ONLINE PRIVACY, INTERNATIONAL DATA TRANSFERS AND EUROPEAN LAW

by

Carter H. Manny*

I. INTRODUCTION

Privacy for personal information[1] is one of the greatest concerns of people using the Internet.[2] E-mail messages might be read by someone other than the intended recipient. Information requested by a web site to enable a consumer to purchase goods or services can be used for purposes unrelated to the transaction. Internet service providers, web site operators and online advertising networks have the technical capacity to track the behavior of individual users of the web and assemble consumer profiles.[3]

If personal information is being abused, several responses are possible. One is a market approach. Consumers can try to protect themselves by restricting, or even eliminating, their use of online services. They can also avoid sites and businesses that provide less protection for privacy. In this way, consumers will punish privacy abusers and drive them from the market. Another approach is for consumers to use privacy enhancing technology. This includes encryption for e-mail, "anonymizing" technology to prevent tracking of web site visits and secure payment systems rather than traditional credit cards. A third approach is for online businesses to regulate themselves through codes of conduct promulgated and enforced by a certification program like TRUSTe[4] or BBBOnline.[5] A fourth approach is for government to regulate either directly through legislation and regulation enforced by one or more administrative agencies, or indirectly through legislation or case law authorizing private rights of action in the court system.

All four approaches exist to some extent in the United States. Market forces, privacy enhancing technology, self regulation and a patchwork of sector specific privacy laws all have some effect on online activities. There is, however, no comprehensive legislation protecting privacy online. In Europe, the situation is different. Privacy is considered to be a fundamental human right.[6] Most countries have comprehensive privacy legislation known as data protection laws administered through national or provincial data protection agencies. The fifteen member states of the European Union have harmonized their general data protection laws through a directive[7] adopted in 1995 which took effect in 1998. Although the Data Protection Directive promotes the free flow of information within the EU, it protects the privacy rights of Europeans by allowing government officials to block the flow of personal data to any country which lacks adequate privacy protection, or if other privacy safeguards are not in place.[8] For the US, there is a self-regulatory arrangement known as the Safe Harbor,[9] through which organizations qualify for eligibility to receive personal data from Europe by promising to follow certain privacy safeguards which are considered to provide adequate privacy protection. Relatively few companies have joined,[10] and financial services, insurance and telecommunications companies are not eligible to become Safe Harbor participants.[11] For companies outside the Safe Harbor, European law requires that the transfer be either pursuant to a model privacy protection contract drafted by the European Commission,[12] pursuant to prior approval granted by the national government of the exporting country[13] or pursuant to exceptions[14] contained within the Data Protection Directive.

There are questions about the applicability of European legislation to online activities.[15] Because the Data Protection Directive was drafted while the Internet was in its infancy, there are questions about its applicability to online transactions. Although its terminology is well-suited to the collection, processing and storage of personal data of customers or employees on a mainframe computer in Europe, many of its provisions are sufficiently general to include online transfers of data through the Internet.

Other European legislation can affect online privacy. A directive protecting privacy in the telecommunications industry[16] supplements the Data Protection Directive and is in the process of being revised[17] to make clear that it applies to Internet service providers as well as telephone companies. Both the existing and proposed versions of this directive apply to providers of electronic communications services in the European Union, and would affect US companies and their subsidiaries in this sector operating in Europe. Because the focus of this study is European law affecting the transfer of personal data to US organizations not physically present in Europe, the existing and proposed directives on privacy in telecommunications and electronic communications are outside the scope of this paper. Other European Union legislation affects online transactions but leaves privacy regulation to the Data Protection Directive, either explicitly, as in the case of a directive on electronic commerce,[18] or implicitly, in the case of a directive on distance contracts,[19] or both, in the case of the a directive on electronic signatures.[20]

Accordingly, the main focus of this paper is on how the Data Protection Directive applies to online transfers of

*Associate Professor of Business Law, University of Southern Maine, Portland, Maine

personal data from Europe to US organizations which are not physically present there. Some consideration is given to provisions of selected European national data protection laws, particularly when they depart from the language of the Directive. There is a discussion of how US businesses can comply with European requirements under the Directive's transborder provisions including the Safe Harbor, a draft model privacy contract issued by the European Commission, prior approval of the government of the exporting country or one of the Directive's exceptions. There is also a discussion of how Europeans might be able to deal with illegal transfers of personal data when the US organization has made no attempt to comply with the Directive's transborder provisions.

II. APPLICABILITY OF EUROPEAN LAW TO ONLINE TRANSFERS OF PERSONAL DATA

How much of the data connected with online activities qualifies as "personal data" under the Data Protection Directive? The Directive's expansive definition reads:

> "Personal data" shall mean 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 physiological, mental, economic, cultural or social identity;[21]

This clearly includes most information voluntarily supplied by the individual when ordering goods online. It could also include things like an e-mail address or telephone number, even when the individual is not supplying a name, because these can be linked to the person's name through a directory. In some instances, the definition could include information obtained without the person's knowledge when he or she visits a web site. One example of how this could happen involves "cookies" or files which can be put on the hard drive of a visitor's computer when he or she visits a web site. Cookies can be placed by the operator web site, or by an online advertising company which has a contract with the web site, to track the person's web activities and assemble a profile, ostensibly for marketing or customer service purposes. Depending upon the circumstances, this data could be linked to the person by name and thus qualify as personal data.[22] In some instances, the tracking technology enables the web site operator or the network advertising company to know the visitor's e-mail address.[23] Although the information could be used to identify good customers, it could also be used to identify less desirable ones and provide the basis for excluding them from some of the free services provided by the web site.[24]

Similar conclusions can be drawn from the definitions of "personal data" in the national laws which implement the Data Protection Directive. Several of the laws use language similar to the Data Protection Directive's definition and include provisions covering indirect identification by means of an identification number.[25] Other national laws use more general language to express the concept that data is personal if the person is "identifiable"[26] or "can be identified."[27] The statutes support the idea that if it is possible that an identifying marker like a cookie can be linked to a living natural person, tracking data obtained by reading the cookie during web surfing is "personal data" and is subject to European data protection law.

Do the Data Protection Directive and the national implementing laws apply to online collection of personal data outside the European Union arising out of online activities of someone who is within the EU? There is a strong argument that the laws apply to all online collection of data regardless of whether the collector is inside or outside the European Union. Using the Data Protection Directive's terminology, the party collecting the data is a "controller"[28] and the acts of collecting, using and storing data are within the definition of "processing."[29] In a situation where the controller is outside the European Union, and "makes use of equipment, automated or otherwise, situated on the territory of [a] Member State . . ." the national data protection law of that Member State shall be applied.[30] The argument is that the collection of the data is being made through the individual's computer within the EU and that the party collecting the data is "making use of" equipment in an EU Member State. Moreover, a controller outside the EU who uses equipment for processing European personal data outside the EU is required to designate a representative in the Member State where the equipment is located.[31] This would mean that any US network advertising company which collects personal data from visits by web surfers located in Europe would need to appoint an agent in each EU member country. Although a web surfer's computer arguably fits within the "makes use of equipment" language, electronic transmission equipment alone would not because of an exception for equipment "used only for purposes of transit through the territory of the Community."[32] Thus the national data protection law of Belgium would not apply to collection of personal data in the US of a web surfer in Poland just because the data went through an Internet routing device located in Brussels.

Many of the national laws follow the Data Protection Directive closely with respect to effect of making use of equipment within the country for processing and the need to appoint a representative.[33] There are some variations, however. Italian law states that it applies to the processing of personal data carried out by any person whomsoever on Italian territory.[34] Although the statutory language is less specific than the language in the Data Protection Directive, the same argument could be made: the "processing" is the collection of personal data on Italian territory by means of the web surfer's computer. Austrian law, however, provides little support for this type of analysis. The Austrian statute has a territorial jurisdiction provision which limits its application to processing of data in Austria and other EU Member States.[35]

Much of the data captured by US web site operators and network advertising companies appears to qualify as personal data which ostensibly is subject to the protection of the Data Protection Directive and implementing national data protection laws. The next section explores the ways that US organizations collecting such data can comply with those laws.

III. INTERNATIONAL TRANSFERS IN COMPLIANCE WITH EUROPEAN LAW

Under the Data Protection Directive there are four categories of lawful transfers of personal data to non-EU destinations. The first category is for countries found by the European Commission to have "adequate" protection for personal data.[36] Adequacy determinations have been made for Hungary[37] and Switzerland[38] based upon their comprehensive data protection laws administered by data protection authorities. As mentioned above a narrower adequacy determination has been made for those US organizations which join a voluntary arrangement known as the Safe Harbor[39] and make public commitments to protect the personal data of Europeans. The Safe Harbor is essentially a self-regulatory program backed up by the threat of enforcement by the US Federal Trade Commission and Department of Transportation when self-regulatory mechanisms fail. US organizations which are not subject to the jurisdictions of these agencies, including financial service and telecommunications companies, are not eligible to join.[40] As of May 21, 2001, there were 43 participants in the Safe Harbor, 40 of whom received personal data online.[41] The second category for lawful transfers is the use of a model privacy protection contract, approved by the European Commission, running between the European exporter of the personal data and the US importer.[42] The third category is a transfer which has the prior approval of the government of the exporting country.[43] The fourth category includes exceptions which permit personal data to be exported without any government approvals or privacy commitments.[44] The following discussion examines the applicability of these categories to online transfers.

A. Transfers Pursuant to the Safe Harbor

A US organization wishing to receive personal data online from Europe can join the Safe Harbor by sending a certification letter annually to the US Department of Commerce stating that it is in compliance with the Safe Harbor Privacy Principles and accompanying Frequently Asked Questions. The Safe Harbor incorporates many of the privacy protection principles found in the Data Protection Directive, but often in a weaker form. The principles fall into the general categories of notice to the data subject, an opportunity to choose how the data will be used, a right of access to the data, and provisions protecting the integrity and security of the data.

1. Notice to Data Subjects

The organization must inform the data subject of the purposes for which the organization is collecting and using the information, how to contact the organization with any inquiries and complaints, the types of third parties to whom it will be disclosing the information, and the choices and means the organization offers individuals for limiting the use and disclosure of the information.[45] In the online context, the notice could appear on the organization's web site, but should be prominently displayed and should also be linked to any place on the site where the site visitor is asked to provide personal information. By its own terms, the Safe Harbor only applies to personal data coming from Europe, so it is permissible for the web site operator to have different privacy policies based upon the location of the web visitor. Unlike the Data Protection Directive, the Safe Harbor has no limits on data collection and relies completely on the ability of informed data subjects to decide whether to provide data, or to block or authorize its use. As in the Data Protection Directive, the general rule is that notice must be given by the organization when an individual is first asked to provide information,[46] although the Safe Harbor has an exception allowing the notice to be given "as soon thereafter as is practicable,"[47] which could harm the privacy interests of the individual in some instances.

The Safe Harbor's notice provisions are well-suited to web sites which request and receive personal information from visitors or which plant and read cookies, but the notice provisions do not clearly address invisible tracking by third party network advertising companies. If a network advertising company decides to join the Safe Harbor, presumably it would need to provide onscreen access to a privacy notice prior to placing a cookie on the European visitor's computer or prior to recording that visitor's tracking data. Given invisible tracking and profiling used in connection with network advertising on web sites, it seems unlikely that any US company in this industry would be willing to join the Safe Harbor.

2. Choice by Data Subjects

The Safe Harbor gives data subjects the right to limit or "opt out" of certain activities and requires that organizations provide clear and conspicuous, readily available, and affordable mechanisms for exercising the choices.[48] An individual has the right to limit disclosure of personal information to third parties, but only if the disclosure is for a purpose other than the one for which the data was collected, or for a purpose which he or she has subsequently authorized.[49] This provides less

protection than the Data Protection Directive which grants the right to object to the transfer regardless of the use to which the data will be put.[50] An individual also has the right to prevent the use of the information for a purpose which is incompatible with the purpose for which it was originally collected, or for a purpose which he or she has subsequently authorized.[51] This "incompatible" purpose limitation is vague and is likely to be less protective than the Data Protection Directive's approach of specifying the types of processing permitted without the data subject's consent.[52]

Different rules apply to sensitive personal information about health, race, ethnicity, religion, trade union membership or sex life. Disclosure of such information to a third party, or use of such information for a purpose other than the purpose for which it was collected or subsequently authorized, is prohibited unless the data subject "opts in" by giving affirmative or explicit consent.[53] This an instance where the Safe Harbor provides greater protection for privacy because it lacks exceptions contained in the Data Protection Directive.[54]

With respect to online transactions, the Safe Harbor's provisions on choice seem to be suited to situations where users are consciously providing information, or are being tracked by the web site itself, but are not well-suited to invisible tracking by network advertising companies. Any network advertising company joining the Safe Harbor would need to provide opt out choices presumably onscreen at the time of placing a cookie or recording tracking data, neither of which a member of this industry seems likely to be willing to do.

3. Access by Data Subjects

Although there is a general right of access including the right to correct, amend or delete inaccurate information,[55] the Safe Harbor contains many limitations which do not appear in the Data Protection Directive. These include possible access fees, limits on the number of requests by any one person and the right to redact confidential commercial information from the data disclosed.[56] Generally, there is no requirement to provide access to information derived from public records.[57] There is also language limiting the right of access when the burden of providing access is disproportionate to the risk to the individual's privacy, or where the rights of other persons would be violated.[58] Many examples of the exceptions are given.[59] Because of the balancing standard and the numerous exceptions, there is the potential that European data subjects in many instances will have inadequate access to the personal data.[60] Moreover, the lack of a requirement that access be provided online, allows Safe Harbor participants to insist that access requests be by slower and less convenient methods of communication, like postal mail.

4. Security and Integrity of Data

The security provisions in the Safe Harbor are similar to those in the Data Protection Directive and require that reasonable precautions be made to protect the data from loss, misuse and unauthorized access disclosure, alteration and destruction.[61] The data integrity provisions require that the data be relevant for the purposes for which it is to be used, and that it may not be processed in a way that is incompatible with the purposes for which it was collected or subsequently authorized by the data subject.[62] In addition, the organization should take reasonable steps to ensure that data is accurate, complete, current and reliable for its intended use.[63]

5. Administration and Enforcement of the Safe Harbor

The Safe Harbor contains procedures designed to ensure that its members are following its rules. These serve the same function as procedures which European data protection authorities administer under European national laws. The annual self-certification letter with the Department of Commerce lists information about the organization, describes its activities relating to personal information received from Europe, states its privacy policy,[64] and includes the name of any privacy program of which the organization is a member (for example, TRUSTe or BBBOnline.)[65] Any misrepresentations in the self-certification letter may be actionable by the Federal Trade Commission, and also may be actionable under the False Statements Act.[66]

Compliance with the Safe Harbor is then subject to verification, either by self assessment or by outside compliance review.[67] Both methods require the preparation of an annual statement which is held internally by the organization, and which must be made available to an individual on request and during an investigation regarding alleged non-compliance.[68] Self assessment should include confirmation that the organization's privacy policy is accurate, comprehensive, prominently displayed, completely implemented, accessible and in compliance with the Safe Harbor.[69] It should also confirm the existence of procedures for periodically conducting compliance reviews, procedures for training employees and procedures for disciplining them for failing to follow privacy policies.[70] Verification by outside compliance review needs to confirm that the privacy policy is in effect, that it conforms to the Safe Harbor, and that individuals are informed of the procedures they can use to pursue complaints.[71] Outside compliance review can include auditing, random reviews, use of decoys or use of technology.[72] Because the methods of verification are subject to scrutiny only when there are external inquiries by individuals

and compliance investigations, the system seems unlikely to ensure that verification procedures will be followed by all participants every year.

The Safe Harbor allows a member to select one of four alternative enforcement mechanisms. The first is a private sector privacy program, like TRUSTe and BBBOnline,[73] that incorporates the Safe Harbor's principles into its rules and has effective enforcement mechanisms.[74] The second is a legal or regulatory supervisory authority, for example a consumer protection division within a federal or state administrative agency, that provides for handling of individual complaints and dispute resolution in the US.[75] The third is a commitment by an organization to cooperate with data protection authorities located in the European Union.[76] The fourth is a general category that includes other private sector mechanisms which meet the enforcement requirements of the Safe Harbor.[77]

Organizations electing to cooperate with European data protection authorities, can have complaints investigated and resolved by an informal European panel of such authorities.[78] Participating organizations must agree to comply with advice given by the panel, including payment of compensation to data subjects.[79] If an organization fails to comply, the panel can either submit the matter to a US agency with enforcement power, or can notify the Commerce Department that the organization has breached its commitment to cooperate,[80] and face liability for a deceptive practice under section 5 of the Federal Trade Commission Act, or other similar statute.[81]

As of May 21, 2001, by far the most popular dispute resolution mechanism selected by Safe Harbor registrants was cooperation with the European data protection authorities. It was chosen by 59% as the primary method of dispute resolution, and by another 19% as a supplement to other mechanisms. This means that a total of 78% of US organizations joining the Safe Harbor committed to work with the data protection authorities. Some of these organizations are required by the Safe Harbor to make this commitment because they receive human resources data from Europe. But even when these organizations are excluded from the tally, 49% of the rest have chosen to cooperate with the data protection authorities.[82]

It is should be encouraging to the Europeans that so many of the Safe Harbor participants have selected the dispute resolution mechanism which best satisfies the requirement that the mechanism be readily available to European data subjects. The data protection authorities have the necessary expertise with privacy issues and the language skills to handle transatlantic disputes effectively. The Europeans should also appreciate that US organizations are willing to make this commitment even though under the Safe Harbor the European data protection authorities are not bound to apply US law when interpreting the Safe Harbor agreement.[83]

B. Transfers Pursuant to a Model Contract

Personal data may also be lawfully transferred out of the European Union under standard contractual clauses, sometimes also called a model contract, approved by the Commission under the Directive.[84] A model contract runs between the data exporter in Europe and the data importer, and would provide the data subject with legal rights as a third party beneficiary. A draft model contract was issued by the Commission in September, 2000, and a revised version was approved by a committee of representatives of the EU's member states, known as the Article 31 Committee, on March 27, 2001.[85] It is possible that the draft will be in final form during the summer and will be available for use in September, 2001.[86] It is also possible that the Commission will approve other forms of model contracts in the future.

In situations in which a US organization is receiving personal data directly from a person in Europe who is visiting a US web site, use of the model contract alternative would make little sense because the "exporter" of the data is the data subject himself or herself. It would be incredibly cumbersome for a contract to be signed with every web site visitor prior to the time he or she provides personal information. Moreover, the form of the Draft Model Contract, especially the third party beneficiary and joint and several liability provisions, assumes that the "exporter" will not also be the data subject. It is even more unrealistic for a network advertising company to enter such contracts prior to collecting web surfing data. Such contracts do make sense, however, in traditional mainframe data processing situations where there is a transfer of personal data between business databases. Under the Draft Model Contract, the medium used for the transfer is not significant and it seems to make little difference whether the data is transferred online or offline. The obligations of the parties are the same regardless of how the data is transferred. Because the March 27 draft of the model contract is not relevant to consumer-to-business transfers, it will be considered only in the business-to-business context.

The Draft Model Contract includes lists of obligations of the data exporter and importer, a third party beneficiary enforcement provision, an election of the applicable data protection principles governing the transfer, a joint and several liability clause, a choice of law clause normally selecting the law of the exporter' country,[87] and choice of forum provisions which include alternative dispute resolution mechanisms as well as judicial enforcement. Once signed, the contract may become available to the public in some instances because it is to be deposited with the data protection authority if requested by that institution or required by the national law of the exporter's country.[88]

The data exporter warrants that its processing and transfer of the data is in compliance with the exporting country's national law and that data subjects have received prior notification if any sensitive data (i.e. data relating to race, ethnicity, political opinions, health, sex life, trade union membership or religious or philosophical beliefs) could be transferred outside of

the EU.[89] The exporter also warrants that it will respond within a reasonable time to questions about the transfer and will provide a copy of the contract to any data subject on request.[90]

The most important features of the Draft Model Contract are the data importer's obligations. The importer must elect to comply either with data protection principles set forth in the national law of the data exporter's country or with data protection principles set forth in a Commission adequacy determination for a sector, which excludes the importer, in the importer's country.[91] Although written in language which could apply to any country, the second election is intended to refer to the Safe Harbor and to enable US businesses in the financial services, insurance and telecommunications sectors, which are not currently eligible to join the Safe Harbor, to qualify for data transfers by making contractual commitments to follow the Safe Harbor's privacy principles. This enables them to commit to the Safe Harbor's privacy provisions which tend to be milder than the exporting country's national law, even though the businesses are not eligible to follow the Safe Harbor's other provisions. Other obligations include a representation that the importer will respond within a reasonable time to questions about the transfer, that it will provide a copy of the contract to any data subject on request[92] and that it will allow an audit of its data processing facilities.[93]

With respect to remedies, data subjects harmed by a breach can recover compensation for which the importer and exporter are jointly and severable liable.[94] A party has a contractual right to seek indemnification if it is held liable for the other party's act.[95] In the event of a dispute, the data subject has the right to take the matter to mediation, to refer the dispute to a court in the exporter's country,[96] and both parties can agree to submit the matter to arbitration, but only in a country which has ratified the New York Convention on enforcement of arbitral awards.[97]

The Draft Model Contract may be attractive to some US businesses as a way to avoid the numerous procedural requirements of the Safe Harbor, especially in situations where the importer is receiving personal data from a limited number of exporters and thus would be involved with a small number of contracts. But if many exporters are supplying data, the Safe Harbor provides a way to avoid the administrative problems associated with managing numerous contracts. There may be a problem getting European businesses to enter into the Draft Model Contract because of a reluctance to risk liability to data subjects for acts of importers, notwithstanding the indemnification provision. Some US importers may be concerned about submitting to the jurisdiction of European courts while others may prefer the risk of defending lawsuits in Europe to the risk of defending a charge of unfair or deceptive trade practice before the Federal Trade Commission.

C. Transfers With Prior Approval of the Government of the Exporting Country

The Directive also allows transfers with prior approval from the government of the EU member country where the transfer will originate. It allows a transfer if the government concludes that "adequate safeguards" to protect the privacy and freedom of individuals are in place,[98] including safeguards contained in "appropriate contractual clauses."[99] A member state must inform the European Commission of any approvals which it grants.[100] The national legislation in many member states is substantially similar to the Directive, although there are some minor variations.[101]

As was the case with model contracts, the alternative of prior government approval seems to apply primarily to "mainframe" business-to-business transactions rather than to direct transfers from consumers to US organizations. Nevertheless, there could be some situations where the operator of a US web site might seek approval for transfers of personal information. For example a US university might offer a course online and seek prior approval the government of the students' home country for online transfers of limited types of personal information connected with the class.

Citibank has already demonstrated the feasibility of obtaining prior approval of the government of the exporting country for a business-to-business transfer from a German subsidiary to the US. In 1996, Citibank entered into a contractual arrangement to provide privacy protection for personal data of German customers who had purchased discount railway cards. The privatized German Railway system had an agreement with a Citibank subsidiary to process railway card information at a Citibank facility in the U.S. Even though the arrangement was proposed prior to the 1998 effective date of the Data Protection Directive, German authorities acted as though it governed the transaction.[102]

D. Transfers Pursuant to Exceptions

The Directive and the conforming national laws contain some additional exceptions, several of which may be useful in transfers of personal data online. These include a transfer to which the data subject has given consent "unambiguously,"[103] a transfer necessary for the performance of a contract, [104] a transfer made on "important public interest grounds," a transfer to exercise or defend legal claims,[105] and a transfer to protect the "vital interests" of the data subject.[106] There is also an exception allowing a transfer from a register which, by law, is intended to provide information to the public.[107]

In theory, getting the data subject's consent for a transfer to a US organization at the time data is collected is one way to avoid the Safe Harbor. Consent, however, must have been given "unambiguously." This has been interpreted by the Article 29 Working Party of data protection commissioners of the EU Member Sstates to require that the consent be freely given, specific and informed.[108] However, some of the national laws are less restrictive by using the word "consent" without

the term "unambiguously".[109] On the other hand, Italy's law is more specific and states that consent be given "expressly" and even that it be in writing in some instances.[110]

In an online context, it might be possible to comply with the strict Italian standard, as well as the Data Protection Directive, by means of a concise, clearly written and prominently displayed, consent provision in the web surfer's native language on the web page where the user is first asked for personal data. Clicking on a box, however, might not satisfy the "unambiguously" requirement because a single click of a mouse could be accidental rather than intentional. A better approach might be to ask the user to type the phrase "I agree" in his or her native language in the consent box. Of course burying consent language in fine print in an obscure place on the web site, or making consent automatic unless the user opts out, would tend to be inadequate under European standards.

The exceptions for transfers necessary for the performance of a contract have been interpreted by the Article 29 Working Party as being subject to a necessity test, meaning that all of the data transferred must be necessary for the performance of the contract. Even with this narrow interpretation, it is likely that many transfers of data from Europe to the US, offline as well as online, currently fit within these exceptions every day. Examples would include electronic transfers of funds and travel reservations. Some US organizations, correctly or incorrectly, may be considering this alternative as being sufficient to permit them to continue receiving data from Europe without needing to use the Safe Harbor, the model contract or prior approval from a member state of the EU. This exception should not be relied upon unless only data which is truly necessary for the performance of the contract is being transferred.

Exceptions for transfers on "important public interest grounds," or to exercise or defend legal claims,[111] are unlikely to be of much use in consumer-to-business situations. The Article 29 Working Party interprets the public interest exception to include transfers between supervisory bodies in the financial services sector, as well as transfers between government institutions relating to taxes, customs duties and social security.[112] The other exception is considered to be limited to legal proceedings.[113]

Similarly, the provision allowing transfers to protect the "vital interests" of the data subject[114] is unlikely to apply to online transfers in the commercial context. According to the Article 29 Working Party, this provision only includes information essential for the data subject's life. This would allow the transfer of medical records when the data subject is facing a health crisis, but would normally not include information about property, finances or family interests.[115]

The Directive includes an exception allowing a transfer from a register which, by law, is intended to provide information to the public.[116] The Article 29 Working Party cautions that the exception should not be considered to permit the transfer of entire registers or entire categories of data from registers for commercial purposes or for the purpose of profiling specific individuals.[117] Instead, the exception is to allow someone to consult a public register within the EU from a location outside the EU.[118] This is much different from the US where there are few limits on the use of information in registers which are open to the public.

Of course some US businesses, deliberately or inadvertently, will collect and use the personal data of Europeans without attempting to comply with the Data Protection Directive or the national data protection laws. What can the Europeans do about this? The following section explores problems of compliance and enforcement.

IV. EUROPEAN RESPONSES TO ILLEGAL ONLINE TRANSFERS OF PERSONAL DATA

A. Actions in Europe Under European Law

The following discussion relates to situations where personal data is exported from Europe with no attempt to comply with any of the transborder transfer provisions arising out of Articles 25 and 26 of the Data Protection Directive and the recipient of the data is a US organization which has no physical presence in Europe. There are potential problems trying to enforce a law against someone who has never been within the state's territory. The Data Protection Directive attempt to avoid those problems by prohibiting the export of the data unless the importer is in a place where there is adequate protection for privacy or has made a binding commitment to provide privacy protection either by using a model contract or by making promises to the government of the exporting country when obtaining its approval for the export. In the event of an export violation, the most likely action by the exporting country's government will be to interrupt the flow of data. It is also possible that other remedies could be pursued either in Europe under European law, or possibly in the US under American law.

Except for a determination of the adequacy of privacy protection in a non-EU country,[119] European Union institutions do not have a formal role in responding to specific instances of illegal transfers of personal data across EU boundaries. Instead, compliance and enforcement are governed by national law usually administered by a data protection authority in the exporting country. The national laws generally include criminal as well as civil penalties. Penalties can involve a prison sentence of up to two years[120] and a criminal or administrative fine.[121] The data protection authority has power to block illegal data exports.[122] In addition, the data subject whose privacy rights have been violated has the right to a judicial remedy for any breach and the right to recover compensation.[123]

1. Questions of Jurisdiction in Europe

In the business-to-business context, an illegal export of personal data would subject the exporter to enforcement action by the data protection authority and to judicial proceedings by the data subject, all in the exporter's country. However, there may be problems obtaining jurisdiction over the importer, especially if the importer has no physical presence or assets in the exporting country. Nevertheless, in the business-to-business context, there is one party, the exporter, who clearly is subject to jurisdiction, and who therefore has an incentive to follow the requirements of the Data Protection Directive and national law.

The business-to-consumer situation, however, is different. The importer is obtaining personal information online directly from the data subject. Assuming that the importer has no physical presence or assets in the exporting country, the importer may believe that it is beyond the jurisdiction of administrative agencies and courts in the exporting country. It may believe that even if a judgment is obtained in the exporting country, a court in the importing country will refuse to enforce it for lack of jurisdiction. Of course these jurisdictional issues apply to many online activities other than privacy.

Within the European Union, jurisdictional questions connected with business-to-consumer transactions are governed by the Brussels Convention,[124] which is in the process of being modified by the proposed "Brussels Regulation."[125] Although the Brussels Convention and the proposed Brussels Regulation purport to deal only with jurisdictional issues within the European Union, they provide useful information about how questions of jurisdiction are addressed. Another recent development, the draft Hague Convention,[126] also deals with jurisdiction relating to consumer transactions. The draft Hague Convention would potentially have broader application depending upon the number of countries who sign and ratify it. In the US, global jurisdictional questions connected with online activities have been the subject of a draft study issued by the American Bar Association.[127] All of these documents attempt to answer the question of when can an out-of-state business be subjected to jurisdiction in the place where the consumer is located.

An important question under all the principles is the extent to which the out-of-state business has targeted the consumer. When a web site or online advertising company is deliberately collecting personal information from European computer users, there may be sufficient activity to be the basis for jurisdiction in the place where the consumer is located. Under the Brussels Convention, if there was advertising or a "specific invitation" addressed to the consumer in his or her state of domicile, and the consumer took steps necessary for the conclusion of the contract in that state, then the business is subject to the jurisdiction of courts there.[128] The language of the Brussels Convention is not well-suited to online activities. Although an e-mail message to a recipient in Europe would trigger this provision, a web site probably would not because it is not communication aimed at a particular person. The Proposed Brussels Regulation, however, is easier to apply to online activities. It provides that if the business "pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several countries including that Member State. . ." the business is subject to the jurisdiction of the courts there.[129] The "by any means" language arguably includes web sites and the use of online tracking technology. The "directs such activities" language is broader than the language about advertising or specific invitations contained in the Brussels Convention. Although the Brussels Convention and the proposed Brussels Regulation are binding only on EU Member States, they demonstrate that targeting of the consumer is an important jurisdictional concept in Europe.

The draft Hague Convention uses more complicated language to express the same idea. The out-of-state business can be subjected to the jurisdiction of the courts of the state where consumer is habitually resident if the conclusion of the contract is related to activities that the business has directed to that State, in particular in soliciting business through means of publicity.[130] Many interactive web sites probably can fit within this language as being activities directed to the consumer's state in soliciting business through means of publicity. Although online tracking technology arguably is activity directed to the consumer's state, it probably is not "soliciting business through means of publicity," as least in a direct sense. But if the tracking is viewed at a means of targeting online advertising, then it may well fit within the Convention's language are being part of "soliciting business."

Under these European principles there is considerable uncertainty as to when online activities will be sufficient to support jurisdiction. Nevertheless, a US web site might try to avoid the issue altogether by including choice of forum language as part of the terms of its online contracts or in a list of stated conditions of using its web site. In Europe, however, choice of forum clauses tend to be enforced only if they favor the consumer.[131] Of course there is no opportunity to attempt to use a choice of forum provisions for online profiling by network advertising companies because the web surfer is not informed of the tracking and profiling that is taking place.

Even if a European data protection authority or court concludes that it has proper jurisdiction, there still is the problem of enforcement of the order or judgment if the US business lacks assets in Europe. In the event that such an order or judgment were brought to a US court for enforcement, there likely would be a question of whether the foreign proceedings were consistent with the US Constitution's principles of due process. The language of the U.S. Supreme court in *Asahi Metal Industry Co. v. Superior Court*[132] is generally consistent with a targeting analysis. Justice O'Connor's opinion stated that a forum's ability to assert personal jurisdiction over the out-of-state defendant depends upon whether the defendant has

purposefully directed its action toward the forum state.[133] Any such analysis is highly dependent upon the facts. It is not clear exactly when a web site or a network advertising company that is collecting personal data of Europeans could be subjected to the jurisdiction in Europe consistent with US notions of due process. Accordingly, the assertion of personal jurisdiction by a European tribunal may face difficulties under a due process analysis when brought to a US court for enforcement.

The question of online activities being the basis for a European court's jurisdiction over a US company has been raised in connection with advertising and sale of Nazi memorabilia through a US web site. Advertising and sale of such items are illegal in France. The company, Yahoo, Inc., listed Nazi items for sale in the online auction service of its US web site, but did not carry the items on its French subsidiary's web site. Nevertheless, a French court issued an order requiring Yahoo, Inc. to block French users from gaining access to information about the Nazi items in its US web site.[134] Yahoo is contesting the French court's jurisdiction.[135] Although the French court's November, 2000, order contains little analysis of the question of its jurisdiction, it did find that current technology permits Yahoo, Inc., to detect correctly the location of 70% of the French visitors to its US web site, and that when the location determination is made, French language banner ads are displayed on Yahoo web pages viewed by the French users.[136] It is possible that the placement of the ads is sufficient evidence of targeting of web surfers in France to support the French court's jurisdiction consistent with US principles of due process.

2. Other Obstacles to Enforcement of European Law

The application of European data protection law to the transfer and processing of personal data of Europeans in the US raises questions about possible violation of the First Amendment of the U.S. Constitution. Several arguments could be raised to defend against enforcement of European orders and judgments in US courts. One argument is that communication of information about customers does not fall within the definition of commercial speech, that legal restrictions on such communication are not justified by a sufficient governmental interest and that the only restriction which is clearly permissible under the First Amendment is one imposed by contract.[137] Even if the communication of personal data is characterized as commercial speech, there are potential problems justifying the restrictions of European law. One issue could be whether the restricted speech concerns lawful activity.[138] This could depend upon whether the US court under its choice of law principles applies American or European law. If American law is applied and the speech concerns lawful activity, then there could also be a problem showing that European data protection law is the least restrictive means of promoting a substantial governmental interest.[139]

Enforcement of European law against illegal transfers of personal data to the US might also be challenged by the US before the World Trade Organization. One argument could be that transfers of personal data are services, that Europeans are illegally discriminating against the US by pursuing transfers to the US to a greater extent than similar illegal transfers to other countries and that this violates the General Agreement on Trade in Services.[140] Whether this argument based upon discriminatory enforcement is ever made will depend upon how the European data protection laws are enforced. Other arguments could be made under Article XX of the 1994 General Agreement on Tariffs and Trade[141] based on allegations of flaws in the process used by Europeans to enact data protection laws. Given the history of European data protection laws and the Safe Harbor negotiations, those arguments are relatively weak.[142]

B. Actions in the US on Behalf of Europeans Under US Law

Even if a US organization has made no attempt to comply with the European data protection law by joining the Safe Harbor, by entering into a model contract or by obtaining prior approval of the government of the exporting country, it may be possible for legal action to be taken in the US against the organization if it has abused the privacy of a European data subject. There following are some of the possibilities under US law.

If the abuse involves a violation of the organization's privacy policy, and if the organization is subject to the jurisdiction of the Federal Trade Commission, the activity could be pursued by the FTC as an unfair or deceptive trade practice under Section 5 of the Federal Trade Commission Act.[143] The FTC does investigate and take action on complaints from overseas.[144] The Department of Transportation could take similar action against a US airline which misuses European personal data in violation of its privacy policy.[145] Actions under state law are also possible under several legal theories including the common law torts of misrepresentation and invasion of privacy.[146] Of course, these legal theories could also be applied in situations where a US organization has joined the Safe Harbor, entered a model contract or has obtained export approval of a European government, but then has failed to abide by its privacy commitments.

VI. CONCLUSION

European data protection law can apply in some situations to online transfers of personal data to the US regardless of whether the recipient has any physical presence in Europe. It can apply to online transfers from European individuals

through e-mail and information entered through a web page, as well as through online transfers from a European database. There are several possible ways to comply with the Data Protection Directive. In many instances, the Safe Harbor is a good choice. In limited situations, a US organization may be able to comply by carefully adhering to one of the exceptions contained in Article 26 of the Data Protection Directive. Prior government approval of data transfers is another method of compliance, but is best suited to a large US organization receiving repetitive transfers of personal data from only a few sources in Europe. The March 27 Draft Model Contract is another possibility, but it is suitable only for transfers of data from a European organization and not from an individual.

There are potential problems enforcing European law against organizations with no physical presence in Europe. If a US organization has not joined the Safe Harbor, has not entered a model contract, has not obtained the approval of the government of the exporting country, has violated European data protection law and has no assets in Europe, the most reliable remedy available to Europeans would be to block future data exports. The ability to pursue other remedies in Europe is limited by jurisdictional issues, especially when trying to enforce a European order or judgment in the US. Clarification of the jurisdictional issues will probably require an international convention on jurisdiction which specifically relates to the Internet. There are also questions about the extent to which the US Constitution's protection of freedom of expression under the First Amendment could affect enforcement of European data protection law in the US. An adverse ruling by the World Trade Organization, however, does not appear to be likely, and therefore a US claim before the WTO should not pose a significant obstacle to the application of European data protection law to US organizations, as long as the US is not singled out for discriminatory treatment in enforcement.

The legal issues in this paper are part of a larger problem about how to deal with new technology that does not conform to existing legal principles, especially those based on territoriality. Greater international cooperation is required to resolve differences as well as update and harmonize legal rules. Many of the other developed countries in the world are taking this approach with respect to privacy. The US government and some US businesses have taken some steps in this direction as well by negotiating and joining the Safe Harbor.

Footnotes

---

1. Personal information is information about a living, natural person. It includes things like name, address, phone number, health condition, financial data, education records etc. It does not include trade secrets or most other business data. Employment records of a business, however, will be considered to be personal data if employees can be identified by name or identification number. The phrase "data protection" tends to be used in Europe because some European languages lack a word for "privacy."
2. A survey by American Express of 11,410 of randomly selected people in ten countries (Argentina, Australia, Brazil, Canada, Great Britain, Hong Kong, Italy, Japan, Sweden and the United States) found that 79% of respondents considered privacy and security to be major concerns with respect to engaging in online transactions. *Online Attitudes Move In Line Across the Globe: The American Express Global Internet Survey, at* http://home3.americanexpress.com/corp/latestnews/gis2000/gis2000.pdf (Oct. 2000).
3. *See generally* SIMSON GARFINKLE, DATABASE NATION (2000).
4. TRUSTe is an organization of web site operators who have agreed to certain privacy principles and who publicize their commitment to privacy through the display of the TRUSTe logo on their web sites. Members include IBM, Microsoft, Disney, the New York Times, L.L. Bean, Land's End and many others. Each web site operator must include its privacy policy on its web site. TRUSTe has a consumer resolution process where complaints about members can be filed on-line. *See generally* TRUSTe *at* http://www.truste.org (last visited May 30, 2001).
5. BBBOnline, which was created by the Council of Better Business Bureaus, Inc., has a privacy program which is similar to TRUSTe. *See generally* BBBOnline http://www.bbbonline.org (last visited May 30, 2001).
6. *See, e.g.,* Charter of Fundamental Rights of the European Union, art. 8, *at* http://eruopa.eu.int/comm/justice_home/unit/charte/pdf/charter_en.pdf (Dec. 7, 2000).
7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Council Directive 95/46, 1995 O.J. (L281) 31 [hereinafter Data Protection Directive].
8. *Id*. at art. 25.
9. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (2000) [*hereinafter* Safe Harbor Principles].
10. As of May 21, 2001, 43 companies have joined. Safe Harbor List, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/ safe+harbor+list (last visited May 21, 2001) [hereinafter *Safe Harbor List*]. Microsoft announced on May

15, 2001, that it would join the Safe Harbor as well. *See, e.g., Microsoft Will Sign EU - U.S. Data Privacy Pact, at* http://www.nytimes.com/reuters/technology...-dhtml?searchpv=reuters&pageswanted=print (May 15, 2001).

11. The European Commission insisted that eligibility be limited to US organizations which are regulated by the Federal Trade Commission and Department of Transportation. *See Safe Harbor Principles, supra* note 9, at 45668.
12. *Data Protection Directive, supra* note 7, art. 26(4). A draft model contract is in the process of being approved. *See, Draft Commission Decision on standard contractual causes on the web, Annex, at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clausesdecision.htm (March 27, 2001).
13. *Data Protection Directive, supra* note 7, art. 26(2).
14. *Id.* at art. 26(1). The term "derogations" is used to describe exceptions.
15. For a thorough discussion of how existing European privacy law affects online activities, *see generally Privacy on the Internet: An Integrated Approach to Online Data Protection* 16 -20 *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf (Nov. 21, 2001) [hereinafter *Privacy on the Internet*]. This report was prepared for and accepted by the Article 29 Working Party of European data protection commissioners organized pursuant to Article 29 of the Data Protection Directive.
16. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 1998 O.J. (L024) 1 [hereinafter *Telecommunications Privacy Directive*]. Article 1(2) recites that this directive supplements the Data Protection Directive.
17. *See* Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *at* http://europa.eu.int/comm/information_society/policy/framework/pdf/comm2000385_er (July 12, 2000). Article 1(2) of the proposed directive recites that supplements the Data Protection Directive.
18. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), 2000 O.J. (L178) 1 (2000). Recital 14 of this directive states that the Data Protection Directive and Telecommunications Privacy Directive govern data protection issues.
19. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, 1997 O.J. (L144) 19 (1997). This directive contains no reference to data protection.
20. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 2000 O.J. (L013) 12 (1999). Article 7(1) requires that electronic signature certification providers from outside the EU must either comply with all provisions of this directive, including Article 8(1) which requires compliance with the Data Protection Directive, have its certification guaranteed by a provider within the EU or be recognized under an international agreement. The latter two alternatives imply that a provider from outside the EU will not qualify unless it adheres to data protection principles which are adequate under the Data Protection Directive.
21. *Data Protection Directive, supra* note 7, art. 2 (a).
22. For a more detailed explanation of invisible profiling *see, e.g., Privacy on the Internet, supra* note 15 at 16-20.
23. Some browsers reveal the user's e-mail address to the web sites which are visited. *See Id.* at 32. Some web-based e-mail services ("webmail") use web bugs which transmit users' e-mail addresses to the network advertising company which places banner ads on the webmail service's web site. *See Id.* at 36.
24. Users could be identified as less desirable because of low income, their reluctance to click on banner ads or their activities in trying to protect their privacy. *See Id.* at 19.
25. Belgian and Dutch statutes follow the definition in the Data Protection Directive. Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC, Belgian State Gazette, February 3, 1999, 3049, art. 1 § 1 (Belgium) *at* http://www.law.kuleuven/ac.be/icri/papers/ legislation/ privacy/engels/ (last visited Aug. 23, 2000); Personal Data Protection Act, Act of 6 July 2000, Official Bulletin 302, providing rules for the protection of personal data, art. 1 (a) (Neth.) http://www.registratiekamer.nl/bis/top_2_6.html (last visited Mar. 12, 2001). The statutes of Italy and Portugal include explicit mention of indirect identification by reference to an identification number. Protection of individuals and other subjects with regard to the processing of personal data, Act no. 675 of 31.12.1996, art. 1(2)(c) (Italy) *at* http://www.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG+2 (last visited Mar. 12, 2001); Act on the Protection of Personal Data, art. 3(a) (Portugal) *at* http://www.cnpd.pt/Leis/lei_6798en.htm. (last visited Mar. 23, 2001).
26. Act on Processing of Personal Data, Act No. 429 of 31 May 2000, art 3(1)(1) (Denmark) *at* http://www.datatilsynet.dk/include/show.article.asp?art_if+443&sub_u.../indhold.asp &nodate= (last visited Mar. 13, 2001); Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000), art. 2 § 4 (Austria) *at*

http://wwwbka.gov.at/datenschutz/indexe.htm (last visited May 23, 2001). The English translation of the Swedish law uses an equivalent term: "referable." Personal Data Act (1998:204) issued 29 April 1998, § 3 (Sweden) *at* http://www.datainspektionem.se/in_english/ (last visited Mar. 13, 2001).

27. Data Protection Act, 1998, § 1(1) (Eng.).
28. *Data Protection Directive*, *supra* note 7, art. 2(d).
29. *Data Protection Directive*, *supra* note 7, art. 2(b).
30. *Data Protection Directive*, *supra* note 7, art. 4(1)(c).
31. *Data Protection Directive*, *supra* note 7, art. 4(2).
32. *Data Protection Directive*, *supra* note 7, art. 4(1)(c).
33. *See, e.g.*, Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC, Belgian State Gazette, February 3, 1999, 3049, art. 3bis(2) (Belgium) *at* http://www.law.kuleuven/ac.be/icri/papers/ legislation/ privacy/engels/ (last visited Aug. 23, 2000); Act on Processing of Personal Data, Act No. 429 of 31 May 2000, art 4(3)(1) (Denmark) *at* http://www.datatilsynet.dk/include/show.article.asp?art_if+443&sub_u.../indhold.asp &nodate= (last visited Mar. 13, 2001); Personal Data Protection Act, Act of 6 July 2000, Official Bulletin 302, providing rules for the protection of personal data, arts. 4(4)(2) & 4(4)(3) (Neth.) http://www.registratiekamer.nl/bis/top_2_6.html (last visited Mar. 12, 2001); Act on the Protection of Personal Data, arts. 4(3)(c) & 4(5) (Portugal) *at* http://www.cnpd.pt/Leis/lei_6798en.htm. (last visited Mar. 23, 2001); Personal Data Act (1998:204) issued 29 April 1998, § 4 (Sweden) *at* http://www.datainspektionem.se/in_english/ (last visited Mar. 13, 2001); Data Protection Act, 1998, §§ 5(1)(b) & 5(2) (Eng.).
34. Protection of individuals and other subjects with regard to the processing of personal data, Act no. 675 of 31.12.1996, art. 2(1) (Italy) *at* http://www.garanteprivacy.it/garante/ frontdoor/1,1003,,00.html?LANG+2 (last visited Mar. 12, 2001).
35. Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000), art. 3 § 1 (Austria) *at* http://wwwbka.gov.at/datenschutz/indexe.htm (last visited May 23, 2001).
36. *Data Protection Directive*, *supra* note 7, art. 25(1).
37. *See Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary*, 2000 O. J. (L 215) 4.
38. *See Commission Decision of 26 July 2000 pursuant to Directive 94/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland*, 2000 O. J. (L 215) 1.
39. *See Safe Harbor Principles*, *supra* note 9.
40. The European Commission insisted that eligibility be limited to US organizations which are regulated by the Federal Trade Commission and Department of Transportation. *See Safe Harbor Principles*, *supra* note 9, at 45,668.
41. *Safe Harbor List*, *supra* note 10.
42. *Data Protection Directive*, *supra* note 7, art. 26(4).
43. *Data Protection Directive*, *supra* note 7, art. 26(2).
44. *Data Protection Directive*, *supra* note 7, art. 26(1).
45. *Id*.
46. *Id.*
47. *Id*. For support for the view that notice should always precede data collection, *see, e.g.*, *Trans Atlantic Consumer Dialogue Statement on U.S. Department of Commerce Draft International Safe Harbor Privacy Principles, at* http://www.tacd.org/press_releases/state300300.html (last visited May 2, 2000)
48. *Id*. The choice to "opt out" may be exercised at any time. Moreover, organizations participating in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. *Frequently Asked Questions (FAQs) FAQ 12 - Choice - Timing of Opt Out, Safe Harbor Principles*, *supra* note 9, at 45674.
49. *Safe Harbor Principles*, *supra* note 9, at 45,666-67.
50. *See Trans Atlantic Consumer Dialogue Statement on U.S. Department of Commerce Draft International Safe Harbor Privacy Principles, at* http://www.tacd.org/press_releases/state300300.html (last visited May 2, 2000).
51. *Safe Harbor Principles*, *supra* note 9, at 45,666-67.
52. The Data Protection Directive permits processing necessary to perform a contract with the data subject, processing required by law, processing necessary to protect the vital interests of the data subject, procesing necessary for performance of a task carried out in the public interest and processing necessary for the legitimate interests of the data controller except when overridden by the interests or fundamental rights and freedoms of the data subject. Other processing requires the consent of the data subject. *Data Protection Directive*, *supra* note 7, art. 7.
53. *Safe Harbor Principles*, *supra* note 9, at 45,666-67.

54. *Compare Safe Harbor Principles, supra* note 9, at 45,666-67 *with Data Protection Directive, supra* note 7, art. 8(2),
55. *Safe Harbor Principles, supra* note 9, at 45,666-67.
56. *Frequently Asked Questions (FAQs) FAQ 8: Access, Safe Harbor Principles, supra* note 9, at 45,670, 45,672. Access may not be refused on cost grounds if the individual offers to pay the costs. *Id.*
57. In many situations, access need not be provided to information derived from public records. *Frequently Asked Questions (FAQs) FAQ 8: Access, Safe Harbor Principles, question 7, Safe Harbor Principles, supra* note 9, at 45,670, 45,672.
58. *Safe Harbor Principles, supra* note 9, at 45,666.
59. The organization can provide the personal information and need not provide access to the database itself. *Frequently Asked Questions (FAQs) FAQ 8: Access, Safe Harbor Principles, supra* note 9, at 45,668 Access may not be refused on cost grounds if the individual offers to pay the costs. *Id.* at 45, 671. Access need not be provided when it would interfere with law enforcement, interfere with private causes of action, reveal personal information about a third party, breach a legal or professional privilege, breach a duty of confidentiality connected with acquisition of a publicly held company, prejudice confidentiality connected with specified matters relating to employees and corporate reorganizations, prejudice confidentiality connected with sound economic management, or in other circumstances when the burden of providing access would be disproportionate, or when the rights or interests of others would be violated. *Id.* at 45,669.
60. The weakness of the access provision has been criticized by the Article 29 Working Party. *See Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles" Adopted on 16th May 2000 at* http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32en.htm (May 16, 2000).
61. *Safe Harbor Principles, supra* note 9, at 45,668.
62. *Id.*
63. *Id.*
64. *Frequently Asked Questions (FAQs) FAQ 6 - Self-Certification, Safe Harbor Principles, supra* note 9, at 45,669-70.
65. See *supra* notes 4 & 5.
66. *Frequently Asked Questions (FAQs) FAQ 6 - Self-Certification, Safe Harbor Principles, supra* note 9, at 45,669-70.
67. *Frequently Asked Questions (FAQs) FAQ 7 - Verification, Safe Harbor Principles, supra* note 9, at 45,670.
68. *Id.* FAQ 7 also states that organizations should maintain their records on implementation and make them available during investigations of complaints.
69. *Frequently Asked Questions FAQ 7 - Verification, Safe Harbor Principles, supra* note 9, at 45,670.
70. *Id.*
71. *Id.*
72. *Id.*
73. *See supra* notes 4 & 5.
74. *Id.*
75. *Frequently Asked Questions (FAQs) FAQ 11: Dispute Resolution and Enforcement, Safe Harbor Principles, supra* note 9, at 45,673-74.
76. *Id.* A U.S. organization that uses human resource data transferred from Europe in the context of the employment relationship must commit to cooperate in investigations by and to comply with the advice of competent European authorities in such cases. *Frequently Asked Questions (FAQs) FAQ 9 - Human Resources, Safe Harbor Principles, supra* note 9, at 45,672-73.
77. *Frequently Asked Questions (FAQs) FAQ 11: Dispute Resolution and Enforcement, Safe Harbor Principles, supra* note 9, at 45,672-73.
78. *Frequently Asked Questions (FAQs) FAQ 5 - The Role of the Data Protection Authorities, Safe Harbor Principles, supra* note 9, at 45,669.
79. *Id.*
80. *Id.*
81. *Id.*
82. *Safe Harbor List, supra* note 10. Of the 43 registrants 2 are exempt from the dispute resolution provisions. Of the remaining 41, 24 or 59% selected cooperation with the European data protection authorities (DPAs) as the primary method of dispute resolution. Another 8 or 19% elected to use cooperation with the DPAs to supplement other mechanisms. This means that 32 or 78% have made some commitment to work with the DPAs. Of the organizations which do not receive any human resources data, and are thus eligible to use any dispute resolution mechanism, 20 or 49% have made some commitment to work with the DPAs. Nine registrants or 22% relied exclusively on a private sector program. Six selected TRUSTe, two selected the Direct Marketing Association and one selected BBBOnline. Another 8 or 22% elected to use private sector programs (BBBOnline or UserTrust) as well as cooperation with the

DPAs. This means that a total of 17 or 41% have made some commitment to work with private sector programs.

83. *Safe Harbor Principles, supra* note 9, at 45,667.
84. *Data Protection Directive, supra* note 7, art. 26(4).
85. *Draft Commission Decision on standard contractual causes on the web, at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clausesdecision.htm (Mar. 27, 2001) [hereinafter *Draft Model Contract*]. The committee is often referred to as the Article 31 Committee because it is established under Article 31 of the Data Protection Directive.
86. *Id*.
87. The contract is to be governed by the law of the exporter's country, as long as that law recognizes the data subject's right to enforce the contract as a third party beneficiary. It is unclear from the draft what country's law should be chosen if the exporting country does not recognize the enforcement rights of third party beneficiaries. *Draft Model Contract, supra* note 85, Clause 10.
88. *Model Contract, supra* note 85, Clause 8.
89. *Model Contract, supra* note 85, Clause 4.
90. *Id*.
91. *Model Contract, supra* note 85, Clause 5(b).
92. *Model Contract, supra* note 85, Clauses 5(a), (c) & (e).
93. *Model Contract, supra* note 85, Clause 5(d).
94. *Model Contract, supra* note 85, Clauses 6(1) & (2).
95. *Model Contract, supra* note 85, Clause 6(3).
96. *Model contract, supra* note 85, Clause 7(1).
97. *Model Contract, supra* note 85, Clause 7(2).
98. *Data Protection Directive, supra* note 7, art. 26(2). The provision applies to a transfer or set of transfers.
99. *Id*.
100. *Data Protection Directive, supra* note 7, art. 26 (3).
101. For example, the Dutch statute authorizes the Minister of Justice to issue a permit for the transfer, after consulting the Dutch Data Protection Commissioner. Personal Data Protection Act, Act of 6 July 2000, Official Bulletin 302, providing rules for the protection of personal data, art. 77 (2) (Neth.) *at* http://www.registratiekamer.nl/bis/top_2_6.html (last visited Mar. 12, 2001). In Sweden, the statute authorizes the government to issue regulations authorizing such transfers. Personal Data Act (1998:204) issued 29 April 1998, sec. 35 (Sweden) *at* http://www.datainspektionem.se/in_english/ (last visited Mar. 13, 2001).
102. *See generally* Alexander Dix, *The German Railway Card: A model contractual solution of the "adequate level of protection" issue?"*, http://www.datanschutz-berlin.de/ doc/int/konf/18/bahn_en.htm.(last visited Mar. 22, 1999). Citibank has since withdrawn from the discount railway card program. Interview with Alexander Dix, Sept. 27, 2000. Dr. Dix is Data Protection Commissioner for the German State of Brandenburg.
103. *Data Protection Directive, supra* note 7, art. 26(1)(a).
104. *Data Protection Directive, supra* note 7, arts. 26(1)(b)-(c).
105. *Data Protection Directive, supra* note 7, art. 26(1)(d).
106. *Data Protection Directive, supra* note 7, art. 26(1)(e).
107. *Data Protection Directive, supra* note 7, art. 26(1)(f).
108. *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (Adopted July 24, 1998) Chapter Five: Exemptions from the Adequacy Requirement *at* http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/sp12en.htm (July 24, 1998) [hereinafter *Working Party Document on Transfers*].
109. *See, e.g.*, Personal Data Act (1998:204) issued 29 April 1998, § 34 (Sweden) *at* http://www.datainspektionem.se/in_english/ (last visited Mar. 13, 2001); Data Protection Act, 1998, schedule 4, § 1 (Eng.).
110. Protection of individuals and other subjects with regard to the processing of personal data, Act no. 675 of 31.12.1996, art. 28(4)(a) (Italy) *at* http://www.garanteprivacy.it/garante/ frontdoor/1,1003,,00.html?LANG+2 (last visited Mar. 12, 2001). Written consent is required for sensitive data (relating to health, race, ethnicity, trade union membership, sex life or religious, political or philosophical beliefs) and for certain data covered under the Criminal Procedure Code.
111. *Data Protection Directive, supra* note 7, art. 26(1) (d).
112. *Working Party Document on Transfers, supra* note 108.
113. *Id*.
114. *Directive, supra* note 5, art. 26(1) (e).
115. *Working Party Document on Transfers, supra* note 108.
116. *Data Protection Directive, supra* note 7, art. 26(1) (f).

117. *Working Party Document on Transfers, supra* note 108.
118. *Id.*
119. *See Data Protection Directive, supra* note 7, art. 25.
120. Maximum sentences of two years are possible in Belgium, Italy and Sweden. Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC, Belgian State Gazette, February 3, 1999, 3049, art. 41 § 3 (Belgium) *at* http://www.law.kuleuven/ac.be/icri/papers/legislation/privacy/engels/ (last visited Aug. 23, 2000); Protection of individuals and other subjects with regard to the processing of personal data, Act no. 675 of 31.12.1996, art. 35(2) (Italy) *at* http://www.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG+2 (last visited Mar. 12, 2001). A maximum sentence of one year is possible in Austria and Portugal. Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000), art. §51(1) (Austria) *at* http://wwwbka.gov.at/ datenschutz/indexe.htm (last visited May 23, 2001); Act on the Protection of Personal Data, art. 43 (1) (e) (Portugal) *at* http://www.cnpd.pt/Leis/lei_6798en.htm. (last visited Mar. 23, 2001). The maximum sentence is six months in the Netherlands. Personal Data Protection Act, Act of 6 July 2000, Official Bulletin 302, providing rules for the protection of personal data, art.72(2) (Neth.) *at* http://www.registratiekamer.nl/bis/top_2_6.html (last visited Mar. 12, 2001); Danish law allow "detention" but the data protection statute states no maximum term. Act on Processing of Personal Data, Act No. 429 of 31 May 2000, art 70(1)(1) (Denmark) *at* http://www.datatilsynet. dk/include/show.article.asp?art_if+443&sub_u.../indhold.asp &nodate= (last visited Mar. 13, 2001).
121. The data protection laws of Denmark, the Netherlands, Sweden and the United Kingdom provide for fines but do not specify amounts. Act on Processing of Personal Data, Act No. 429 of 31 May 2000, art 70 (1) (Denmark) *at* http://www.datatilsynet.dk/include/show.article.asp?art_if+443&sub_u.../indhold.asp &nodate= (last visited Mar. 13, 2001); Personal Data Protection Act, Act of 6 July 2000, Official Bulletin 302, providing rules for the protection of personal data, art.75 (1) (Neth.) *at* http://www.registratiekamer.nl/bis/top_2_6.html (last visited Mar. 12, 2001); Personal Data Act (1998:204) issued 29 April 1998, § 49 (c) (Sweden) *at* http://www. datainspektionem.se/in_english/ (last visited Mar. 13, 2001); Data Protection Act, 1998, § 60(2) (Eng.). Fines of up to approximately $2100 are possible in Belgium, up to approximately $8100 in Austria and up to approximately $8600 in Portugal. Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC, Belgian State Gazette, February 3, 1999, 3049, art. 39 (12) (Belgium) *at* http://www.law.kuleuven/ac.be/icri/papers/ legislation/ privacy/engels/ (last visited Aug. 23, 2000); Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000), art. §52(2) (Austria) *at* http://wwwbka.gov.at/datenschutz/indexe.htm (last visited May 23, 2001); Act on the Protection of Personal Data, art.38 (Portugal) *at* http://www.cnpd.pt/Leis/ lei_6798en.htm. (last visited Mar. 23, 2001).
122. This power is implied in provisions of national law implementing articles 25(1) of the Data Protection Directive which provides that Member States shall provide that exports take place only if the destination country ensures an adequate level of protection. *Data Protection Directive, supra* note 7, art 25(1). In at least one national law, this power is explicitly stated. *See, e.g.*, Protection of individuals and other subjects with regard to the processing of personal data, Act no. 675 of 31.12.1996, art. 29(5) (Italy) *at* http://www.garanteprivacy.it/garante/frontdoor/ 1,1003,,00.html?LANG+2 (last visited Mar. 12, 2001).
123. The Data Protection Directive requires that national implementing laws grant a judicial remedy to data subjects for any breach of his or her statutory privacy rights. *Data Protection Directive, supra* note 7, art. 22. A right of compensation must also be included in national law. *Id.* at art. 23(1).
124. Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, Sept. 30, 1968, 1978 O.J. (L304) 36 [hereinafter *Brussels Convention*].
125. Amended proposal for a Council Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *at* http://europa.eu.int/eur-lex/en/com/dat/2000/en_500PCo689.html (Mar. 5, 2001) [hereinafter *Proposed Brussels Regulation*].
126. Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, *at* http://www.hcch.ned/e/conventions/draft36e.html (Oct. 30, 1999) [hereinafter *Draft Hague Convention*].
127. Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet (London Meeting Draft) *at* http://www.abanet.org/buslaw/cyber/initiatives/draft.rtf (2000) [hereinafter *Draft ABA Report on Jurisdiction*].
128. *Brussels Convention, supra* note 124, arts.13 & 14.
129. *Proposed Brussels Regulation, supra* note 125, art. 15.
130. *Draft Hague Convention, supra* note 126, art. 7(1).
131. *See, e.g., Draft ABA Report on Jurisdiction, supra* note 127 at 35.

132. 480 U.S. 102 (1987).
133. *Id*. at 121.
134. League Against Racism and Antisemitism v. Yahoo, County Court of Paris, No. RG: 00/0538 *at* http://www.istf.org/archive/yahoo_france.html.
135. *See, e.g., Yahoo to defy French court order*, INDUSTRY STANDARD, *at* http://www.siliconvalley.com/docs/hottopics/hahll/002985.htm (Feb. 21, 2001).
136. *Id*.
137. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: the Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000).
138. Commercial speech which relates to unlawful activity is not protected by the First Amendment. *See, e.g.*, Central Hudson Gas & Electric v. Public Service Commission, 447 U.S. 557 (1980).
139. *See, e.g.*, 44 Liquormart v. Rhode Island, 517 U.S. 484 (1996).
140. *See* PETER P. SWIRE AND ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 189 (1998). Article XIV of the General Agreement of Trade in Services explicitly authorizes WTO members to enact laws to protect the privacy of individuals. General Agreement on Trade in Services, Apr. 15, 1994, art. XIV, 33 I.L.M. 1167 (1994).
141. General Agreement on Tariffs and Trade, Apr. 15, 1994, 33 I.L.M. 1554 (1994).
142. For an analysis of the relative strength of the European position based upon analogies to the 1998 WTO Appellate Body Report involving a US law protecting sea turtles, *see* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 52-55 (2000).
143. 15 U.S.C. §§ 41-58. The Federal Trade Commission does not have jurisdiction over financial institutions, insurance companies or telecommunications carriers. *See, e.g., Safe Harbor Enforcement Overview: Federal and State "Unfair and Deceptive Practices" Authority and Privacy*, July 19, 2000, *Safe Harbor Principles, supra* note 9, at 45675 (2000).
144. *See, e.g.*, letter from Robert Pitofsky, Chairman, Federal Trade Commission, to John Mogg, Director, DG XV, European Commission, dated July 14, 2000, *Safe Harbor Principles, supra* note 9, at 45,684 (2000).
145. 49 U.S.C. § 4712 is patterned after Section 5 of the Federal Trade Commission Act. *See, e.g.*, letter from Samuel Podberesky, Assistant General Counsel for Aviation Enforcement and Proceeding, U.S. Dept. of Transportation, to John Mogg, Director, DG XV, European Commission, dated July 14, 2000, *Safe Harbor Principles, supra* note 9, at 45,685 (2000).
146. *See, e.g.*, Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law, July 19, 2000, *Safe Harbor Principles, supra* note 9, at 45,678 (2000).