

the Nuts & Bolts of the EU Safe Harbor

The European Commission's Directive on Data Protection went into effect in October 1998, and prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union.

One of the most significant effects of increased online trading between Europe and the United States is the growing concern about privacy and data protection. There is no general agreement between Europe and the United States in the area of ecommerce and likewise, there is no specific agreement between the European Union and the United States on jurisdiction and applicable law in civil matters. Although the current consumer data privacy protection principles of the European Union and the United

By Brett Tarr

States are both founded upon the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued in 1980 by the Organization for Economic Cooperation and Development,

they are based on different approaches. The United States uses a mix of legislation, regulation and self-regulation.

Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices in the marketplace. (15 USCA § 45 (2000)). The Federal Trade Commission (FTC) has brought a number of cases to force companies to keep the promises they make to consumers about privacy and, in particular, the precautions they take to secure consumers' personal information. The FTC has implemented rules to protect consumers' personal financial information held by financial institutions (15 USC §§ 6801-6809 (2000)) and also protects consumer privacy under the Fair Credit Reporting Act (15 USC § 1681 et seq. (2000)), among other statutory regulations.

While the United States leans more heavily on a "code of conduct" for businesses, the European Union relies on the comprehensive legislation outlined above. As a result of these different privacy approaches, the directive could have significantly hampered the ability of US companies to engage in many trans-Atlantic transactions. (See: www.lctjournal.washington.edu/vol11/a010kierkegaard.html - cite18)

The 1998 EU Data Protection Directive states that personal data can only be transferred to third countries that provide "adequate protection." The existence of a fairly aggressive privacy regime in the European Union creates problems for American multinational firms operating in both markets. Personal data is defined as "any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." (See: www.cdt.org/privacy/eudirective/eu_directive_.html (art. 2a))

This definition is meant to be very broad. Data is "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of personal data indicate employee records, customer/client information, address, credit card number, bank statements and criminal record.

Additional key definitions in the directive include:

Processing of Personal Data

Processing of personal data (or “processing”) is defined as any operation or set of operations which is performed upon personal data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. (See: www.cdt.org/privacy/eudirective/eu_directive_.html (art. 2a))

Controller

Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.

Processor

Processor refers to a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Third Party

Third party is any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

Recipient

Recipient is a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not. However, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

Sensitive Data

To comply with the EU Directive, there is a new regime for sensitive data, with stricter conditions for processing than for other data (generally requiring express consent). Individuals have to be informed on request of the logic behind any automated decision-making, and there is a new right to object to direct marketing. (See: www.cdt.org/privacy/eudirective/eu_directive_.html (art. 2a))



BRETT TARR serves as general counsel for eMag Solutions, based in Atlanta, GA. Previously, Tarr worked as a practicing attorney at King & Spalding LLP, and has held chief operating officer, legal counsel and senior marketing executive positions. Tarr graduated Phi Beta Kappa from University of California at Los Angeles. He earned his law degree from Duke University School of Law and also holds an MBA in marketing and management from Georgia State University. He can be contacted at btarr@emagsolutions.com.

Directive on Data Protection

Article 25 of the EU Directive prohibits any EU country from transferring personal data via the internet to, or receiving data from, countries deemed to lack “adequate” internet privacy protection. The United States is among those countries since it has no national data privacy laws that meet the EU standards. Instead of federal legislation, the US government permits American companies to address privacy issues through self-regulation, which many EU officials regard as too lax to adequately safeguard individuals who use the web.

In order to bridge these different privacy approaches and provide a streamlined means for US organizations to comply with the directive, the US Department of Commerce in consultation with the European Commission developed a “Safe Harbor” framework. Under the Safe Harbor program, US companies who voluntarily adhere to a set of data protection principles recognized by the EU as providing adequate protection are deemed

to meet the requirements of the directive. Companies can self-certify or join a privacy seal program that has been certified as in compliance with the Safe Harbor agreement. The application for Safe Harbor certification is available online and is fairly straightforward. (See <http://ita-web.ita.doc.gov/safeharbor/shreg.nsf/login?openform>.)

The US Dept of Commerce manages the list of firms that have joined the Safe Harbor program. It is publicly available, kept up-to-date and includes firms that have let their Safe Harbor status lapse.

Decisions by organizations to qualify for Safe Harbor certification are entirely voluntary, but organizations that decide to adhere to these principles must comply with these principles in order to obtain and retain the benefits of certification and publicly declare that they do so. All organizations qualifying for the Safe Harbor should, for purposes of transparency and other beneficial reasons, notify the Department of Commerce or its nominee in accordance with the guidance set forth in the Guide to Self-Certification found at www.export.gov/static/sh_selfcert_guide_lat-est_eg_main_018879.pdf.

In addition to any exceptions provided for by the directive and EU member state law, adherence to these principles may be limited to the extent necessary to meet US national security, public interest and law enforcement requirements, as well as other US statutory and regulatory provisions.

Safe Harbor Benefits

Safe Harbor certification provides a number of important benefits to US firms. Benefits for US organizations participating in the Safe Harbor program will include:

- All 27 member states of the European Union will be bound by the European Commission's finding of adequacy of Safe Harbor certification. (Current EU member states include Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.)
- Additionally, several non-EU member states have adopted the EU model for data privacy and data transfer control (including Argentina, Canada, Hong Kong, Norway and Switzerland), allowing data transfer between the United States and these EU-model countries under the Safe Harbor program.
- Companies participating in the Safe Harbor will be deemed adequate, and data flows to those companies will continue.
- Member state requirements for prior approval of data transfers to non-EU countries either will be waived or approval will be automatically granted.
- Claims brought by European citizens against US companies will be heard in the United States subject to limited exceptions.
- In exchange for Safe Harbor certification, US companies are shielded from prosecution under the EU data protection laws.

The Safe Harbor framework offers a simple and cheap means of complying with the adequacy requirements of the directive, which should particularly benefit small and medium enterprises.

An EU organization can ensure that it is sending information to a US organization participating in the Safe Harbor by viewing the public list of Safe Harbor-certified organizations posted at www.export.gov/safeharbor.

The Safe Harbor framework offers a simple and cheap means of complying with the adequacy requirements of the directive, which should particularly benefit small and medium enterprises.

How Does an Organization Join?

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

To qualify for the Safe Harbor, an organization can:

1. join a self-regulatory privacy program that adheres to the Safe Harbor's requirements. (As noted above, self-certification is easy and straightforward, and even a very small company without in-house legal resources should be able to do it without the expense of recourse to a third party organization or group) or
2. develop its own self-regulatory privacy policy that conforms to the Safe Harbor.

Any organization that violates the Safe Harbor principles may be held in violation of state or federal unfair and deceptive trade practices law.

Seven Principles of Safe Harbor

Notice

Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers for limiting its use and disclosure.

Choice

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

Onward Transfer (Transfers to Third Parties)

To disclose information to a third party, organizations must apply the notice and choice principles.

Additional Topics for Model Privacy Policy and Other Key Elements of Data Privacy

A wide array of organizations, legal support institutions, symposiums and tools are available to assist with development of conduct codes, model privacy policies and alternative dispute resolutions. A partial list of valuable resources is provided below as a starting point.

Codes of Conduct/Privacy Frameworks:

Online Privacy Alliance

The alliance has developed guidelines for creating an effective privacy policy, establishing enforcement mechanisms and protecting children's privacy online. The alliance is comprised of more than 40 global corporations and associations.

Privacy Leadership Initiative (PLI)

PLI has developed model practices for the exchange of personal information between business and consumers. It is the initiative comprised of more than 20 companies and associations.

Network Advertising Initiative

Created by leading online advertisers engaged in "online profiling." Sets forth self-regulatory principles for online advertisers to protect consumers' privacy while engaging in online advertising.

Global Business Dialogue on Electronic Commerce (GBDe)

A worldwide, CEO-led business initiative established in January 1999 to assist in the creation of a policy framework for the development of a global online economy. It has developed personal data protection guidelines for online merchants, trustmark providers and many other businesses.

AICPA/CICA Privacy Framework

The Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants (AICPA), and the Assurance Services Development Board (ASDB) of the Canadian Institute of Chartered Accountants (CICA) have issued an exposure draft of a proposed Privacy Framework. The proposed Framework provides criteria and related material for protecting the privacy of personal information and can be used by certified public accountants (CPAs) in the United States and chartered accountants (CAs) in Canada, both in industry and in public practice, to guide and assist the organizations they serve in implementing privacy programs.

Where an organization wishes to transfer information to a third party outside the EU that is acting as an agent (1), it may do so if it makes sure that the third party subscribes to the Safe Harbor principles or is subject to the directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles. The EU has established Standard Contract Clauses that should be included in any contract which involves the transfer of data between an organization's EU operations and a third party outside the EU. Even if the third party organization is Safe Harbor-certified, "downstream" communication of the data, for example, from the third party to the organization's US headquarters requires the Standard Contract Clauses. There are two versions (one for data importer/data exporter and one for data controller/data processor) and the EU prohibits any departure from the model language. (See Commission Decision of December 27, 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.)

Access

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

Security

Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity

Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use — accurate, complete and current.

Enforcement

In order to ensure compliance with the Safe Harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable

law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Those that fail to provide annual self-certification letters will no longer appear in the list of participants and Safe Harbor benefits will no longer be assured.

How and Where Will the Safe Harbor Be Enforced?

In general, enforcement of the Safe Harbor will take place in the United States in accordance with US law and will be carried out primarily by the private sector. In practice, EU data privacy principles, which are the basis of the Safe Harbor program, are enforced against multi-nationals operating in the EU by the various data protection agencies established under the EU Directive in each EU member state. For example, the Commission Nationale de l'Informatique et des Libertés (CNIL) (France) issued a decision in 2005 against MacDonald's concerning an employee hotline operated by a third-party service provider in the United States. This is the real risk for companies that do not adhere to Safe Harbor requirements: enforcement in the EU.

Private Sector Enforcement

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

Organizations can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities by committing to cooperate with data protection authorities located in Europe or through independent recourse mechanisms. The 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. Note, however, that the Enforcement Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute. www.export.gov/safeharbor/eg_main_018258.asp

Government Enforcement

While generally the Safe Harbor principles are enforced against multinational companies in the EU countries in which they operate, there may be situations, — depending on the industry sector — where the Federal Trade Commission, comparable US government agencies and/or the states may provide overarching government enforcement of the Safe Harbor principles. Where a company relies in whole or in part on self-regulation in complying with the Safe Harbor principles, its failure to comply with such self regulation must be actionable under federal or state law prohibiting unfair and deceptive acts — or it is not eligible to join the Safe Harbor.

At present, US organizations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation with respect to air carriers and ticket agents may participate in the Safe Harbor. The Federal Trade Commission and the Department of Transportation, with respect to air carriers and ticket

Privacy Policy Generator Tools

Organization for Economic Cooperation and Development (OECD)

Electronic commerce is a central element in the OECD's vision of the potential that the networked world holds for sustainable economic growth, more and better jobs, expanding world trade and improved social conditions.

Direct Marketing Association (DMA)

This tool was developed to help marketers create policies that are consistent with the DMA's Privacy Principles for Online Marketing.

agents, have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the Safe Harbor framework but then fail to live up to their statements. (See: www.export.gov/safeharbor/eg_main_018258.asp)

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

Failure to Comply with the Safe Harbor Requirement:

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

On the public list it maintains of organizations self-certifying, the Department of Commerce will indicate adherence to the Safe Harbor requirements any notification it receives of persistent failure to comply and will make clear

Safe Harbor: A Practical Discussion of What It Means for In-house Counsel

For multinational corporations, the 1998 EU Data Protection Directive creates limitations on the transfer of personal data from the European Union to other countries. How does corporate counsel reconcile the need for information transfer as a part of day-to-day business with the notion of providing adequate protection when that information moves back and forth in an increasingly globalized world?

The existence of a fairly aggressive privacy regime in the European Union creates problems for US multinational firms operating in both markets since Article 25 of the EU Directive prohibits the transfer of personal data via the internet between EU member states and countries deemed to lack adequate Internet privacy protection. The United States is among those countries, since it has no national data privacy laws that meet the EU standards.

The first and seemingly obvious question is this: To what extent does an organization operate within the European Union and the United States concurrently? The higher the degree of involvement, the greater the need to reconcile EU data privacy laws with company policy to avoid incurring organizational risk during routine information transfer between trans-Atlantic offices.

The legal department will need to either:

1. develop its own self-regulatory privacy policy that conforms to the Safe Harbor; or
2. join a self-regulatory privacy program that adheres to the Safe Harbor requirements.

Either way, the organization will need to get onto the Department of Commerce's register for Safe Harbor companies to avoid prosecution under EU data privacy laws.

In-house counsel need to monitor risk to the organization through the seven key principles of data privacy:

1. Notice,
2. Choice,
3. Transfer to Third Parties,
4. Access,
5. Security,
6. Data Integrity, and
7. Enforcement.

First, the legal department will need to adopt standard language in corporate communications and bylaws that will notify individuals about the purposes for which they collect and use information about them. As part of this notice, the legal department will need to develop appropriate language allowing individuals to opt out of having their information transferred to third parties (or opt in in the case of sensitive personal data). Once this language is in place, the legal department still will need to provide individuals with access to the information the organization is holding in order to allow review and correction of erroneous information on file.

Another element the legal department must oversee in conjunction with the IT department is the protection of individuals' information from misuse, unauthorized access, accidental disclosure or possible destruction. Not only is the legal department responsible for maintaining integrity of the data, but they also must ensure the underlying information is reliable and continues to serve its intended purpose. This is similar to a spoliation principle in legal discovery, where the legal department carries the burden of the continuing accuracy and viability of the data being held.

which organizations are assured and which organizations are no longer assured of Safe Harbor benefits. To date, there are no Safe Harbor-certified organizations that have received any notice of persistent failure to comply

An organization applying to participate in a self-regulatory body for the purposes of requalifying for the Safe Harbor must provide that body with full information about its prior participation in the Safe Harbor.

Model Contracts

Another option may permit American companies to bypass the Safe Harbor program altogether by negotiating “model contracts” with either an EU country’s data protection authority or with an individual whose personal data will be transferred electronically. These contracts would verify that company practices conform with the EU’s data protection laws.

In 2001, 2002 and 2004, the Commission issued three separate decisions anointing three different boilerplate contracts as appropriate cover for an EU data controller (data exporter) to send personal data to controllers and processors in the United States and elsewhere abroad (data importers). The Commission’s three decisions amount to pre-approved adherence contracts which data importers and exporters can either agree to accept in whole, or not. To negotiate terms within the forms would kill the Commission’s protection, so after a data exporter and importer decide to use a model contract, all there is to negotiate is which of the three forms to use.

Despite the model contracts acting as a type of pre-approved adherence contract, some data processing authorities (including the French CNIL), must approve filed model contracts before they can be relied upon for data transfers.

The final obligation of the legal department relates to enforcement of the company’s ongoing compliance with Safe Harbor principles, specifically implementation of processes for verification of data, remedy for breaches and/or inaccuracies and the annual submission of self-certification letters to maintain up-to-date status on the Department of Commerce Safe Harbor Register.

Since Safe Harbor requires annual re-filing to maintain certification, there will be a continuing burden on the legal department within a corporation to ensure these filings are not only executed in a timely manner, but also that the company’s procedures and bylaws continue to reflect the proper language to satisfy the key principles of data privacy across its multinational operations.

Additional Topics for Consideration in the Age of Data Privacy

Additional issues to consider in light of increasing focus on data privacy include areas such as identity theft, cyber fraud and cyber harassment. For more information on these topics, see the following resources:

Identity Theft:

- www.reuters.com/article/pressRelease/idUS207947+25-Feb-2009+BW20090225
- www.lifelock.com/about-us/press-room/2009-press-releases/top-identity-theft-trends
- [www.smartbrief.com/news/pci/storyDetails.jsp?issueid=E0F5E0A8-B8BF-47D2-8113-C3592DFF8D29©id=858638A9-0523-4D7E-](http://www.smartbrief.com/news/pci/storyDetails.jsp?issueid=E0F5E0A8-B8BF-47D2-8113-C3592DFF8D29©id=858638A9-0523-4D7E-A2E8-DE79FAF920F0&sid=9a375f81-708d-44e5-a5f7-ca5c11478ab7&brief=pci)

[A2E8-DE79FAF920F0&sid=9a375f81-708d-44e5-a5f7-ca5c11478ab7&brief=pci](http://www.identitytheftblog.info/identity-theft/identity-theft-cybercrime-2009)

- www.identitytheftblog.info/identity-theft/identity-theft-cybercrime-2009
- <https://365.rsaconference.com/blogs/articles/2009/03/02/top-identity-theft-trends-to-watch-out-for-help-net-security;jsessionid=D3CAE28B00A5CCE38FA4B757C9C5DE80>

Cyber Fraud:

- www.sec.gov/investor/pubs/cyberfraud.htm
- www.fbi.gov/cyberinvest/escams.htm
- www.crime-research.org/articles/computer-crime-cyber-fraud
- www.ic3.gov/default.aspx
- http://findarticles.com/p/articles/mi_m4153/is_1_59/ai_82804404
- http://voices.washingtonpost.com/securityfix/2008/04/consumers_report_239_million_l.html

Cyber Harassment:

- <http://en.wikipedia.org/wiki/Cyberstalking>
- www.officer.com/article/article.jsp?id=30373&siteSection=18
- www.wiredsafety.org/cyberstalking_harassment/index.html
- <http://crime.about.com/b/2004/11/18/man-sentenced-for-cyber-harassment.htm>
- <http://quitstalkingme.com/2009/02/20/a-new-state-law-to-expand-cyber-harassment-to-social-networks>
- www.ireport.com/docs/DOC-260423

Speaking very broadly, the Commission's model contracts act like private Safe Harbor arrangements, where a US data importer contractually pledges to follow a package of rules that fairly closely tracks the obligations of Safe Harbor.

Although the model contractual clauses themselves are pure boilerplate, parties must pinpoint in an appendix the precise categories of data and types of processing they will conduct. (General catchall language like "all human resources data for any and all HR purposes" is not good enough.) Parties must also say whether they will transmit any sensitive data. And parties to model contracts have to promise to respond to reasonable inquiries from data subjects and supervisory authorities, as well as commit to accepting data audits by data exporters or independent inspection bodies.

Liability: If a party breaches a model contract, then data subjects (third party beneficiaries) who suffer injury can win compensation from the data exporter or importer, as could a member state data protection authority.

The Model Contract is a contract between the transferor of personal data in the EU and the transferee, and creates certain rights and obligations for the benefit of the "data subjects" (i.e., the individuals to whom the personal data pertains). The Model Contract may be enforced by the data subjects, either in the courts of the EU member country from which the personal data is transferred or, at the data subjects' option, by referring any dispute to mediation by an independent party or by the Data Protection Authority of the transferor's home country. The parties to the Model Contract are liable to the data subject for any damages resulting from a violation of the Model Contract clauses

Under the Model Contract clauses, the transferor of personal data is required to (1) comply with the data protection laws of the transferor's home country in collecting and processing the data, (2) inform the data subject of the proposed transfer where special categories of data (i.e., data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade

Privacy "Seal" Programs/Verification (and/or Audit) Services

TRUSTe

TRUSTe is an independent, non-profit privacy organization whose mission is to build users' trust and confidence on the Internet and, in doing so, accelerate growth of the Internet industry. TRUSTe was founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium, who act as independent, unbiased trust entities.

The Better Business Bureau OnLine (BBBOnLine)

BBBOnLine is a wholly owned subsidiary of the Council of Better Business Bureaus. BBBOnLine's mission is to promote trust and confidence on the internet through the BBBOnLine Reliability and Privacy Seal Programs. BBBOnLine's website seal programs allow companies with websites to display the seals once they have been evaluated and confirmed to meet the program requirements. The BBBOnLine Privacy Seal confirms a company stands behind its online privacy policy and has met the program requirements regarding the handling of personal information that is provided through its website.

The Direct Marketing Association (The DMA)

The Direct Marketing Association (The DMA) is the largest trade association for businesses interested in

interactive and database marketing. Companies displaying The DMA Member logo have committed to the association's Privacy Promise. The DMA's Privacy Promise is an assurance to consumers that US marketers who are DMA members will use personal information in a manner that respects consumers' wishes.

AICPA WebTrust

The WebTrust program is a set of ecommerce standards comprised of prevailing best practices and requirements from around the world; an independent verification that a site meets the standards; and a webtrust seal.

SquareTrade

SquareTrade's mission is to build trust in transactions and to create a better online trading experience. SquareTrade's services aim to help buyers identify trustworthy sellers they can buy from safely, as well as help good sellers show buyers that they can be trusted.

Entertainment Software Rating Board (ESRB)

ESRB Privacy Online addresses consumers' concerns regarding privacy by requiring web publishers to develop and implement privacy policies and practices for their websites.

union membership, health or sex life) are involved, and (3) provide the data subjects with a copy of the Model Contract clauses upon request.

The transferee of personal data is required to process the data according to a body of laws selected by the parties to the Model Contract from among those approved by the EU as offering adequate protection. These may include the laws of the transferor's home country, the "Mandatory Data Protection Principles" adopted by the EU Commission, or specific laws of the transferee's home country which are determined by the EU Commission to provide adequate data protection, but which might not otherwise be applicable to the particular business of the transferee. The transferee is also required to comply with requirements and restrictions substantially similar to those found in the EU Data Protection Directive with respect to matters such as the purpose of processing data, the data subjects' right to access, and onward transfer, as well as to cooperate with the supervisory authority of the transferor's home country with respect to any inquiries regarding data processing and to abide by any advice given by such supervisory authority.

The Model Contract offers US companies a much-needed alternative to the Safe Harbor. For companies in certain industries to which the Safe Harbor is not available, such as financial institutions and telecommunications companies, the Model Contract offers the only means by which personal data may be transferred from within the EU. However, US companies should be cautious in using the Model Contract clauses, as they may be required to defend lawsuits in foreign courts, become liable for the processing of data by European companies from which it receives personal data, and otherwise subject themselves to the requirements of the EU Data Protection Directive, compliance with which may be quite costly.

Safe Harbor Struggles

Safe Harbor has struggled to get off the ground and major US corporations have been slow to embrace the program. In April 30, 2009, 1,790 US companies were officially listed on the Department of Commerce's register for Safe Harbor companies. Interestingly, financial-services companies, such as insurers and banks, continue to argue that they did not need to participate in the Safe Harbor program because the online privacy protections contained in the Gramm-Leach-Bliley Act of 1999 assure their compliance with the EU Directive.

Because Safe Harbor emerged as a compromise between the EU Commission and the United States very different from what each party had originally wanted, and because Safe Harbor is a unique-in-the-world arrangement that applies only to the United States, it should not be surprising that Safe Harbor has attracted criticisms from the beginning. www.proskauerguide.com/law_topics/28/III

Alternative Dispute Resolution (Independent Recourse) Mechanisms

In addition to the "seal" programs listed above, the following organizations provide dispute resolution services for their members/clients:

American Arbitration Association

The American Arbitration Association is available to resolve a range of disputes through mediation, arbitration, elections and other out-of-court settlement procedures. The American Arbitration Association assists in the design of ADR systems for corporations, unions, government agencies, law firms and the courts.

JAMS

JAMS provides the highest quality dispute resolution services to our clients and to our local, national and global communities. JAMS' neutrals include the ADR industry's most respected mediators, arbitrators, private judges, facilitators, special masters (or referees) and neutral advisors.

Detractors tend to focus on shortcomings in compliance; Safe Harbor is a self-certification system without mandatory independent verification of what a business actually does (Safe Harbor companies can have an independent body check their compliance up front and annually thereafter, but independent-body check-ups are not required, and few companies seem to do them.)

The fact that Safe Harbor enforcement tends to be complaint-driven, rather than overseen by regulators, makes Europeans nervous — especially in light of Europeans' fear that US data processors are less than vigilant about complaints coming in from across the Atlantic.

Many prominent US trade analysts question the need to follow the EU framework when addressing data privacy. According to Aaron Lukas, a trade policy analyst with the Cato Institute's Center for Trade Policy Studies, Safe Harbor, at best, faces an uncertain future (www.freetrade.org/node/47). Lukas states that while The United States should recognize that Europe has the right to set its own privacy policies, it should not be pressured into copying the EU's unwise data protection model. Relying on technology and market incentives, rather than regulation, to protect privacy empowers individual consumers to make their own choices, encourages new business and innovation, and protects free speech. Lukas

posits that the United States should stick to that course regardless of what Europe does. At the same time, he notes, if European law is enforced in such a way as to put US companies at an unfair disadvantage — which is entirely possible — the United States should not hesitate to defend its interests through the dispute resolution mechanism of the World Trade Organization.

Over the past decade, the EU Commission has studied the operation of the Safe Harbor and issued reports on its effectiveness, in 2002 and 2004, each time finding that it has substantially failed to live up to the expectations of its drafters. Notwithstanding this disappointment, each time the European Union has reported on the operation of the Safe Harbor, it has reiterated its commitment to working with the United States within the Safe Harbor framework. As a result, US businesses that transfer personal information from the European Union to the United States can still take advantage of the Safe Harbor. In addition, US businesses that do not wish to join the Safe Harbor but do wish to transfer personal information from the European Union to the United States can add standard terms to their contracts setting out minimum privacy guarantees and submitting them to the jurisdiction of EU privacy regulators with regard to the transaction in question. (Sylvia Mercado

Kierkegaard, “*Safe Harbor Agreement - Boon or Bane?*,” 1 Shidler J. L. *Com. & Tech.* 10 (Aug. 2, 2005).


Interpretations of Provisions

The Investment Company Institute drafted a long proposal to the Department of Commerce suggesting guidelines in the interpretation of Safe Harbor data protection and how enforcement should be carried out, referencing many of the seven key principles identified by the European Commission’s Data Protection Act.

Specific privacy regulations adopted by securities regulators must be given appropriate deference. The Investment Company Institute argued that the Securities and Exchange Commission and the National Association of Securities Dealers understand the structure and organization of mutual fund organizations and, as a result, are in the best position to craft rules that would appropriately regulate the protection of individual privacy in the industry. Should one of these regulators promulgate a rule specifically relating to privacy, firms that are subject to and in compliance with it should qualify for the Safe Harbor, regardless of whether the rule precisely mirrors the Safe Harbor principles.

The transition period must be long enough to allow US firms to come into compliance with the Safe Harbor. The institute commented that the transition period for compliance with the Safe Harbor must be long enough to allow regulators to act and companies to respond and must take into account the difficulties modifying systems during 1999 and 2000, particularly in light of the Y2K problem. We suggested that the transition period, at a minimum, should be 18 months long.

The principles of notice, choice and onward transfer must allow for uses of information that are not incompatible with the relationship between an investment company and its shareholders. The institute stressed that the principles of notice, choice and onward transfer in the Safe Harbor must be interpreted to permit companies to efficiently provide customers with the service and the products that they have come to expect. The restrictions on choice and onward transfer should not hinder firms from using information to create benefits for shareholders, such as unified account statements.

Rights of access must be reasonable. The institute strongly supported including explicit language in the Safe Harbor principle and the FAQ on access that a consumer’s right of access to information about him or her should be tempered by reasonableness. The institute also supported making clear that companies may deny access to the extent it would reveal confidential commercial information. 

Have a comment on this article? Email editorinchief@acc.com.

Privacy Protection Training/ Awareness

US Federal Trade Commission

Provides public information on privacy compliance initiatives and safeguards.

GetNetWise

ISP organization that educates parents on tools and measures to protect their children’s privacy and security online.

Center for Democracy and Technology and the Privacy Leadership Initiative

Created “privacy toolboxes” for online users, which are posted on their websites. These “toolboxes” typically tell users how they can limit disclosure of their personal information, what choices they have about how such information is used and shared, and under what circumstances they can access it.

Econsumer.gov

Website provides means of consumer reporting in Internet privacy complaints and those relating to cross-border ecommerce transactions.



12

13

14

15

16

6

7

8

9

10