at [www.ftc.gov/opa/2000/07/toysmart.htm](http://www.ftc.gov/opa/2000/07/toysmart.htm)).

on the Commission's authority under Section 5.<sup>40</sup> In that case, the FTC alleged that GeoCities misrepresented, both to adults and children, how their personal information would be used. The Federal Trade Commission's complaint alleged that GeoCities represented that certain personal identifying information it collected on its Web site was to be used only for internal purposes or to provide consumers with the specific advertising offers and products or services they requested, and that certain additional "optional" information would not be released to anyone without the consumer's permission. In fact, this information was disclosed to third parties who used it to target members for solicitations beyond those agreed to by the member. The complaint also charged that GeoCities engaged in deceptive practices relating to its collection of information from children. According to the FTC's complaint, GeoCities represented that it operated a children's area on its Web site and that the information collected there was maintained by GeoCities. In fact, those areas on the Web site were run by third-parties who collected and maintained the information.

The settlement prohibits GeoCities from misrepresenting the purpose for which it collects or uses personal identifying information from or about consumers, including children. The order requires the company to post on its Web site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, the settlement also requires GeoCities to obtain parental consent before collecting personal identifying information from children 12 and under. Under the order, GeoCities is required to notify its members and provide them with an opportunity to have their information deleted from GeoCities' and any third parties' databases. The settlement specifically requires GeoCities to notify the parents of children 12 and under and to delete their information, unless a parent affirmatively consents to its retention and use. Finally, GeoCities also is required to contact third parties to whom it previously disclosed the information and request that those parties delete that information as well.<sup>41</sup>

<sup>40</sup> *GeoCities*, Docket No. C-3849 (Final Order Feb. 12, 1999) (available at [www.ftc.gov/os/1999/9902/9823015d%26o.htm](http://www.ftc.gov/os/1999/9902/9823015d%26o.htm)).

<sup>41</sup> The Commission subsequently settled another matter involving the collection of personal information from children online. Liberty Financial Companies, Inc., operated the Young Investor website which was directed to children and teens, and focused on issues relating to money and investing. The Commission alleged that the site falsely represented that personal information collected from children in a survey would be maintained anonymously, and that participants would be sent an e-mail newsletter as well as prizes. In fact, the personal information about the child and the family's finances was maintained in an identifiable manner, and no newsletter or prizes were sent. The consent agreement prohibits such misrepresentations in the future and requires Liberty Financial to post a privacy notice on its

### ReverseAuction.com

In January 2000, the Commission approved a complaint against, and consent agreement with, ReverseAuction.com, an online auction site that allegedly obtained consumers' personally identifying information from a competitor site (eBay.com) and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business.<sup>42</sup> Our complaint alleged that ReverseAuction violated Section 5 of the FTC Act in obtaining the personally identifiable information, which included eBay users' e-mail addresses and personalized user identification names ("user IDs"), and in sending out the deceptive e-mail messages.

As described in the complaint, before obtaining the information, ReverseAuction registered as an eBay user and agreed to comply with eBay's User Agreement and Privacy Policy. The agreement and policy protect consumers' privacy by prohibiting eBay users from gathering and using personal identifying information for unauthorized purposes, such as sending unsolicited commercial e-mail messages. Thus, our complaint first alleged that ReverseAuction misrepresented that it would comply with eBay's User Agreement and Privacy Policy, a deceptive practice under Section 5. In the alternative, the complaint alleged that ReverseAuction's use of the information to send the unsolicited commercial e-mail, in violation of the User Agreement and Privacy Policy, was an unfair trade practice under Section 5.

Second, the complaint alleged that the e-mail messages to consumers contained a deceptive subject line informing each of them that his or her eBay user ID "will expire soon." Finally, the complaint alleged that the e-mail messages falsely represented that eBay directly or indirectly provided ReverseAuction with eBay users' personally identifiable information, or otherwise participated in dissemination of the unsolicited e-mail.

The settlement obtained by the FTC bars ReverseAuction from committing these violations in the future. It also requires ReverseAuction to provide notice to consumers who, as a result of receiving ReverseAuction's e-mail, registered or will register with ReverseAuction. The notice informs these consumers that their eBay users IDs were not about to expire on eBay, and that eBay did not know of, or authorize, ReverseAuction's dissemination of the unsolicited e-mail. The notice also provides these consumers with the opportunity to cancel registration with ReverseAuction and have their personal identifying information deleted from ReverseAuction's database. In addition, the order requires ReverseAuction to delete, and refrain from using or disclosing, the personal identifying

children's sites and obtain verifiable parental consent before collecting personal identifying information from children. *Liberty Financial Cos.*, Docket No. C-3891 (Final Order Aug. 12, 1999) (available at [www.ftc.gov/opa/1999/9905/younginvestor.htm](http://www.ftc.gov/opa/1999/9905/younginvestor.htm)).

<sup>42</sup> See *ReverseAuction.com, Inc.*, Civil Action No. 000032 (D.D.C.) (filed January 6, 2000) (press release and pleadings at [www.ftc.gov/opa/2000/01/reverse4.htm](http://www.ftc.gov/opa/2000/01/reverse4.htm)).

information of eBay members who received ReverseAuction's e-mail but who have not registered with ReverseAuction. Finally, consistent with prior privacy orders obtained by this agency, the settlement requires ReverseAuction to disclose its own privacy policy on its Internet site, and contains comprehensive record keeping provisions to allow the FTC to monitor compliance.

The *ReverseAuction* case demonstrates that the FTC is committed to using enforcement to buttress industry self-regulatory efforts in the area of online consumer privacy. Indeed, this case directly challenged conduct that undermined a Privacy Policy and User Agreement protecting consumers' privacy, and that could erode consumer confidence in privacy measures undertaken by online companies. Because this case involved the misappropriation by one company of consumer information protected by another company's privacy policy, it also may have particular relevance to the privacy concerns raised by the transfer of data between companies in different countries.

Notwithstanding the Federal Trade Commission's law enforcement actions in *GeoCities*, *Liberty Financial Cos.*, and *ReverseAuction*, the agency's authority in some areas of online privacy is more limited. As noted above, to be reachable under the FTC Act, the collection and use of personal information without consent must constitute either a deceptive or unfair trade practice. Thus, the FTC Act likely would not address the practices of a Web site that collected personally identifiable information from consumers, but neither misrepresented the purpose for which the information was collected, nor used or released the information in a way that was likely to cause substantial injury to consumers. Also, it currently may not be within the FTC's power to broadly require that entities collecting information on the Internet adhere to a privacy policy or to any particular privacy policy.<sup>43</sup> As stated above, however, a

<sup>43</sup> For this reason, the Federal Trade Commission stated in Congressional testimony that additional legislation probably would be required to mandate that all U.S. commercial Web sites directed toward consumers abide by specified fair information practices. "Consumer Privacy on the World Wide Web," Before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, July 21, 1998 (the testimony can be found at [www.ftc.gov/os/9807/privac98.htm](http://www.ftc.gov/os/9807/privac98.htm)). The FTC deferred calling for such legislation in order to give self-regulatory efforts the opportunity to demonstrate widespread adoption of fair information practices on Web sites. In the Federal Trade Commission's report to Congress on online privacy, "Privacy Online: A Report to Congress," June 1998 (the report can be found at [www.ftc.gov/reports/privacy3/toc.htm](http://www.ftc.gov/reports/privacy3/toc.htm)), the FTC recommended legislation to require that commercial Web sites obtain parental consent before collecting personally identifiable information from children under 13 years old. See footnote 3 *supra*. Last year, the FTC's report, "Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress," July 1999 (the report can be found at [www.ftc.gov/os/1999/9907/index.htm#13](http://www.ftc.gov/os/1999/9907/index.htm#13)), found sufficient progress in self-regulation and, accordingly, chose not to recommend legislation at that time.

In May 2000, the Commission issued a third report to Congress, "Privacy Online: Fair

company's failure to abide by a stated privacy policy is likely to be a deceptive practice.

Furthermore, the FTC's jurisdiction in this area covers unfair or deceptive acts or practices only if they are "in or affecting commerce." Information collection by commercial entities that are promoting products or services, including collecting and using information for commercial purposes, would presumably meet the "commerce" requirement. On the other hand, many individuals or entities may be collecting information online without any commercial purpose, and thereby may fall outside the Federal Trade Commission's jurisdiction. An example of this limitation involves "chat rooms" if operated by noncommercial entities, e.g., a charitable organization.

Finally, there are a number of full or partial statutory exclusions from the FTC's basic jurisdiction over commercial practices that limit the FTC's ability to provide a comprehensive response to Internet privacy concerns. These include exemptions for many information intensive consumer businesses such as banks, insurance companies and airlines. As you are aware, other federal or state agencies would have jurisdiction over those entities, such as the federal banking agencies or the Department of Transportation.

In cases where it does have jurisdiction, the FTC accepts and, resources permitting, acts on consumer complaints received by mail and telephone in its Consumer Response Center ("CRC") and, more recently, on its Web site.<sup>44</sup> The CRC accepts complaints from all consumers, including those residing in European Union member states. The FTC Act provides the Federal Trade Commission equitable power to obtain injunctive relief against future violations of the FTC Act, as well as redress for injured consumers. We would, however, look to see whether the company has engaged in a pattern of improper conduct, as we do not resolve individual consumer disputes. In the past, the Federal Trade Commission has provided redress for citizens of both the United States and other countries.<sup>45</sup> The FTC will continue to assert its authority, in appropriate cases, to provide redress to citizens of other countries who have been injured by deceptive practices under its jurisdiction.

Information Practices in the Electronic Marketplace," (the report can be found at [www.ftc.gov/os/2000/05/index.htm#22](http://www.ftc.gov/os/2000/05/index.htm#22)) which discusses the FTC's recent survey of commercial Web sites and their compliance with fair information practices. The report also recommended (by a majority of the Commission) that Congress enact legislation that would set forth a basic level of privacy protection for consumer-oriented commercial Web sites.

<sup>44</sup> See <https://www.ftc.gov/ftc/complaint.htm> for the Federal Trade Commission's online complaint form.

<sup>45</sup> For example, in a recent case involving an Internet pyramid scheme, the Commission obtained refunds for 15,622 consumers totaling approximately \$5.5 million. The consumers resided in the United States and 70 foreign countries. See [www.ftc.gov/opa/9807/fortunar.htm](http://www.ftc.gov/opa/9807/fortunar.htm); [www.ftc.gov/opa/9807/ftcrefund01.htm](http://www.ftc.gov/opa/9807/ftcrefund01.htm).

## Employment Data

Your most recent letter sought additional clarification concerning the FTC's jurisdiction in the area of employment data. First, you pose the question whether the FTC could take action under Section 5 against a company that represents it complies with U.S. safe harbor principles but transfers or uses employment-related data in a manner that violates these principles. We want to assure you that we have carefully reviewed the FTC authorizing legislation, related documents, and relevant case law and have concluded that the FTC has the same jurisdiction in the employment-related data situation as it would generally under Section 5 of the FTC Act.<sup>46</sup> That is to say, assuming a case met our existing criteria (unfairness or deception) for a privacy-related enforcement action, we could take action in the employment-related data situation.

We also would like to dispel any view that the FTC's ability to take privacy-related enforcement action is limited to situations where a company has deceived individual consumers. In fact, as the Commission's recent action in the *Reverse Auction*<sup>47</sup> matter makes clear, the FTC will bring privacy-related enforcement actions in situations involving data transfers between companies, where one company allegedly has acted unlawfully vis a vis another company, leading to possible injury to both consumers and companies. We expect this situation is the one in which the employment issue is most likely to arise, as employment data about Europeans is transferred from European companies to American companies that have pledged to abide by the safe harbor principles.

We do wish to note one circumstance in which FTC action would be circumscribed, however. This would occur in situations in which the matter is already being addressed in a traditional labor law dispute resolution context, most likely a grievance/arbitration claim or an unfair labor practice complaint at the National Labor Relations Board. This would occur, for example, if an employer had made a commitment in a collective bargaining agreement regarding the use of personal data and an employee or union claimed that the employer had breached that agreement. The Commission would likely defer to that proceeding.<sup>48</sup>

<sup>46</sup> Except as specifically excluded by the FTC's authorizing statute, the FTC's jurisdiction under the FTC Act over practices "in or affecting commerce" is coextensive with the constitutional power of Congress under the Commerce Clause, *United States v. American Building Maintenance Industries*, 422 U.S. 271, 277 n. 6 (1975). The FTC's jurisdiction would thus encompass employment-related practices in firms and industries in international commerce.

<sup>47</sup> See "Online Auction Site Settles FTC Privacy Charges," FTC News Release (Jan. 6, 2000), available at <http://www.ftc.gov/opa/2000/01/reverse4.htm>.

<sup>48</sup> The determination whether conduct is an "unfair labor practice" or a violation of a collective bargaining agreement is a technical one that is ordinarily reserved to the expert labor tribunals who will hear the complaints, such as arbitrators and the NRLB.

## Jurisdiction Over "Seal" Programs

Second, you ask whether the FTC would have jurisdiction over "seal" programs administering dispute resolution mechanisms in the United States that misrepresented their role in enforcing the "safe harbor" principles and handling individual complaints, even if such entities were technically "not for profit." In determining whether we have jurisdiction over an entity that holds itself out as a non-profit, the Commission closely analyzes whether the entity, while not seeking a profit for itself, furthers the profit of its members. The Commission has successfully asserted jurisdiction over such entities and as recently as May 24, 1999, the United States Supreme Court, in *California Dental Association v. Federal Trade Commission*, unanimously affirmed the Commission's jurisdiction over a voluntary nonprofit association of local dental societies in an antitrust matter. The Court held:

The FTC Act is at pains to include not only an entity "organized to carry on business for its own profit," 15 U. S. C. § 44, but also one that carries on business for the profit "of its members." \* \* \*. It could, indeed, hardly be supposed that Congress intended such a restricted notion of covered supporting organizations, with the opportunity this would bring with it for avoiding jurisdiction where the purposes of the FTC Act would obviously call for asserting it.

In sum, determining whether to assert jurisdiction over a particular "non-profit" entity administering a seal program would require a factual review of the extent to which the entity provided economic benefit to its for-profit members. If such an entity operated its seal program in a manner that provided an economic benefit to its members, the FTC likely would assert its jurisdiction. As a separate point, the FTC likely would have jurisdiction over a fraudulent seal program that misrepresents its status as a non-profit entity.

## Privacy in the Offline World

Third, you note that our prior correspondence has focused on privacy in the online world. While online privacy has been a major concern of the FTC as a critical component to the development of electronic commerce, the FTC Act dates back to 1914 and applies equally in the offline world. Thus, we can pursue offline firms that engage in unfair or deceptive trade practices with regard to consumers' privacy.<sup>49</sup> In fact, in a case brought by the Commission last year, *FTC v. TouchTone Information, Inc.*,<sup>50</sup> an "information broker" was charged with illegally obtaining and selling consumers' private financial information. The

<sup>49</sup> As you know from earlier discussions, the Fair Credit Reporting Act also gives the FTC the authority to protect consumers' financial privacy within the purview of the Act and the Commission recently issued a decision pertaining to this issue. See *In the Matter of Trans Union*, Docket No. 9255 (March 1, 2000) (press release and opinion available at [www.ftc.gov/os/2000/03/index.htm#1](http://www.ftc.gov/os/2000/03/index.htm#1)).

<sup>50</sup> Civil Action 99-WM-783 (D.Colo.) (available at <http://www.ftc.gov/opa/1999/9904/touchtone.htm>) (tentative consent decree pending).

Commission alleged that Touch Tone obtained consumers' information by "pretexting," a term of art coined by the private investigation industry to describe the practice of getting personal information about others under false pretenses, typically on the telephone. The case, filed April 21, 1999, in federal court in Colorado, seeks an injunction and all illegally gained profits.

This law enforcement experience, as well as recent concerns about the merging of offline and online databases, the blurring of distinctions between online and offline merchants, and the fact that a vast amount of personal identifying information is collected and used offline, make clear that significant attention to offline privacy issues is warranted.

## Overlapping Jurisdiction

Finally, you pose the question of the interplay of the FTC's jurisdiction with that of other law enforcement agencies, particularly in cases where there is potentially overlapping jurisdiction. We have developed strong working relationships with numerous other law enforcement agencies, including the federal banking agencies and the state attorneys general. We very often coordinate investigations to maximize our resources in instances of overlapping jurisdiction. We also often refer matters to the appropriate federal or state agency for investigation.

I hope this review is helpful. Please let me know if you need any further information.

Sincerely,  
Robert Pitofsky  
July 14, 2000.

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

Dear Director General Mogg:

I am providing you this letter at the request of the U.S. Department of Commerce to explain the role of the Department of Transportation in protecting the privacy of consumers with respect to information provided by them to airlines.

The Department of Transportation encourages self-regulation as the least intrusive and most efficient means of ensuring the privacy of information provided by consumers to airlines and accordingly supports the establishment of a "safe harbor" regime that would enable airlines to comply with the requirements of the European Union's privacy directive as regards transfers outside the EU. The Department recognizes, however, that for self-regulatory efforts to work, it is essential that the airlines that commit to the privacy principles set forth in the "safe harbor" regime in fact abide by them. In this regard, self-regulation should be backed by law enforcement. Therefore, using its existing consumer protection statutory authority, the Department will ensure airline compliance with privacy commitments made to the public, and pursue referrals of alleged non-compliance that we receive from self-regulatory organizations and others, including European Union member states.

The Department's authority to take enforcement action in this area is found in 49 U.S.C. 41712 which prohibits a carrier

from engaging in "an unfair or deceptive practice or an unfair method of competition" in the sale of air transportation that results or is likely to result in consumer harm. Section 41712 is patterned after Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). However, air carriers are exempt from Section 5 regulation by the Federal Trade Commission under 15 U.S.C. 45(a)(2).

My office investigates and prosecutes cases under 49 U.S.C. 41712. (See, *e.g.*, DOT Orders 99-11-5, November 9, 1999; 99-8-23, August 26, 1999; 99-6-1, June 1, 1999; 98-6-24, June 22, 1998; 98-6-21, June 19, 1998; 98-5-31, May 22, 1998; and 97-12-23, December 18, 1997.) We institute such cases based on our own investigations, as well as on formal and informal complaints we receive from individuals, travel agents, airlines, and U.S. and foreign government agencies.

I would point out that the failure by a carrier to maintain the privacy of information obtained from passengers would not be a per se violation of section 41712. However, once a carrier formally and publicly commits to the "safe harbor" principles of providing privacy to the consumer information it

obtains, then the Department would be empowered to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier that has committed to honoring the "safe harbor" principles, any failure to do so would likely cause consumer harm and be a violation of section 41712. My office would give the investigation of any such alleged activity and the prosecution of any case evidencing such activity a high priority. We will also advise the Department of Commerce of the outcome of any such case.

Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties for violations of those orders. Although we do not have the authority to award damages or provide pecuniary relief to individual complainants, we do have the authority to approve settlements resulting from investigations and cases brought by the Department that provide items of value to consumers either in mitigation or as an offset to monetary penalties otherwise payable. We have done so in the past, and we can and will do so in the context of the safe harbor

principles when circumstances warrant. Repeated violations of section 41712 by any U.S. airline would also raise questions regarding the airline's compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority. (See, DOT Orders 93-6-34, June 23, 1993, and 93-6-11, June 9, 1993. Although this proceeding did not involve section 41712, it did result in the revocation of the operating authority of a carrier for a complete disregard for the provisions of the Federal Aviation Act, a bilateral agreement, and the Department's rules and regulations.)

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,  
Samuel Podberesky,  
*Assistant General Counsel for Aviation Enforcement and Proceeding.*

[FR Doc. 00-18489 Filed 7-21-00; 8:45 am]

**BILLING CODE 3510-DR-U**