Bridging the Difference:  
The Safe Harbor and Information Privacy in  
The United States and The European Union

Barbara S. Wellbery¹

1. Introduction

Today’s information technologies allow information to be collected, compiled, analyzed, and delivered around the world more quickly and inexpensively than ever before. Where it was once difficult, time-consuming, and expensive to obtain and compile information, it is now often available with a few simple clicks of a computer mouse. This increased access to information facilitates personal and political expression as well as commerce, education, and health care.

Information technologies are transforming the face of global commerce. World trade involving information technologies and related services and products (computer software, movies, sound recordings, databases, and financial services, to name just a few) has grown rapidly in the past decade and now accounts for over $120 billion of U.S. exports alone.² We are now said to live in an “Information Economy.”

Consumers benefit from the increased access to information. They surf the “Internet” seeking all kinds of information. Thinking of buying a house? You can shop for it on the Internet. Information is available about neighborhoods, prices, and schools; you can even take a virtual tour of the house while on-line.

Companies, too, benefit. They can create new markets as the Internet allows them to reach potential customers easily and cheaply. Increased access to information about customers can reduce marketing and inventory costs, and allow better target advertising. As a result, consumer information has become a “hot” commodity.

¹ Barbara Wellbery is a partner in the Washington office of Morrison & Foerster LLP. She was previously Counsellor to the Under Secretary for Electronic Commerce in the U.S. Department of Commerce. While there, she was the chief architect and a principal negotiator of the safe harbor privacy accord between the U.S. and the European Union. The author would like to thank Rebecca Richards and Cynthia Rich for their valuable assistance on this article.
² Digital Economy 2000, Department of Commerce p. 53.
Not surprisingly, then, there is a growing demand for all kinds of information. The great promise of the Information Age is, however, also its greatest threat. The increased market for personal information, coupled with the ability to collect and compile it easily, has led to an enormous increase in the amount of information collected about individuals as they conduct commercial transactions and cruise the Net. Banks and credit card companies maintain information on financial records, payment histories, where people shop, and what they buy. Supermarkets and other retail stores track consumer purchases using checkout scanners. As individuals peruse various sites on the Internet, mouse clicks can be tracked, so-called “cookies.” Profiles can be compiled not only of what people buy, but also of what they read, their health concerns, and perhaps their political and sexual preferences as well. Thus, information technologies increase the risks to privacy exponentially.

Moreover, privacy issues are complicated by the fact that so much information is now used on a global basis. Multinational companies may ship all their personnel data to one location for record keeping, benefits, and payroll purposes; credit card companies may do the same with bankcard information for billing purposes. Credit and insurance markets increasingly operate on a global basis and may require the transfer of information about individuals across borders to evaluate their creditworthiness or insurance risks. And, the inherently global nature of the Internet further complicates the matter. Citizens of one country may easily visit web sites in other countries, transferring personal information across borders as they visit. But laws, which generally are limited by nations’ borders, may have little effect in a medium without borders.

Many nations share concerns about the impact of the expansion of electronic networks on information privacy. The United States and the European Union (EU) are both addressing these concerns, but in markedly different ways. This essay briefly examines the U.S. and EU approaches to privacy, their differences and similarities, the disruptions in global commerce the differences could cause, and one solution that has been developed for bridging those differences.

2. The European Approach to Privacy Protection

While the United States and EU generally agree on the underlying principle that individuals should have the opportunity to control the ways their personal information
is used, the U.S. and the EU employ very different means to achieve this goal. The EU’s approach to privacy grows out of Europe’s history and legal traditions. In Europe, protection of information privacy is viewed as a fundamental, human right. The emphasis given to information privacy in Europe arises at least in part from intrusions into information privacy that were at the root of certain World War II abuses. Europe also has a tradition of prospective, comprehensive lawmaking that seeks to guard against future harms, particularly where social issues are concerned.

The EU began examining the impact of technology on society over a fifteen years decade ago; the inquiry culminated in the adoption of a directive in July 1995 specifically addressing information privacy issues. The Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and On the Free Movement of Such Data (“Directive”) took effect in October 1998. Member states were required to bring into force laws, regulations, and administrative provisions to comply with the Directive by its effective date. Several have not yet done so. Presently, six of the fifteen Member States are being sued by the Commission for failure to implement measures within the deadline established by the Directive.3

A quick review of its basic terms makes clear that, consistent with European tradition, the Directive takes an overarching, highly regulatory and inclusive approach to privacy issues. It has two basic objectives: first, to protect individuals with respect to the “processing” of personal information (defined as information relating to an identified or identifiable natural person); and second, to ensure the free movement of personal information within the EU through the coordination of national laws (Article 1).

The scope of the Directive is extraordinarily broad. It applies to all processing of data, online and off line, manual as well as automatic, and all organizations holding personal data. It excludes from its reach only data used “in the course of purely personal or household activity” (Article 3). The Directive establishes strict guidelines for the processing of personal information. “Processing” includes any operations involving personal information, except perhaps its mere transmission (Article 2). For example, copying information or putting it in a file is viewed as “processing.”


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

**Legitimate Data Processing.** The Directive sets forth rules for “legitimate” data processing. Most basically, this requires obtaining the consent of the data subject before information is processed unless specific exemptions apply (Article 7). In addition, certain information must be provided to data subjects when their personal information is processed (Article 10), such as whether they have rights to see the data, to correct any information that is inaccurate, or to know who will receive the data (Article 12).

**Sensitive Data.** “Sensitive” data, such as that pertaining to racial or ethnic origins, political or religious beliefs, or health or sex life, may not be processed at all unless such processing comes within limited exceptions (Article 8).

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

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

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

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

3. **What Constitutes Adequacy Under the Directive?**

The aspect of the Directive that raises major questions for the United States and other non-EU countries is the question of what constitutes an “adequate level of (privacy) protection.” The Directive provides some guidance on how adequacy is to be determined. For example, the Directive states that the adequacy of the protection offered by the recipient country shall be assessed in the light of all the circumstances surrounding a data transfer. These include: (1) nature of the data; (2) purpose and duration of the proposed processing operation; (3) country of origin or the country of final destination; (4) rules of law in force in the destination country and (5) professional rules and security measures that apply within the recipient country (Article 25). And, while there seems to be general consensus that “adequacy” means
less than “equivalence,” the Directive leaves unspecified the substantive rules that in fact constitute “adequacy” as well as the procedural means for achieving it.

In June 1997, the European Commission’s Working party on the Protection of Individuals with Regard to the Processing of Personal Data (“Working Party”) released a discussion paper entitled “First Orientations on Transfers of Personal Data to Third Countries, Possible Ways Forward in Assessing Adequacy.” The Working Party paper identifies two criteria essential to a finding of adequacy, the core substantive rules and enforcement mechanisms. The substantive rules identified in the paper closely track the Directive’s requirements discussed above. They include: (1) information must be processed for a particular purpose and used only insofar as its use is not incompatible with the purpose of its collection; (2) information must be accurate and up to date and not excessive in relationship to the purposes for which it is collected; (3) individuals must be provided with information about the purpose of the collection; (4) organizational and technical measures must be taken to keep the data secure; (5) data subjects must be able to obtain copies of all data and have a right to rectification if they are inaccurate, as well as to oppose processing; and (6) transfers to third countries must be restricted unless they provide an adequate level of protection. The enforcement mechanisms must provide: (1) a good level of compliance; (2) support and help to individual data subjects; and (3) appropriate redress. The Working Party Paper also recognizes that legislation is not necessary for adequate privacy protection so long as these goals are accomplished through other means.

In issuing Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, a more recent report issued in July 1998, the Working Party elaborated further on the criteria a self-regulatory regime had to meet to be considered adequate. First, it reiterated that the substantive rules and enforcement mechanisms identified in its July 1997 report must be met. The self-regulatory regime must also be binding for all companies or institutions to which personal data are transferred and provide for adequate safeguards if data are passed on to non-members. In addition, the privacy regime must be transparent and have mechanisms that effectively ensure a good level of compliance. Individuals must be ensured certain rights, such as easy access to an impartial and independent body to hear complaints that can adjudicate breaches of the code and provide a remedy and
compensation, as appropriate. Finally, there must be a guarantee of appropriate redress in cases of non-compliance.

Neither paper issued by the Working Party, however, provides guidance on how and where an “adequate” privacy law or program in a third country might differ from the requirements of the Directive. Until the European Union actually made “adequacy” findings and there were specific examples to examine, exactly what would constitute “adequacy” under the Directive would remain unclear.

4. The U.S. Approach to Privacy Protection

Legal and historical traditions have evolved quite differently in the United States than in Europe, and the United States takes a different approach to privacy issues from the EU’s. The U.S. legal tradition, rooted in concerns about governmental excesses, has led to a preference for decentralized authority, a reluctance to regulate the private sector absent demonstrated need, and generally greater concern about government excess than about private sector excess. And, while the U.S. Constitution establishes certain privacy protections for individuals, such as the right to be free from warrantless searches, it does not explicitly protect information privacy, nor has any such right been inferred from the Constitution. In addition, a fundamental tenet of American democracy + the First Amendment to the U.S. Constitution + requires a balance between the privacy rights of individuals and the benefits that stem from the free flow of information within and across U.S. borders.

Accordingly, when the U.S. adopted a comprehensive privacy law -- the Privacy Act of 1974 -- it governed only the Federal Government’s use of citizens’ personal information. Other federal privacy protection statutes apply to specific government agencies or information, such as income tax and census data. Neither federal nor state governments, however, have adopted comprehensive information privacy protections affecting private sector data use. (Some state constitutions, such as those of California, Florida, and Hawaii, explicitly set forth a right to information privacy without specifying any rights relating directly to information privacy.)

In contrast, the information privacy laws that govern the private sector in the United States were adopted either because of specific instances of abuse, perceived market failure, or because particularly sensitive information and/or groups were
involved. There is also concern that information privacy issues differ so across different industry sectors that “a one size fits all” legislative approach would lack the necessary precision to avoid interfering with the benefits that flow from the free flow of information. For that reason, too, the U.S. has adopted limited sector-specific privacy legislation. As a result, a number of statutes cover the collection and use of personal information in specific contexts, such as children’s personal information, information collected by telephone and cable companies and credit bureaus, and financial, video rental and drivers’ license information. A brief review of three of these statutes makes clear that privacy statutes in the U.S take different approaches and impose different schemes for protecting privacy depending on the circumstances.

5. Fair Credit Reporting Act

Congress enacted the Fair Credit Reporting Act (FCRA) in 1970 to deal with widespread concerns about incorrect and widely disseminated consumer credit reports. The FCRA governs disclosure of consumer credit information by credit bureaus. It starts with the premise that widespread availability of correct credit information to parties with a real need for the information will benefit the U.S. economy. For this reason, it provides consumers with a limited right to consent to the use of their personal information.

The Act imposes strict regulations on who may use the credit information and on ensuring that the information is accurate. It thus limits the disclosure of credit information to businesses with a legitimate need for the information and provides certain rights to consumers when credit information is used to deny them an important benefit. To help ensure accuracy, the Act requires that consumers have access to information maintained about them and sets out fairly prescriptive rules governing how access must be provided. The Act also requires that the recipients of credit reports be identified, prohibits the reporting of obsolete information, and provides a correction process for inaccurate or incomplete information. And, if a consumer is denied credit for personal, family, or household purposes or is denied employment and the denial is based on information in a consumer report, the entity receiving the report is required to notify the consumer and identify the credit bureau that furnished the report in question. The FCRA allocates enforcement responsibilities among a number of federal agencies, primarily to the Federal Trade Commission.
6. Children’s On Line Privacy Protection Act

In October 1998, Congress passed the Children’s On line Privacy Protection Act (COPPA). The law applies to operators of commercial web sites and online services that collect or maintain information from web site or service visitors and users and prohibits the collection of information from children under the age of 13 without verifiable parental consent. It also provides for a safe harbor from privacy liability where companies adhere to a self-regulatory program approved by the Federal Trade Commission. The Federal Trade Commission, which was charged with enforcing developing regulations under the statute, issued implementing rules in April 2000.

These rules set out criteria for web site operators and on-line services that are targeted to children or have actual knowledge that the person from whom they seek information is a child. They require notice of what personally identifiable information is being collected, how it will be used, and whether it will be disclosed. Subject to certain exceptions, a web site must notify parents that it plans to collect information from their child and obtain parental consent before it is collected, used, or disclosed. Conditions for more than reasonably necessary information may not be placed on a child’s participation in on-line activities. In addition, parents must be allowed to review information collected from the child, to have it deleted, and to prohibit further collection. Finally, companies must implement procedures to protect the confidentiality, security and integrity of personal information collected from children.

7. Financial Modernization Act

More recently, in November 1999, the President signed into law the Financial Modernization Act. The Act’s primary purpose was to overhaul the U.S. laws governing the financial services industry, but the legislation also increased the level of financial privacy protections afforded to consumers. The law requires financial institutions to disclose clearly their privacy polices up front and annually, allowing consumers to make informed choices about privacy protection. Financial institutions must also inform consumers if they intend to share or sell consumers’ financial data either within the corporate family or to third parties. Consumers are entitled to choice if a financial institution plans to share information with unaffiliated third parties, subject to certain exceptions. Enforcement is allocated among Federal
functional regulators (for example, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the Federal Reserve Board), the Federal Trade Commission, and State insurance authorities. The legislation directs these agencies to prescribe regulations necessary for its implementation. Regulations have been finalized for all federal regulators. Businesses must be in full compliance by July 2001.

8. U.S. Self Regulatory Privacy Initiatives

Without broad, multi-sector information privacy laws, information privacy protection in the United States has in large part relied on voluntary adoption of self-regulatory codes of conduct by industry. These codes take as their point of departure the same Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the OECD as form the basis for the European Directive on Data Protection. As long ago as 1983, 183 U.S. companies endorsed those Guidelines. The U.S. Government has also repeatedly endorsed these guidelines, most recently in October 1998, when the Clinton Administration reiterated endorsement of those Guidelines as part of the Ministerial Declaration on the Protection of Privacy on Global Networks issued at the Ottawa Ministerial Conference.

Recent years have witnessed the growing importance of information privacy in the United States and increasing concern, from both consumers and Clinton Administration officials, about whether such privacy is sufficiently protected. This concern has led to enactment of additional sector-specific legislation. It has not, however, resulted in any significant movement toward a European type regulatory approach or law. Rather, the emphasis has been primarily on adoption and implementation of more effective self-regulatory regimes to protect privacy or on self-regulation with teeth.

Thus, when in 1997, the Clinton Administration released *A Framework for Global Electronic Commerce*, which examines the policy issues raised by the development of electronic commerce, it noted the growing concerns about information privacy and recognized that, unless they were addressed, electronic commerce would not develop to its full potential. The report specifically recognized the high value Americans place on privacy and recommended private sector efforts and technological solutions to protect privacy. The report also identified several
factors suggesting that adopting comprehensive legislation could harm the development of electronic commerce at this time.

The lack of national borders on the Internet has heightened interest in self-regulation and technological solutions to problems generally and to privacy concerns specifically. On the Internet, national laws are difficult if not impossible to enforce. In addition, since the Internet and electronic commerce are still rapidly evolving, any legislated approach at best is likely to be outdated as soon as it is adopted and at worst likely to stifle further development of these media. As a result the view taken in the report is that government should be a last, not a first, resort to fix problems. Accordingly, at the time the report was issued, the President directed the Secretary of Commerce and the Director of the Office of Management and Budget to encourage private industry and privacy advocacy groups to develop and adopt effective codes of conduct, industry-developed rules, and/or technological solutions to protect privacy on the Internet.

Subsequent annual reports on electronic commerce issued by the Clinton Administration confirmed the Administration’s preference for self-regulatory solutions to privacy protection. At the same time, the Clinton Administration continued to recognize that sector-specific privacy legislation may be appropriate in certain areas, such as where the information is considered highly sensitive, as is the case with children’s and financial information, as discussed above. The Clinton Administration also repeatedly cautioned that if industry did not produce adequate privacy policies, government action will be needed to safeguard legitimate privacy interests.

Since the issuance of the Clinton Administration’s landmark electronic commerce report in 1997, industry has undertaken concerted efforts to create effective privacy protection via self-regulation. More than 80 of the largest companies doing business on the Internet and 23 business organizations that represent thousands of other companies formed the On-line Privacy Alliance (OPA) to promote privacy online. The Online Privacy Alliance developed Guidelines for Effective Privacy Policies, which outline protections for individually identifiable information in an on-line or electronic commerce environment. OPA has also produced guidelines for effective enforcement of these policies.
Independent third party enforcement organizations such as the BBBOnLine, TRUSTe, and CPA WebTrust have also been formed to provide independent third party enforcement regimes that promote compliance with information practice codes. For example, the Council of Better Business Bureaus, a well-regarded, non-profit organization that helps to resolve consumer complaints, established BBBOn-Line as a privacy program for online businesses. Businesses joining the program may display a seal or trust mark to notify consumers that their web sites follow fair information practices but only after they adopt privacy policies that comport with the program’s fair information practice principles and complete an assessment indicating that they have implemented those policies. Members must also submit to monitoring and review by BBBOnLine and agree to participate in a consumer complaint resolution system. The other enforcement programs include similar requirements and also include the display of a seal or trust mark to notify consumers. More than 1950 sites carry a privacy seal from a trusted third party and more than additional 1200 sites have applied for a seal from third-party enforcement services.

In what is perhaps a uniquely American approach to self-regulation, enforcement of self-regulatory programs is backed up by Federal Trade Commission (and other federal and state agency) enforcement. Section 5 of the Federal Trade Commission Act prohibits “unfair and deceptive acts or practices” in or affecting commerce. Deceptive practices have been defined to include representations, omission, or practices that are likely to mislead reasonable consumers in a material fashion. The FTC has repeatedly used its equitable powers under Section 5 to enforce the provisions of privacy (and other self regulatory) policies against companies failing to comply with the policies they have adopted even where those policies have been adopted voluntarily. The operational effect of these unfair and deceptive statutes is to make adoption by a company of a privacy policy akin to adoption of a privacy law for that particular company.

The FTC Act provides the FTC with authority to seek injunctive relief against future violations of the statute as well as to provide redress for injured consumers. And, the FTC can obtain substantial penalties where its orders are violated. The FTC’s (and other federal and state agencies’) unfair and deceptive authority and willingness to use this authority to enforce self-regulatory policies helps to ensure the effectiveness of self-regulation in the U.S. All fifty states plus the District of
Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws similar to the Federal Trade Commission Act to prevent unfair or deceptive acts. These are enforced by their Attorneys General, adding additional resources to government enforcement of self-regulation.

Evidence now exists that shows the United States’ decentralized, self-regulatory approach to privacy issues can be an effective means of ensuring that individuals’ personal information is adequately protected in a globally networked environment. A 1999 Federal Trade Commission survey involving a random sample of web sites found that the number of privacy policies had risen from 14% in 1998 to 88% and that 100% of the most popular group of web sites now have privacy policies. While only 8% of the random sample had privacy seals from one of the independent third party enforcement groups, 45% of the most popular group did. Other surveys also show that privacy self-regulation is working and that businesses are taking effective steps to establish and post privacy policies. For example, a Jupiter Communications study determined that 70 percent of web sites in the United States that collect information post a privacy policy linked to their home pages.

At the same time, there have been increasing calls for privacy legislation in the U.S. In May, 2000, the Federal Trade Commission called for legislation to protect privacy online based upon its most recent report, which identified problems of "free riders" and poor quality privacy policies. The report stated that the number of web sites disclosing information practices had increased, but that the quality of these information practices fell short. In addition, the report noted that while the creation of the self-regulatory enforcement programs has been a positive development, the number of participants to date in these groups has been relatively small (8% of a random sampling and 45% of the most popular sites). In part because these enforcement programs have not been widely implemented, the FTC has concluded that such efforts alone are not sufficient for ensuring adequate protection of consumer privacy online.

Several members of Congress have also introduced privacy legislation in Congress to protect privacy, particularly in the areas of online privacy, electronic surveillance, and medical and financial record-keeping. While many of these bills are given little chance of passage, at a minimum they indicate impatience with the pace of adoption and dissatisfaction with the quality of private sector codes of conduct. For
example, in the first few months of this year alone, there have been at least 18 bills proposing privacy legislation. These have ranged from the basic requirements that disclosure must be provided with an opportunity to prohibit further interaction to more stringent bills requiring affirmative consent in advance to collect and disclose personally identifiable information. Even some industry officials are, for the first time, urging Congress to pass limited privacy laws. They are concerned that the lack of federal standards will lead to a confusing patchwork of state regulations.

For its part, the Clinton Administration saw substantial progress being made by the private sector, although it too believed more needed to be done and more quickly. The new Administration, however, has yet to articulate its policies in this area and whether it will also encourage adoption by industry of effective privacy policies and technological solutions.

Although the privacy situation in the U.S. is evolving, this much is clear. While the U.S. is committed to ensuring personal privacy, it does through a variety of means that reflect its deeply rooted tradition of enhancing the free flow of information and avoiding unnecessary government intervention in private affairs. In the first instance, the U.S relies on private sector self-regulatory efforts backed up by government enforcement to ensure that companies implement their privacy policies. The government gets involved only where it determines that the privacy rights of individuals are not otherwise being sufficiently protected. The U.S. approach to privacy relies on an amalgam of laws, codes of conduct, and technology to provide effective privacy protection.

Given U.S legal traditions and history and the advantages of a self-regulatory approach to privacy in an information economy, the United States is unlikely at this time to abandon its self-regulatory approach to privacy issues. And even if it were to adopt privacy legislation in new and different situations, it is highly unlikely that the United States would adopt the type of overarching, comprehensive, highly regulatory and centralized approach to privacy that the European Union has adopted.

9. SAFE HARBOR

Neither the EU or the U.S. appears likely to change significantly its approach to privacy protection. Given these longstanding differences, many U.S. organizations
were concerned about the impact of the “adequacy” standard on personal data transfers from the European Community to the United States. Many feared an across the board interruption in data flows. Such across the board interruptions could affect as much as $120 billion in trade each year and interfere with multinational companies’ ability to pay and manage their employees and with the routine activities carried out by investment bankers and accountants and by pharmaceutical and travel companies. Others dismissed fears of a complete interruption in data flows as unlikely, pointing out that it would be potentially devastating for both economies.

The more likely situation -- of limited data flow interruptions involving one industry sector or perhaps one company -- posed similar dangers, however, since it was feared they could easily evolve into a trade war, depending on U.S. reactions and European counter reactions. And, just the threat of action by European authorities left U.S. companies with a great deal of uncertainty. Alternative, ad hoc approaches available to satisfy the Directives “adequacy” standard threatened to be expensive and time consuming and thus suitable for larger companies only.

Against the backdrop of these different privacy approaches and the serious consequences that could flow from them, the United States and the EU took up the difficult challenge of bridging the differences in their respective approaches to privacy. Toward that end, in March, 1998 the U.S. Department of Commerce initiated a high-level informal dialogue with the European Commission Directorate for Internal Markets to ensure the continued free flow of data. From the start, both sides recognized that any interruptions in transborder data transfers could have a serious impact on commerce between the EU and the US, and that they thus needed to begin with an acceptance of their differences and develop ways to bridge those differences. At the outset, therefore, the two sides agreed on twin goals -- of maintaining data flows between the U.S. and EU while maintaining high standards of privacy protection and worked to identify common ground on which to build a solution. The dialogue revealed that there is much common ground between the two sides on what constitutes effective privacy protection. Both the U.S. and the European approaches, despite their differences, are based on the 1981 OECD Privacy Guidelines.

This dialogue led in late 1998 to a proposal of a “safe harbor” for U.S. companies that adhere to a certain framework, the so-called safe harbor framework. The safe harbor framework encompasses the safe harbor principles and frequently
asked questions (FAQs). U.S. companies adhering to the framework will be judged adequate and data flows to them from Europe will continue. The safe harbor principles more closely reflect the U.S. approach to privacy, but at the same time would meet the European Union Privacy Directive’s requirements. The FAQs were developed to provide further guidance to U.S. companies and to elaborate on how various issues, such as enforcement, will work. Both the principles and FAQs were developed in close consultation with the European Commission and the U.S. public and both are considered integral to an “adequacy” determination. Drafts of documents were posted for U.S. public comment fours times during the two-year negotiation, and numerous meetings were held by U.S. negotiators with consumer advocacy and industry groups to obtain their views on the draft documents.

Importantly, the dialogue also led to a standstill between the U.S. and the EU in late 1998. The EU made a political commitment to the U.S. not to interrupt data flows while the dialogue proceeded in good faith.

On March 14, 2000, the Department of Commerce and the European Commission announced that they had reached a tentative conclusion to the safe harbor dialogue. At the same time, the two sides agreed to continue their discussions with respect to the financial services sector, given the recent passage of the Financial Modernization Act and the fact that the regulations had not yet been issued. On May 31, the EU Member States voted unanimously to approve the safe harbor arrangement.

The safe harbor will provide a number of important benefits to U.S. firms. Most importantly, it will provide predictability and continuity for U.S. companies that receive personal information from Europe. All 15 Member States will be bound by the European Commission’s finding of adequacy. The safe harbor also streamlines the bureaucratic burdens imposed by the Directive, by creating one privacy regime applicable to U.S. companies, rather than 15. It also eliminates the need for prior approval to begin data transfers to the U.S. or makes such approval automatic. The safe harbor offers a simpler and less expensive means of complying with the adequacy requirements of the Directive, which should benefit all U.S. companies and particularly small and medium enterprises.

An organization’s decision to enter the safe harbor is entirely voluntary. An organization that decides to participate in the safe harbor, however, must publicly
declare in its published privacy policy statement that it adheres to the safe harbor and then it must do so. To continue to be assured of safe harbor benefits, an organization needs to self certify annually to the Department of Commerce in writing that it adheres to the safe harbor’s requirements. The Department of Commerce will maintain a list of all organizations that file self-certification letters and make both the list and the self-certification letters publicly available.

10. Safe Harbor Requirements

Organizations must comply with seven privacy principles and the FAQs to be compliant with the safe harbor. The principles require the following:

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

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

**Onward Transfer (Transfers to Third Parties).** Where an organization wishes to transfer information to a third party that is acting as an agent, 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.

---

4 The principles, frequently asked questions and answers, as well as other safe harbor documents can be located at www.export.gov/safeharbor.

5 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.
Access. Generally, individuals must be given access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate. Exceptions to this general rule are permitted where the burden or expense of providing access would be disproportionate (unreasonable) 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. Organizations must have readily available and affordable independent recourse mechanisms that allow each individual’s complaints to be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide. In addition, the organization must establish procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented. Finally, the organization must remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization.

The FAQs provide further guidance that clarifies and supplements the safe harbor principles on issues such as access, publicly available information, and public record information as well as sector-specific guidance for information processing by medical, pharmaceutical, travel, and accounting firms. They also address how human resources information will be handled under the safe harbor.

11. Safe Harbor Enforcement

Perhaps the most difficult difference to bridge in the safe harbor dialogue was the issue of enforcement. While the EU’s Working Group had already determined in the abstract that self regulation was a valid means to “adequacy,” accepting the adequacy of a particular self-regulatory enforcement regime proved far more difficult. Adding to this difficulty, was the complexity of the multi-layered approach to privacy
enforcement in the U.S., which relies on self-regulation, backed up by FTC enforcement, sector specific laws, and recourse to lawsuits.

Ultimately, an understanding was reached on an enforcement arrangement. In general, enforcement of the safe harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. The safe harbor provides for at least three different ways to satisfy the enforcement principle. An organization can join a self-regulatory privacy program that adheres to the safe harbor’s requirements. It can also develop its own self-regulatory privacy policy that conforms to the safe harbor. And, an organization can meet the safe harbor enforcement principle’s requirements if it is subject to a statutory, regulatory, administrative or other body of law (or rules) that effectively protects personal privacy.

As part of their safe harbor obligations, organizations are required to make available 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 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.

As noted above, the dispute resolution, verification, and remedy requirements can be satisfied in different ways. For example, an organization could comply with a private sector developed privacy seal program that incorporates and satisfies the safe harbor principles. If the seal program, however, only provides for dispute resolution and remedies but not verification, then the organization would have to satisfy the verification requirement in an alternative way. Organization can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities or by committing to cooperate with data protection authorities located in Europe.

Where an organization relies on self-regulation to ensure privacy protection under the safe harbor, there must be a U.S. agency (state or federal) with jurisdiction over the organization that will enforce the safe harbor policies against that organization. The agency must also be willing to take action under federal or state
law prohibiting unfair and deceptive acts where the company fails to comply with the safe harbor or the organization is not eligible to join the safe harbor. Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or the states will provide overarching government enforcement of the safe harbor principles. An annex to the safe harbor principles will contain a list of U.S. enforcement agencies recognized by the European Commission. Third party self regulatory programs, (such as BBB On-line, TRUSTe, and WEBTrust) are also subject to enforcement under these unfair and deceptive practice statutes in many if not most instances if they claim to be enforcing the safe harbor framework for their safe harbor members but do not.

12. Failure to Comply with Safe Harbor Requirements

If an organization persistently fails to comply with the safe harbor requirements, it will no longer be entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). The Department of Commerce will indicate on the public list it maintains of organizations self certifying adherence to the safe harbor requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits. An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

13. Conclusion

This safe harbor arrangement has been called a major accomplishment for both the U.S. and the EU. It comes at a time when trade disagreements rather than agreements between the U.S. and Europe dominate the news. The framework has also been labeled a landmark accord for electronic commerce. It bridges the different approaches of the US and the EU to privacy protection in a way that protects EU citizens’ privacy when it is transferred the U.S., maintains data flows, and creates the
necessary environment for electronic commerce. And it will provide predictability for U.S. companies. At the same time, the arrangement demonstrates EU recognition that a carefully constructed and well-implemented system of self-regulation, as advocated by the Clinton Administration, can protect privacy. It is a creative and innovative vehicle, perhaps the first international framework to rely on the private sector for its implementation. It thus can serve as a model in other contexts as we seek to ensure the development of seamless global environment for electronic transactions.

The challenge in providing privacy protection in the Information Economy is to balance appropriately the free flow of information against the individual's right to privacy so we do not jeopardize the benefits these new information technologies promise or trench on the First Amendment. Whether the safe harbor will provide that balance remains to be seen. Sufficient numbers of companies will have to join the safe harbor and consumers will have to feel comfortable with how their personal information is used and their ability to control its use, if the safe harbor is ultimately to be judged a success.
Bridging the Difference:
The Safe Harbor and Information Privacy in The United States and The European Union