Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Data Protection in Europe and the Internet

Dhont, Jan; Bergkamp, Lucas

Published in:
The EDI Law Review

Publication date:
2000

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (HARVARD):
Dhont, J & Bergkamp, L 2000, 'Data Protection in Europe and the Internet: an analysis of the European Community's Privacy Legislation in the Context of the World Wide Web', *The EDI Law Review*, vol. 7, no. 2-3, pp. 71-114.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. May. 2026

The EDI Law Review 7: 71–114, 2000.
© 2001 *Kluwer Law International. Printed in the Netherlands.*

Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web

LUCAS BERGKAMP AND JAN DHONT
Hunton & Williams, Ave. Louise 326, B6, 1050 Brussels, Belgium

1. Introduction

Over the last decade, due in large part to technological advances, data protection has become a worldwide topic of debate. The computer and information society greatly facilitate the ability of people to quickly gather and manipulate data relating to other persons. To prevent the ensuing risk to privacy, the European Union (the "EU") enacted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Directive"), which lays down general principles on data protection. The Directive applies to the processing of personal data, protects individuals from nonconsensual uses of personal data, and, subject to limited exceptions, prohibits the transfer of personal data to non-EU Member States which are deemed to offer an "inadequate" level of data protection. The Directive is supplemented by Directive 97/66 on the protection of privacy and personal data in the telecommunications sectors, which establishes specific legal and technical provisions for the telecommunications sector. The Commission has proposed an overhaul of Directive 97/66/EC to update it and provide for rules which are technology neutral.[1] The EU has also proposed to include the right to data protection in a proposed European charter of fundamental rights.[2]

In the Directive's recitals, the Commission recognizes that, although data processing systems are designed to serve man, such systems must respect the fundamental rights and freedoms, especially the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals. The stated purpose of the Directive is to "amplify" the rights and freedoms of individuals contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[3] Also, by making the level of protection of the rights and freedoms of individuals with regard to the processing of personal data equivalent in all Member States, the Directive seeks "to remove the

obstacles to flows of personal data" and thereby allow transmissions of such data from the territory of one Member State to that of another Member State. Providing a general framework, the Directive calls for the completion of the legal prescriptions by self-regulatory action.

Thus far, in the US, the concern about the invasion of privacy that might result from the use of automatic data processing has not resulted in the regulation of the collection or use of personal data. In the US, where there is concern about ever increasing state intervention, the government encourages a self-regulatory approach with respect to data protection. This an important issue between the US and the EU. The EU believes that the self-regulatory approach largely relied on by the US does not offer an adequate level of protection to the privacy of individuals and therefore dislikes the transfer of data to the US. The US and the EU have agreed Safe Harbor Principles which are designed to serve as guidance to US organizations seeking to comply with the "adequacy" requirement of the Directive. Organizations complying with the Safe Harbor Principles will be considered as providing an adequate level of protection to privacy, and data transfers from the EU to them would be permitted.[4]

This article analyzes of the main principles, rights and procedures set forth in the Directive. Specifically, it examines their scope and application in the context of the processing of personal data by means of automated technologies. Part 2 discusses the Directive's background. In Part 3, the main definitions are analyzed. We focus specifically on the concept of personal data and the key concepts of controller and processor. The definitions of consent and processing of data are also reviewed. Part 4 addresses the Directive's geographical scope and the exceptions to its scope. In Part 5, the substantive requirements applying to data processing are analyzed. Relatedly, Part 6 focuses on the requirements regarding the processing of sensitive data, which is subject to additional restrictions. Part 7 deals with rights of data subjects, including the right to information, the right to access and the related right to rectify and erase, the right to object to processing, and the right to confidentiality. Technical and organizational measures are discussed in Part 8, and notification obligations in Part 9. The transfer of personal data to a non-EU country is analyzed in Part 10. This Part discusses conditions for transfer and exemptions, as well as the EU/US Safe Harbor Arrangement. Self-regulation, including codes of conduct, are reviewed in Part 11. In Part 12, we analyze the processing of personal data over the internet, specifically the applicability of the Directive. It discusses also the Telecommunications Directive, the Electronic Commerce Directive, the EU Working Party's Report on Internet Privacy, and the international law on extra-territorial jurisdiction. In Part 13 we turn to remedies and sanctions. Some final observations and a critique of the EU's privacy regime are set forth in the last part.

2. The Directive's Background

The EU adopted the Directive in 1995. Member States were required to implement it in their national legislation by October 25, 1998. As of May, 2000, the Directive has been implemented in the following Member States: Sweden, Greece, Italy, Belgium, Portugal, Austria, United Kingdom, Denmark (partial implementation), Spain, Finland and the Netherlands. As France, Luxembourg, Germany and Ireland have failed "to notify all the measures necessary to implement the Directive on the protection of personal data," the Commission has taken these member states to court.[5]

Even though some Member States have failed to implement, or have not fully implemented, the Directive, individuals in those Member States may be able to invoke some of the Directive's provisions against the state before national courts.[6] This is the doctrine of "direct effect." Under EU law, direct effect is accorded to provisions in a Directive that are "unconditional and sufficiently precise."[7] In addition, under the indirect effect doctrine (also known as the interpretation principle) the national administrations and courts of Member States are required to interpret their national laws in light of the wording and the purpose of the Directive. This doctrine enhances the effectiveness of non-implemented or misimplemented Directives. The obligation to interpret a national provision in conformity with a Directive arises whenever such provision is open to interpretation. In interpreting a national provision, the national court must use its methods of interpretation and give precedence to the method that enable it to construe the relevant national provision in a manner which is consistent with the Directive. The limits, however, to the interpretation principle are not clear. Initially, in *Marleasing*, the European Court of Justice (the "ECJ") stated that "in applying national law, whether the provisions in question were adopted before or after the Directive, the national court called upon to interpret it is required to do so, as far as possible, in light of the wording and the purpose of the Directive in order to achieve the result pursued by the latter." In cases subsequent to *Marleasing*, however, the ECJ seems to have given national courts discretion to determine whether or not an interpretation in conformity with the Directive was possible.[8] In addition, it is unclear whether the interpretation principle applies horizontally, i.e. between individuals. Individuals incurring damages as a result of a Member State's failure to implement the Directive are in some cases entitled to seek compensation from a Member State before national courts.[9]

The Directive has been heavily influenced by the concept of "informational self-determination" endorsed by the German Federal Administrative Court (Bundesverfassungsgericht).[10] This theory holds that an individual should have a right to control "the image of his personality" that is presented to others through the processing of his personal data. Individual control implies that all processing modalities are transparent and known, and agreed and verifiable

by the data subject. The theory acknowledges, however, that personal autonomy is not absolute, and that limitations to these principles are legitimate.

3. The Directive's Key Definitions

Personal Data and Special Categories of Data

The Directive defines the term "*personal data*" as "any information relating to an identified or identifiable natural person." An *identifiable person* "is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." It is not necessary that data identifies the data subject. The mere fact that data can be related to an identifiable or identified person suffices. [11] To determine whether a person is identifiable, Recital 26 of the Directive specifies that one should consider "the means likely reasonably to be used either by the controller *or by any other person* (emphasis supplied) to identify" the data subject. This is generally interpreted to mean that the Directive is applicable also to personal data rendered "anonymous"[12] by an intermediary, unless "reverse identification" would be infeasible or unreasonably difficult. In the context of a medical research program, for instance, if a medical doctor replaces the personal identifiers of medical data sent to a pharmaceutical enterprise by an ad random number assigned by the computer, the Directive applies, since the supplier of the information, i.e. the doctor, can relate the data to a specific patient.[13] Data in the form of sounds or images are also covered by the Directive, if they identify specific individuals. Thus, multimedia processing may be subject to the Directive's regime.[14]

Identifiability turns on "the means likely reasonably to be used." The meaning of these words is unclear. The reference to means is probably intended to cover only technical means. In practice, reversible coding may be supplemented by contractual restrictions (and sanctions) to prevent identification of individuals. Such restrictions make the use of technical means less likely and unreasonably and should thus be taken into account in determining whether data are personal data. Also, the cost of decoding is a factor that impacts on the likelihood of possible decoding; the higher the cost the less likely decoding is.[15]

The Directive also covers special categories of data, which are typically referred to as sensitive data in the national data protection laws of Member States. The Directive includes the following data within its special categories of data (hereinafter referred to as "sensitive data"): "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex-life." These data are subject to additional restrictions.

In the context of the internet, two types of personal data can be distinguished, i.e. user related data and data contained in a message (e.g. an e-mail message). User related data are electronic data that are generated when a user connects to and uses the internet. To effect a transmission of information between a web site and a personal computer, an IP number is granted by the access provider to the computer of the user. If the IP number is not person-specific but assigned only for a particular session, and changes regularly, it does not constitute "personal data."[16] Most access providers, however, demand the user's name and address before offering their services. In these cases, the IP number and traffic and navigation data (e.g. URLs) might constitute personal data. On the other hand, IP numbers are not personal, and one and the same IP number is used and reused for a large group of persons. Further, when connecting to the internet via a telephone line, the user's telephone number will be communicated to the provider, which enables indirect identification of the user. As noted above, if identification entails significant costs or is technically difficult, the European data protection rules do not apply. The EU Privacy Working Party has correctly observed that "it might not be possible to identify a user in all cases and by all internet actors from the data processed on the internet."[17] This would be the case, for instance, in respect of work stations where one general IP number is used by a server for all personnel.[18]

The digital data generated by an internet user exceeds the mere IP number and may involve invisible processing. Examples of invisible processings are the "chattering" at the HTTP level,[19] automatic hyperlinks to third parties, and the cookies mechanism currently implemented in the common browsers.[20]

Data collected by such mechanisms, are not necessarily personal data. Technical data generated by the browser[21] or data collected and sent by a cookie to a web site do not, as such, constitute personal data. This information can not *ipso facto* be related to an identified or identifiable person. However, the information contained in a cookie may be deemed personal data in two cases: (1) if it is supplemented added to personal data (e.g. the user provides his name and address, e-mail address, etc.), or (2) if the web site that receives the data already has personal data about the specific user at his disposal, and is able to crosslink the data (e.g. the site bought data from an online direct marketing company), so that direct or indirect identification becomes possible. Some national privacy authorities take the position that all data collected by a cookie constitutes personal data. They argue that a cookie contains an identification number in the sense of Article 2(a) of the Directive, permitting indirect identification. The term "identification number," however, is generally understood to refer to a number assigned to a specific individual known by name, not a number used only to identify the source of communications. Moreover, on the basis of cookie data, no direct or indirect identification would normally seem possible. Privacy advocates have argued that utilization of the

mechanisms described above, may create a picture of the internet user corresponding to the personality of the user's personality. Such a "virtual personality," according to these advocates, should be protected under the privacy legislation. As noted, without more, such data are not personal data.[22]

Data contained in an e-mail message may include personal information. If, for instance, a person orders a book via the internet, he transmits his name and address, and credit card number. The internet user may also voluntary disclose certain personal data (e.g. publication of c.v. on the internet). There is no question that this information should be considered personal data, although it would be awkward to apply the Directive's regime to data voluntarily published by the data subject.

Controller, Processor, Third Party, and Recipient

The terms controller, processor, third party and recipient are defined in the Directive in the following manner. The "*controller*" is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[23] If a controller is established outside the EU, he is required to appoint a representative in the EU. Actual possession of the data is not required; a person may have actual control over the processing without possessing the data (e.g. a company that outsources the processing of employee-related data).[24] A "*processor*" is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." The term "*third party*" refers to "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process data," while "*recipient*" refers to "a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not (the Directive excludes authorities which receive data in connection with a particular inquiry from the definition of recipients). Each of these "data holders" must comply with his respective obligations set forth in the Directive; most of the obligations are imposed on the controller.

Applying these definitions in the context of the internet often is a challenge. Identifying a data controller in an open network, for instance, is difficult. Such a network is characterized by numerous intervening actors, such as (1) telecommunication network providers, (2) access providers supplying services for storage, transmission and presentation, (3) information providers, (4) content service providers and (5) individuals making use of these services.[25] Some of these services may be offered by the same actor (e.g. a network provider offering access). In such a network, there may be multiple controllers. The traffic data and other user related data generated by the network are

controlled by network and access providers. They decide upon the purpose and means of processing.[26] The information service provider or e-tailer may also collect and process personal data in an overt (e.g. the user filling in an order form) or hidden (through a cookie) fashion; these entities are controllers with respect to these data.

E-mail traffic may also involve multiple controllers. Recital 47 of the Directive states that where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be deemed to be the person from whom the message originates, rather than the person offering the transmission services. Consequently, when an individual uses an e-mail service on the internet, he should be considered as a controller of the personal data in the e-mail, since he determines the purpose and means of processing. The transmittor will be deemed the controller in respect of the processing of additional personal data necessary for the operation of the service; once the data is received or intercepted, the receiver or interceptor will become the controller.

Definition of Consent

The Directive's purpose is the protection of individual privacy. Accordingly, as a general principle, the "unambiguous consent" of the data subject is necessary for the processing of personal data relating to him by a third party. Also, the transfer of data to a third country which does not ensure an adequate level of protection is generally prohibited, unless the data subject has "unambiguously consented" to it. While the term "unambiguous" is not defined, the Directive defines the data subject's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

"Freely given" is generally interpreted to require that consent is given without undue external pressure. In two situations the freedom to consent may be deemed diminished. First, consent may be deemed not freely given if there is a hierarchical relationship between controller and data subject or the data subject is otherwise dependent on the controller. This may be the case, for instance, where an employer requests access to personal data to evaluate the health of an employee. The employee may feel that his refusal will be held against him. If the data subject is significantly dependent on the controller, additional guarantees may be required for consent to be regarded as freely given (e.g. in a patient-doctor relationship, the doctor should explain that refusal to consent will not influence the care to be provided to the patient). Second, consent may be tainted if refusal to consent is penalized directly. For

instance, refusing to deal unless consent is given, in some situations, may render consent unfree. On the other hand, if a refusal to deal imposes only a small burden, consent will likely not be deemed unfree. For instance, free electronic mail services may not be available without accepting a cookie. In this case, consent is freely given since equivalent services are available in the market.

The consent principle reflects the idea of "informational self-determination," which, as noted above, is a foundational principle of the European data protection rules. Applying the consent principle in practice raises several issues. First, although consent in many cases is a necessary condition to legitimate processing, it is not a sufficient condition; the law imposes additional restrictions on data processing. Unlike the Safe Harbor Principles, discussed in Section 10 below, consent does not legitimize processing for purposes to which the data subject has agreed. Under the Directive, processing may be done only for specified, explicit and legitimate purposes.[27] The Member States have the authority to define the concept of the legitimate purpose when transposing the Directive. However, most Member States have merely copied the Directive's words, and adopt a case-by-case approach.[28] The legitimacy requirement is not specified by law, and the controller is responsible for determining what is legitimate, but the authorities may disagree and overrule his assessment. Consequently, controllers are exposed to significant legal uncertainty and the national privacy authorities' discretion.

Second, and relatedly, an individual may not be able consent to acts that are deemed a violation of his rights. While in the US privacy is conceived as an "interest" that can be negotiated away, a contractual waiver would not necessarily be effective in Europe where privacy is conceived as a "fundamental right."[29] This issue is particularly relevant in the context of schemes such as the Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS).[30] Under these schemes, privacy protection is agreed between the internet user and the service provider collecting the data. P3P involves obtaining the user's consent through a choice function in the browser, enabling the user to specify the data processing purposes to which he agrees.[31] The system's philosophy is that the user consents to a site collecting his personal data, if the site's declared privacy practices, the purposes for which data are collected, the intended use of the data (e.g. whether data are used for secondary purposes or passed on to third parties), and other conditions satisfy the user's requirements.[32] P3P would appear to meet the consent and self-determination principles for internet applications. However, it may not be considered to fulfil the legal requirements with respect to legitimate processing. Depending on the specific circumstances, "legitimate processing," in the opinion of data protection authorities, may require additional guarantees. In this regard, the EU Privacy Working Party emphasized that "a technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. (. . .)

> Use of P3P and OPS (. . .) risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the 'data controller' who is responsible for complying with data protection principles. (. . .) There is a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the online negotiation."[33] These statements suggest that national data protection authorities may enforce data subjects' rights, even if the data subjects involved have explicitly waived their rights. Thus, by supplementing the consent requirement with the legitimate processing requirement, the Directive imposes an additional open-ended test that decreases legal certainty and increases the government's discretionary powers to the detriment of both data subjects and controllers.

Processing of Data

The term "processing of personal data" refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking erasure or destruction." The definition of processing is so broad that virtually all data operations from "cradle" (collection) to "grave" (destruction) are deemed to be the processing of data in the EU. Note, however, that the processing of personal data carried out solely for journalistic, artistic or literary expression purposes are exempted from the scope of the Directive if such exemptions are "necessary to reconcile the right to privacy with the rules governing freedom of expression."[34] The term "use" is not defined in the Directive and may also cover addressing a person through mail, e-mail, telephone, fax or otherwise.[35]

The broad definition of "use" is troublesome and could lead to absurd situations when applied to open networks. For instance, the simple consultation of a web site, i.e. the mere reading of information, qualifies as "processing" under the "use" part of the definition. If the web site contains personal data about other persons – which is not uncommon – the user should inform the data subjects that he has consulted a site containing personal information about them, notify the privacy authority of his processing, and grant the data subjects a right of access to the information that the user temporarily stored in the RAM memory of his computer, and in his mind. Obviously, this scenario falls outside the Directive's *ratio legis*. Mere consultation of data without sufficiently

durable storage should therefore not deemed to be covered by the notion of "processing."[36]

4. Scope of Application of the Directive

The Directive's territorial scope of application is broad. Under Article 4 of the Directive, a Member State must apply its national data protection legislation in three situations. First, the *processing* is carried out by a controller established on the territory of that member state. If a data processor has controllers established on the territory of several Member States, he must ensure that each of those establishments complies with the laws of each Member State on which it is established. Second, the controller, although not established on the territory of that member state, *uses equipment* (automated or otherwise) situated on the territory of the member state for the purposes of processing personal data. This does not apply to equipment used for the transmission of data through a Member State. The "use of equipment" test may establish jurisdiction over data controllers who are established outside the EU and collect data from EU residents via the internet. Third, the controller, although not established on the territory of the member state, is established in a place where the national law of that member state applies by virtue of international public law. This clause most likely applies only to embassies, military bases and the like, and not to private companies. These provisions regarding the Directive's territorial scope raise questions when applied to the internet. These issues are discussed in Section 13, below.

There are two general exceptions to the Directive's scope. Article 3 of the Directive provides that the processing of personal data shall not be subject to the Directive if (1) it occurs "in the course of an activity which falls outside the scope of Community law such as those provided for by Titles V and VI of the Treaty on the European Union and in any case to processing operations concerning public safety, defense, state security (including economic well-being of the state when the processing operation relates to State security matters) and in areas of criminal law"; or (2) it is carried out by a natural person in the course of a purely personal or household activity.

5. Lawfulness of Data Processing

Chapter II of the Directive sets forth general rules on the processing of personal data and authorizes Member States to determine more precisely the conditions under which the processing of personal data is lawful. Specifically, the Directive requires that personal data be: (a) processed "fairly and lawfully, (b) collected for specified, explicit, and legitimate purposes and not further

processed in a way incompatible with those purposes, (c) adequate, relevant, and not excessive in relation to such purposes, (d) accurate, and, where necessary, kept up to date; and (e) kept in a form that permits identification of data subjects for no longer than is necessary." The legitimate purpose requirement set forth in article 6(b) of the Directive, according to some authors, encompasses the consent requirement,[37] but is broader than consent (see Section 3, above). Compliance with these requirements must be ensured by the controller. The lawfulness and legitimacy of the processing imply ad-hoc balancing of the controller's and data subject's interests in each specific case.[38] The outcome may vary between Member States, and even among authorities in the same Member State. Such variances might hamper the free flow of information within the EU.

In addition to these general requirements, the Directive imposes further restrictions on the processing of personal data. Pursuant to the Directive, personal data may be processed only under certain circumstances. In principle, the processing of personal data is permitted only if the data subject has unambiguously given his consent to such processing. As discussed in Section 9 below, to obtain the "unambiguous" consent of a data subject, it is advisable to disclose certain information to him.

The data subject's consent for the processing of personal data relating to him is not necessary in a number of narrowly defined situations. First, consent is not required if processing is necessary for the performance of a contract with the data subject or is done at his request in connection with preparing to enter into a contract (e.g. a service provider requests that, in order for certain services to be performed, the e-mail address and the name and phone number of the data subject be provided to him).

Second, processing may proceed without consent if it is necessary to protect the vital interests of the data subject or of another person. According to the Directive's Recital 31, this exception applies only if processing is necessary to protect an interest which is "essential for the data subject's life." The processing of personal data in urgent medical situations is covered by this provision.

Third, consent is not required if processing is necessary for the purposes of the "legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject." As noted above, the term "legitimate interests" is not defined in the Directive. Recital 30 of the Directive, however, refers to "the legitimate ordinary business activities of companies and other bodies." As a result, "legitimate interests" probably cover "legitimate business interests," which may include direct marketing. If this exemption applies to a database used for direct marketing, it should also be determined whether the privacy interests of the data subject do not override the business interests of the data controller. This determination

is to be made under the national data protection laws of the Member States. For example, to make such a determination in the Netherlands, the controller would be required to answer and document answers to the following questions: (1) Is there an interest that justifies the processing of data? (2) Does the processing infringe upon the interests of the data subjects and, if so, should data processing therefore not be undertaken. (3) Can the purpose for which the processing is carried out be pursued through alternative means that meets privacy concerns? (4) Is the processing proportional to the objective pursued? Ultimately, it is for the national legislation implementing the Directive to specify the meaning of "legitimate interests." For example, the Italian[39] and Spanish[40] legislation stipulate that the processing of personal data for direct marketing purposes does not require the consent of the data subject.[41] The Dutch law does not explicitly provide that consent is necessary with respect to direct marketing; if the general proportionality standard is met, direct marketing without consent may be permissible.

Fourth, consent is not required if processing is necessary for the controller to comply with his legal obligations. Fifth, if processing is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's or a third party's (to whom data are disclosed) official authority. The notion of "public interest" is vague and interpretation will likely vary between the Member States. In Belgium, for instance, processing for epidemiological purposes is deemed a public interest and thus may proceed without prior consent. Similarly, the phrase "exercise of an official authority" will likely be interpreted differently across the EU. National legislation is to determine whether only public agencies or also natural or legal persons governed by public law or by private law, such as professional associations, may qualify under this exemption.[42]

6. Processing of Sensitive Data

The processing of sensitive data,[43] in principle, is prohibited, unless the data subject has given his explicit consent to such processing. However, data protection laws of the Member States may provide that this general prohibition may not be waived by the data subject's.

The Directive also authorizes the processing of sensitive data, without the need of the data subject's consent, under either of the following conditions. The first condition is that "processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards." Second, the data subject is physically or legally incapable of giving his consent and the processing is necessary to protect the "vital interests" of the data subject or of another person. Third, the processing

is carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects." Fourth, "the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims." Fifth, the processing of "data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health services," and if such data are processed by "a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."[44] Note, however, that meeting one of these conditions does not imply that the other requirements imposed by the Directive do not apply.

In some Member States, the processing of personal data for marketing purposes may pass the legitimacy test, even if no consent is obtained. However, consent is always required for processing of sensitive data for these purposes. Accordingly, an opt-out arrangement for direct marketing purposes offered to data subjects visiting a web site offering medical or pharmaceutical products or services, would not be deemed sufficient. Only an opt-in formula is sufficient when health data is processed for direct marketing purposes (cf. Section 13 below).

7. The Rights of Data Subjects

Data subjects have a number of legal rights vis-à-vis the controller. These rights constitute, together with the fairness and legitimate purpose requirements, are the heart of the EU data protection regime. They are based on the idea that processing should be done transparently and in a controllable manner, and in general be subject to the data subject's wishes.

Right to Information

The controller or his representative must provide a data subject from whom data is collected with certain information if such information is necessary "to guarantee fair processing in respect of the data subject." This qualification is not further explained in the Directive, which merely refers to the transparency requirement.[45] For example, the following information must be provided: (1) the identity of the controller and of his representative (if any); (2) the purpose of the processing; (3) any other information such as a) the recipients or

categories of recipients of the data, b) whether the data subject is obligated to answer the questions and the consequences for failing to reply to such questions; c) the existence of the right of access to and the right to rectify data relating to him, and d) given the specific circumstances surrounding the processing of data, any other information that is necessary to guarantee the fair processing of data. For instance, the processing of sensitive data requires that this supplementary information is provided to the data subject.

If, however, personal data are not collected from the data subject but from other sources, such information must also be provided to the data subject at the time of the recording of such personal data, or if such data are to be disclosed to a third party no later than the time when the data are first disclosed to such party, except where providing such information would be "impossible" or involve a "disproportionate effort," or if recording or disclosure is expressly required by law (i.e. processing for statistical purposes or for the purposes of historical or scientific research). In addition to the information set forth above, the categories of the data (e.g. name, address, etc.) concerned must also be disclosed to the data subject.

Hyperlinking, the cookies mechanism and chattering of browsers are generally deemed impermissible if the internet user is not adequately informed, unless the service provider can prove that the user was already aware.[46] Proving the latter is typically impossible. The EU Privacy Working Party has taken the position that internet software and hardware products should provide internet users information about the data that they intend to collect, store or transmit and the purpose for which the data are necessary.[47] Further, software and hardware products should also enable a data user to easily access any data collected about him at any later stage.[48]

Right of Access and Right to Rectify or Erase

Every data subject has the right to obtain from the controller, without constraints, at reasonable intervals and without excessive delay or expense, (1) confirmation as to whether or not data relating to him are being processed and information regarding the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, (2) a "communication" (in an intelligible form) regarding the data that is undergoing the processing and of any available information as to their source, and (3) information regarding the logic involved in any automatic processing of data concerning him in connection with automated decisions (e.g. automated data processing intended to evaluate certain personal aspects of the data subject such as creditworthiness, reliability, conduct etc.). The term "excessive expense" is to be interpreted by the Member States.[49] The Member States are also to adopt procedures for obtaining access.

Article 13 of the Directive provides some exemptions and restrictions with respect to, *inter alia,* the right of information and access. These rights may be restricted by the Member States if necessary to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offenses, or of breaches of ethics for regulated professions. In the context of medical telematics, Article 13 (g) of the Directive comes into play. This article provides an exception to the rights of information and access to safeguard the protection of the data subject or the rights and freedoms of others. This provision allows, for instance, that national legislatures limit these rights of the patient to accommodate the therapeutic liberty of medical doctors (e.g. no access to the doctor's personal notes in the patient's medical file).

The data subject also has the right to have the controller rectify, erase, or block data which is inaccurate or incomplete and the processing of which does not comply with the Directive. In addition, unless it is impossible or it involves a disproportionate effort, the data subject has the right to have the controller notify third parties (to whom data have been disclosed) of the rectification, erasure or blocking of such data.

Right to Object to Processing

In certain situations where the processing of personal data may take place without the data subject's consent, Member States must at least grant the data subject the right to be informed about the intended processing and to object to it on "compelling legitimate grounds relating to his particular situation," save where otherwise provided by national legislation. These situations are the following. First, processing may proceed without the data subject's consent if it is carried out for the purposes of the "legitimate interests pursued by the controller or by the third party to whom the data are disclosed." Article 40 of the Dutch Data Protection Act provides for an employee's explicit right to object to processing in certain specific circumstances.[50] What these circumstances might be, is not clarified further. Some authors suggest that the notion of 'compelling legitimate grounds' set forth in the Directive implies that the data subject must show that the consequences of intended processing have detrimental effects for him personally.[51] Second, processing may be done without consent if it refers to the performance of a task carried out in the public interest or in the exercise of the controller's or a third party's (to whom data are disclosed) official authority.

However, the data subject always has the right to object if processing is done for purposes of direct marketing. The exercise of this right must be free of charge and the data subject may not be required to state reasons for his objection. The

Directive leaves it to the Member States to implement this right. Member States may require that when the controller anticipates that data will be processed for the purposes of direct marketing, he must inform the data subject and give him an opportunity to object to the processing before it commences. If personal data is intended to be transmitted to a third party for direct marketing purposes, data subject must be given an opportunity to object before transmission.

In the context of the internet, the Telecommunication Privacy Directive also imposes restrictions on direct marketing. Under the current Directive, unsolicited calls through voice telephony for purposes of direct marketing are not allowed without the subscriber's consent (opt-in) or in respect of subscribers who have indicated that they do not wish to receive these calls (opt-out); national law determines whether an opt-in or opt-out regime applies.[52] The proposed Directive concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, which will replace the Telecommunication Privacy Directive, provides the same choice to national legislatures with respect to open network applications, such as the internet, but imposes an opt-in regime for communications by e-mail for purposes of direct marketing.[53] Consequently, in every Member State, the controller will have to obtain the consent of the addressees of unsolicited e-mail communications for direct marketing purposes. Depending on the national law, with respect to unsolicited commercial communications by means other than e-mail, the controller may have to give data subjects only an opportunity to object, for instance, by the implementation of an opt-out mechanism.

Further, the E-commerce Directive stipulates that Member States permitting unsolicited commercial communication by electronic mail (opt-out) are to ensure that "such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient."[54] This transparency requirement is aimed at facilitating the functioning of appropriate filtering mechanisms.[55] Moreover, the E-commerce Directive requires that Member States take measures to ensure that service providers that send unsolicited commercial communications by electronic mail, consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications may register.[56]

Right to Confidentiality

The Directive also prohibits any processor or any person, acting on behalf of the controller or processor and who has access to personal data, from processing such data except pursuant to instructions of the controller (unless it is required by law). Such a prohibition is aimed at ensuring that the processor, controller or their representative process data in a confidential manner.

8. Technical and Organizational Measures

Member States must require that the controller implements "appropriate technical and organizational measures" to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, especially where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. In implementing such measures, the technology available as well as the costs of implementing the measures should be considered. The measures must ensure a level of security appropriate to the risks represented by the processing and the nature of data to be protected. Consequently, the requirements will be stricter for sensitive data than for non-sensitive data. In the context of medical telematics applications, the security principles contained in Recommendation R (97)5 of the committee of Ministers of the Council of Europe[57] is intended to offer practical guidance for establishing an adequate security policy (e.g. control of transport, control of data introduction, control of utilization, etc.). Of course, since technology evolves, any security measures should be revised and updated regularly.

If data processing is carried out by a processor on behalf of the controller, Member States must require that (1) such processor provide sufficient guarantees in connection with the technical security and organizational measures governing the intended processing, and (2) the controller ensures compliance with such measures. In addition, a contract or legal act between the processor or the controller must govern the data processing carried out by such processor and must stipulate that (1) the processor may only act on instructions from the controller, and (2) the processor must implement the technical and organizational measures required to protect personal data (the parts of the contract referring to such measures and relating to data protection must be in writing).

Security of processing is believed to be essential to protect personal data against misuse by third parties gaining unauthorized access to a system. The controller may incur liability under national legislation implementing the Directive if insufficient security measures are taken. Research has shown that unauthorized access to personal data takes place mostly within the organization that controls the data. A 1998 Computer Security Survey by the Belgian institute CLUSIB[58] showed that 30% of computer crime has an external source, 24% has an unknown source, and 46% occur within the victim's organization. To address internal security breaches, firms are well advised to adopt a privacy policy and a code of conduct binding the employees.[59]

9. Prior Notification

The controller or his representative must notify the data protection authorities before carrying out any fully or partly automatic processing operation, or any

set of such operations intended to serve single or multiple purposes. At a minimum, at least the following information must be provided to such authorities, (1) the name and address of the controller or his representative, if any; (2) the purpose(s) of the processing; (3) the description of the category or categories of data subjects and the data or the categories of data relating to them; (4) the recipients or categories of recipients to whom such data may be disclosed; (5) any proposed transfer of data to third countries; and (6) general description of the measures taken to ensure the security of the processing (to allow a preliminary assessment of the measures taken).

In addition, a public register of processing operations must be established by each Member State, and Member States must provide a procedure pursuant to which changes to the aforementioned information is to be notified to the data protection authorities. Member States, however, may provide for the simplification of, or exemption from, notification for the following categories of data processing and under the following conditions.

First, when taking into account the data to be processed, the categories of processing operations are unlikely to adversely affect the rights and freedoms of data subjects. In this case, the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subjects, the recipients or categories of recipients to whom the data are to be disclosed and the length of time the data are to be stored, must be specified. For example, the Italian data protection legislation exempts from the notification requirement data processing carried out by small enterprises, for the management of museums, libraries, exhibitions, and for organization of other cultural and sportive activities.[60]

Second, a simplified notification procedure is allowed, if pursuant to the national law of the relevant Member State, the controller appoints a personal data protection official responsible, in order to ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. This personal data protection official must be responsible (1) for ensuring the application of the national laws implementing the Directive in an independent manner and (2) for keeping a register of processing operations carried out by the controller which contains the information set forth in paragraphs 1 through 5 above.

Third, simplification of notification is possible if the processing of personal data involves only the keeping of a register which according to the law is intended to provide information to the public and is open to consultation. Finally, a simplified procedure is allowed also if the processing is carried out by a non-profit organization with a political, philosophical, religious or trade union aim, in the course of its legitimate activities and with appropriate guarantees, and relates solely to members or persons in contact with that organization and data are not disclosed to third parties without the consent of the data subject. In addition, Member States may require also that certain or all non-automatic processing operations be notified to the authorities or that such processing be subject to simplified notification.

Following receipt of a notification from the controller (or a data protection official, who, in case of doubt, must consult the authorities), data protection authorities must determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and ensure that such operations are examined prior to the start thereof. In connection with this assessment, the authorities may prohibit certain processing operations or impose additional restrictions.

10. Transfer of Personal Data to a Third Country

Conditions to Transfer

Under Chapter IV of the Directive, the transfer of personal data to a third country may take place only if that third country ensures an "adequate" level of protection. The transfer of personal data to a third country is not permitted, unless one of the exceptions is met, if such third country is deemed to ensure an inadequate level of protection. The adequacy of the level of protection is to be assessed "in the light of all the circumstances surrounding a data transfer operation." More specifically, the following factors must be considered: (1) the nature of the data; (2) the purposes and duration of the proposed processing operation(s); (3) the country of origin and country of final destination; (4) the rules of law, both general and sectoral, in force in the third country in question; and (5) the professional rules and security measures of such third country.

Transfers of personal data to third countries offering an inadequate level of protection may, on a case by case basis, be prevented. If a Member State considers that a third country does not ensure an adequate level of protection, it must inform the Commission thereof. If the Commission confirms that the third country in question does not ensure an adequate level of protection, the member state concerned must take the necessary measures to prevent any transfer of data to that country. The Commission will then enter into negotiations with the third country, with a view to remedying that situation. If, on the other hand, the Commission finds that a third country does ensure an adequate level of protection, the Member State concerned must comply with the Commission's decision.

Exemptions

By way of derogation from the transfer prohibition, the Directive provides that personal data may be transferred to a country with an inadequate level of

protection if one of six conditions are met. First, transfer may proceed if data subjects have given their "unambiguous consent" to such transfer. "Unambiguous consent," which is not required to be in writing, may be deemed to require that the data subject be made aware of the implications of the transfer and any risks involved. In addition, it may require that the data subject be provided with the information required by Article 10 of the Directive. This provision stipulates that at least the following information should be provided to the data subject (a) the identity of the controller and of his representative, if any; (b) the purposes of the intended processing; and (c) any further information such as the recipients of the data, the existence of the right to access and the right to rectify the data concerning him and any other necessary information. To avoid potential problems, it would be advisable for companies to obtain and document the consent of the data subjects to the transfer of data outside the EU.

Second, data may be transferred to any country if the transfer is necessary in order (i) to perform a contract between the data subject and the controller or to implement precontractual measures taken in response to the data subject's request, or (ii) to conclude or perform a contract, which is concluded in the interest of the data subject, between the controller and a third party.

Third, such transfer is also permitted if the transfer is necessary or required by law for important public interest reasons, or for the establishment, exercise or defense of legal claims (this may allow discovery in connection with US litigation).

Fourth, the transfer is legitimate if it is necessary to protect the vital interests of the data subject or if the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions" required by law are satisfied.

Finally, transfer is permitted if the relevant data protection authorities authorize the transfer of personal data based on the controller agreeing to provide "adequate safeguards" to protect the privacy and fundamental rights and freedoms of individuals and the exercise of their corresponding rights. Adequate safeguards may result from the application of contractual clauses. The Commission or other Member States may object to an authorization granted by a national data protection authority on justified grounds (e.g. protection of privacy and fundamental rights and freedoms of individuals). In this case, the Commission takes a decision at European level, and member States must comply with it.

EU/US Safe Harbor Arrangement

As discussed above, in principle, personal data may be transferred only to non-EU countries that offer "adequate" data protection. The Commission is authorized to determine whether the protection offered by a particular country meets this adequacy requirement. Because the US uses a sectoral approach that largely relies on self-regulation rather than comprehensive legislation, it is uncertain whether the US offer adequate protection. To reduce this uncertainty, the US Department of Commerce ("DOC"), in consultation with the Commission, has prepared so-called "Safe Harbor Privacy Principles" for the protection of personal data transferred from the EU to the US (the "Principles"). The aim of the Principles is to offer "clear and practicable guidance to US organizations" to enable them to comply with the adequacy requirement laid down in the Directive. Companies choosing to adhere to the Safe Harbor Principles would be deemed to provide adequate privacy protection within the meaning of the Directive.

Negotiations between the DOC and the Commission on the Safe Harbor arrangement were concluded in March, 2000, and agreement was reached on a set of Principles. While the negotiations on the Safe Harbor proposal were on-going, the EU agreed not to interrupt the flow of personal data to the US,[61] and agreed to condone such transfers until the Safe Harbor arrangement is finalized. The Safe Harbor Principles were issued by the DOC on July 21, 2000, and have been incorporated into a formal Commission Decision of July 28, 2000.[62] Member States were required to ensure that the decision was implemented 90 days after notification.

Scope of Application

The scope of application of the Safe Harbor arrangement is broad. The DOC indicates that the Principles are "intended for use solely by US organizations receiving personal data from the EU for the purpose of qualifying for the Safe Harbor and the presumption of 'adequacy' it creates." The draft Principles clarify that they "are not a substitute for the national provisions implementing the Directive in situations where those national provisions apply."

The Principles cover the transfer of any personal data from EU to US,[63] including personal data collected in the context of an employment relationship. Thus, a US company that receives employee information from a EU-based company under the Safe Harbor arrangement may disclose it to third parties, or use it for different purposes (e.g. non-employment related purposes, such as marketing), only in accordance with the so-called 'Notice and Choice' Principles described below. Moreover, an employee's refusal may not be used to restrict employment opportunities or take punitive action against the employee concerned. However, only "identified records" (apparently not including "identifiable" data) concerning employees are considered to raise privacy concerns, and "statistical data relying on aggregate employment data and/or the use of anonymized or pseudonymized data" are excluded from the scope of application of the Principles. Since the Federal Trade Commissioner

has no jurisdiction in the labor area, enforcement would rely on the cooperation of US organizations with data protection authorities in the EU (see Section 14, below).

The Principles apply also to clinical trial data. Such data may be used for future specific uses (e.g. further scientific research activities) if the data subject's consent has been obtained. In addition, it may be used for unanticipated future medical and pharmaceutical research if the data subject was so informed, unless the use is not consistent with the purpose for which the data was originally collected or to which the data subject has consented subsequently.

Organizations are entirely free to apply the Principles. To benefit from the Safe Harbor arrangement, organizations must (1) comply with the Principles, (2) self-certify publicly and state in their relevant published privacy policy statements that they do so, and (3) subject themselves to the jurisdiction of the Federal Trade Commissioner under Section 5 of the Federal Trade Commission Act – which prohibits unfair or deceptive acts or practices affecting commerce – or that of another statutory body that will ensure compliance with the Principles.[64] The US Department of Commerce will maintain a public list of organizations that have self-certified their adherence to the Principles and fall within the jurisdiction of the government bodies specified below. With respect to procedural arrangements, organizations may qualify for the Safe Harbor in one of four ways, i.e. (1) by joining a self regulatory privacy program that adheres to the Principles, (2) by developing their own self regulatory privacy policies provided that they conform with the Safe Harbor Principles, (3) for organizations subject to "statutory, regulatory, administrative or other body of law" that effectively protect personal privacy, by self-certification to DOC; (4) once model contracts have been authorized by the Commission and the Member States, by including substantive privacy provisions in written agreements with parties transferring data from the EU to the US. An organization is considered to comply with the Principles as soon as it notifies to DOC the public disclosure of its commitment to the Principles, and the identity of the body to whose jurisdiction it is subject.

The EU Privacy Working Party has criticized the fact that the DOC does not check beforehand whether an organization meets the criteria set out above. Moreover, it questioned the reliability of the list of self-certified organizations, arguing that an organization could adhere to the principles for one year, and subsequently withdraw from the Safe Harbor arrangement. According to the EU Privacy Working Party, self-certification could be problematic in the context of a merger or take-over (e.g., of an online business) if a firm adhering to the principles is taken over by, or merges with, an organization that does not qualify for Safe Harbor.[65] In response to the Working Party's objections, the Commission has requested that the DOC or its designee publish any proper and final adverse determinations pertaining to non-compliance with the

principles by a Safe Harbor organization or to other events that might bring to an end an organization's participation in the Safe Harbor, such as a takeover or a merger.

2. Substantive Principles

The Safe Harbor Principles with which US organizations must comply to be considered as offering an adequate level of protection are discussed before. It should be noted here that the Safe Harbor Principles, apply to the data once they have been transferred to the US. Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the US.[66] The EU Privacy Working Party has noted that "data controllers established in the EU are subject to the national provisions implementing the Directive, and the same would normally apply where personal data are collected directly from individuals in the EU by a US organization that makes use of equipment situated on the territory of a Member State."[67] The Working Party seems to suggest that the obligations under the Directive, including the obligation to inform, apply when personal data is collected in the EU by means of the internet. This point is discussed further in Section 12, below.

Notice

An organization must inform data subjects about (1) the purposes for the collection and use of their data, (2) how to contact the organization in order to make inquiries or file complaints, (3) the types of third parties to which it discloses their data; and (4) the choices and means an organization offers data subjects for limiting the use and disclosure of such data. This information must be clear and conspicuous when the data subject is first asked to provide personal information to the organization or as soon as is practicable, but in any event "before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization, or discloses it for the first time to a third party."

The Safe Harbor obligation to inform the data subject is not identical to the information obligation under the Directive. It is doubtful, for instance, whether the term "consent" has the same meaning as set forth in Article 2 (h) of the Directive. Uncertainty exists also as to the meaning of the term "third party" (e.g. is a direct marketing company that has contractual relations with an internet service provider a third party?). It has been argued that where the Safe Harbor Principles are unclear, they should be interpreted in such a way that they comply with the Directive's "adequate level of protection standard." This standard, however, is too vague to provide much guidance. In accordance with the pertinent international law,[68] the text of the Safe Harbor Principles should be deemed decisive. Accordingly, the Safe Harbor Principles do not

require that data subjects be informed about the categories of data concerned, the existence of the right of access, and the right to rectify data concerning them, as required by the Directive.

Choice

Data subjects must have the option to choose (opt out) whether and how their personal information is to be (a) used for a purpose which is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the data subject, or (b) disclosed to third parties, where disclosure is for a purpose other than the purpose for which it was originally collected or subsequently authorized by the data subject. Individuals must be provided with "clear and conspicuous, readily available, and affordable mechanisms" to exercise such choice. The choice principle permits that personal data are processed for any purpose as long as the data subject has not opted out. The EU's legitimacy test does not have to be met to qualify for Safe Harbor. This interpretation is consistent with the concept of individual autonomy, which requires that privacy rights may be waived.

With respect to sensitive data (i.e., data "specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual"), data subjects must be given an "affirmative or explicit" (opt in) choice if data is to be (1) used for a purpose other than that for which it was originally collected or subsequently authorized by the data subject through the exercise of the opt-in choice, or (2) disclosed to a third party. Also, organizations must treat as sensitive any information received by a third party if such party so considers it. The Safe Harbor definition of sensitive data is narrower than the Directive's definition, which refers to "revealing" and not "specifying." For instance, information about an individual's use of a pharmaceutical product may not be deemed sensitive data under the Safe Harbor Principles, although it will be regarded as sensitive under the Directive. Accordingly, such data could be processed for direct marketing purposes under the Safe Harbor Principles without prior consent.[69]

Onward Transfer

Personal data may be disclosed by an organization to third parties only if such organization complies with the principles of notice and choice described above. Where an organization intends to transfer personal data to a third party that has not provided the data subject with choice, the organization may transfer such data to such third party only if it ascertains that the third party (1) subscribes to the Principles, (2) is subject to the Directive, (3) is subject to another adequacy finding, or (4) the organization enters into a written agreement with the third party requiring the third party to provide at least the same level of protection required under the relevant Principles.

If the aforementioned requirements are satisfied by an organization, such organization shall not be held responsible – unless agreed otherwise – if a third party to which it transfers data processes such data in a manner that is contrary to any restrictions or representations, unless the organization knew or should have known that the third party would process data in such way and it did not take reasonable steps to prevent or stop that processing.

Security

Organizations that create, maintain, use or disseminate personal data must take reasonable precautions to protect such data from loss, misuse, unauthorized access, disclosure, alteration and destruction. The Safe Harbor Principles do not provide any further guidance on the nature and level of security that is required.

Data Integrity

As a general principle, a personal information must be "relevant" for the purposes for which it is to be used. In particular, an organization may not process personal data in a way that is incompatible with the purposes for which it was collected or subsequently authorized by the data subject. In addition, an organization should take reasonable steps to ensure that the data is accurate, complete, current and reliable for its intended use.

Access

Data subjects must (1) have access to their personal data, and (2) be able to correct, amend, or delete inaccurate data, unless the burden or expense of providing such access "would be disproportionate to the risks to the individual's privacy," or where the rights of persons other than the data subject would be violated. The procedures for obtaining access are not further specified. In a trans-Atlantic context, providing adequate access may not be without problems.

While access under the Directive is a right, under the Safe Harbor Principles, it is merely an interest, to be weighed against the controller's legitimate interests. The DOC has indicated that the circumstances under which access can be denied must be limited and specific reasons must be provided. The DOC sets forth some exemptions in FAQ 8.5, which cover, for instance, processing for research and statistical purposes.[70] Further, the EU Privacy Working Party has stressed that cost considerations are relevant to determining the conditions under which this right may be exercised but can not be a condition to the right

itself. It would appear entirely appropriate, however, for a controller to require that a data subject reimburse the cost of providing access, in particularly where the cost are significant and a data subject requests access frequently.

Enforcement

Enforcement of the Safe Harbor Principles has been a contentious issue. The EU believes that it is very important that the Safe Harbor Principles be enforceable against the organizations adopting such principles and that data subjects have recourse against such organizations. The draft Safe Harbor Principles require, at a minimum, the following mechanisms: (1) readily available and affordable independent recourse mechanisms pursuant to which (a) a data subject's complaints and disputes are investigated and resolved by reference to the Principles, and (b) damages are awarded where the applicable law or private sector initiatives so provide, (2) procedures to verify that the attestations and assertions made by businesses about their privacy practices are true and that such practices have been implemented as described, and (3) obligations to remedy problems arising out of failure to comply with the Safe Harbor Principles by organizations announcing their adherence to them and the consequences of such failure to comply. Examples of ways to comply with the aforementioned requirements are: (1) compliance with private sector privacy programs incorporating Safe Harbor Principles into their rules and including effective enforcement mechanisms described above, (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution, or (3) commitment to cooperate with data protection authorities in the EU or their authorized representatives. The latter would be the only feasible option for the transfer of employment data. Accordingly, European employees will have to address complaints about violations of their data protection rights that occurred in the US – if they constitute a breach of the Principles – to the national authorities in the jurisdiction where they work. US organizations participating in the Safe Harbor and handling employment data will have to commit to cooperating in investigations and complying with the decisions of data protection authorities in the EU.[71]

The DOC will note any persistent failure to comply in a public list of organizations self-certifying their compliance with the Principles. It will determine also which organizations are no longer assured Safe Harbor benefits. In any event, these enforcement principles are in addition to the requirement that self-regulatory efforts must be enforceable under Section 5 of the Federal Trade Commission Act or similar statute.

The EU Working Party is of the opinion that the enforcement regime is weak, in particular with respect to the link between alternative dispute resolution (ADR) and the injunctive powers of the Federal Trade Commissioner to enforce ADR

bodies' decisions, or challenge these decisions. It is also concerned that the enforcement for employment data relies only on the cooperation with data protection authorities in the EU. To address such concerns, Article 3 of Commission Decision C (2000) 2441 states that the competent authorities in the Member States may exercise their powers to suspend data flows to an organization that has self-certified its adherence to the Principles implemented in accordance with the FAQs "in order to protect individuals with regard to the processing of their personal data when (1) the FTC or the US Department of Transportation or an "independent recourse mechanism"[72] has determined that the organization is violating the Principles implemented in accordance with the FAQs, or (2) there is substantial likelihood that the Principles are being violated. Under these circumstances, according to the Commission, there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to remedy the issue, and the continuing transfer would create an imminent risk of grave harm to data subjects. However, before the competent authorities in the Member States prohibit further transfer, they must have made reasonable efforts under the circumstances to provide the organization with notice and an opportunity to respond.

Limits to Safe Harbor Application

Adherence to the principles may be limited (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulations, or case law that create conflicting obligations or explicit authorizations, provided that such non-compliance is limited to the extent necessary to meet "overriding legitimate interests, and (c) if the effect of the Directive or Member State law is to allow exceptions or derogation, provided that such exceptions or derogation are applied in comparable context of EC legislation.

These limitations provide some much needed flexibility in an otherwise rigid system. They will hopefully ensure reasonable application and interpretation of the principles when conflicting interests are at stake.[73] In any event, organizations are requested to implement the principles "transparently" to enhance privacy protection.

11. Self-Regulation

This section briefly reviews self-regulation, in particular with respect to online privacy. It discusses first the role of codes of conduct under the EU regime, and then focuses on the research regarding online privacy conducted by the US Federal Trade Commission.

Codes of Conduct

As noted in the Introduction, the Directive provides only a general framework for the protection of personal data. Considering that much of the Directive's effectiveness depends on the implementation mechanisms used, the Directive requires that Member States and the Commission encourage the drawing up of codes of conduct, which should contribute to the proper implementation of the national provisions adopted pursuant to the Directive. In particular, Member States must provide that trade associations or other bodies representing other categories of controllers be able to submit draft or amended national codes to national data protection authorities to ascertain compliance of these national codes with national provisions adopted pursuant to the Directive. Draft Community codes may be submitted to the European Commission's Working Party on the Protection of individuals with regard to the processing of personal data.[74]

In parallel, dialogues between various bodies interested in data protection issues have focused on whether there is a role for standardization in support of the Directive.[75] The thinking is that European standards would offer organizations processing personal data clear and practical guidelines on how to meet the legal requirements set forth in the Directive.[76] However, contrary to the so-called "new approach Directives," the Directive does not make any explicit reference to standardization. Data protection standards could have a technical character and cover self-regulatory aspects. In any event, broad consensus between the parties affected by data protection, including industry, consumers, would be necessary for a voluntary standard to have widespread acceptance.

FTC Privacy Online Report

Unlike the EC, the US thus far has relied primarily on self-regulation to deal with online privacy issues. Since 1995, the US Federal Trade Commission (FTC) has been monitoring the state of online privacy and the efficacy of industry self-regulation. In May 2000, it issued a Online Privacy Survey to the US Congress. This Survey reviews the nature and substance of US commercial Web sites' privacy disclosures, and assesses the effectiveness of self-regulation.[77] The survey shows that an increased number of web sites post a privacy statement. The FTC reviewed also nature and substance of these privacy disclosures against the fair information practice principles of notice, choice, access, and security.[78] It found that 20% of 335 randomly chosen web sites implement, at least in part, all four fair information practice principles.

As to adherence to industry primary self-regulatory enforcement initiatives, so-called "online seal programs," the FTC noted an increase of sites enrolled in these programs, but concluded that the self-regulatory initiatives have not been sufficient. Because such efforts alone cannot ensure that the online marketplace as a whole will comply with the standards adopted by industry leaders, the FTC recommended that Congress enact legislation to ensure, in conjunction with self-regulatory programs, adequate protection of consumer privacy online. Despite the increase in self-regulation initiatives and their effectiveness, the FTC believes that detailed regulatory standards are required. The effectiveness and desirability of such standards is not beyond doubt. The enforcement of regulatory requirements would pose a challenge, and would require an enormous bureaucracy. More importantly, requiring that all web sites offer exactly the same privacy policies would restrict competition as to privacy and limit consumer choice. This, of course is also one of the major adverse consequences of the EU's data protection regime.

12. Processing of Personal Data over the Internet

Scope of the Directive's Application Revisited

The Directive is deemed to cover any processing of personal data falling under its scope, irrespective of the technical means used. Accordingly, the Directive fully applies to the processing of data over the internet.[79] As discussed in Section 5, above, the Directive applies to processing (a) carried out in the context of the activities of an establishment of the controller on the territory of a Member State, and (b) when the controller is not established on Community territory, but makes use of equipment situated within the territory of a Member State. Pursuant to one of Recitals of the Directive, an establishment on the territory of a Member State, implies the effective and real exercise of activity through stable arrangements.[80]

The internet makes it hard to apply the "use of equipment" test and to localize the processing of personal data. The physical location of the server is not generally accepted as the decisive criterion for determining the applicable law. Accordingly, Recital 19 of the E-commerce Directive defines the place of establishment of a company providing services via an internet web site as "not the place at which the technology supporting its web site is located or the place at which its web site is accessible, but the place where it pursues its economic activity." The same definition will likely be deemed to apply under the data protection Directive. If, for instance, a French book shop sells books online, the French data protection law applies since the business has a physical address in France. Airplane tickets sold via the internet by a German subsidiary of an English parent airline company, will trigger the application of German data protection legislation, even if the server hosting the web site of the German enterprise is located in the UK or in Latin America.

In addition, the Directive will likely be deemed to apply to controllers not established in the EU, but processing data submitted over the internet by data

subjects in the Member States. These controllers would be considered to make use of "equipment" in the Member States. Indeed, at least some Commission officials interpret the concept of "using equipment" very broadly. These Commission staffers consider that the flow of data via the internet from individual consumers located in Member States to companies located outside the EU falls within the Directive's scope. In one of the replies to Frequently Asked Questions on the Commission's web site, the Commission states that "it would be illogical and without legal justification to exempt such means of transfers [through the internet] of data from the scope of the [D]irective." The approach applied in traditional commerce, namely a business actively seeking customers in another country subjects itself to that other country's laws, is believed to support its view, although the concept of "actively seeking customers" takes on quite a different meaning in the context of the internet. The Working Group intends to release guidance on the application of the Directive to the internet. More specifically, the current unofficial view at the Commission appears to be that there is interaction between an internet user in the EU and the web site outside the EU that such internet user is visiting, and, accordingly, there is "use of equipment" in the EU by the person in control of the web server.[81] Although the ECJ has the authority and jurisdiction to interpret the application and scope of the Directive, it has not yet heard any cases on the Directive's scope, and no cases are scheduled to be heard by the ECJ on this subject.

The broad interpretation of "use of equipment," however, is not only impractical, but also inconsistent with the transfer provisions set forth in the Directive. If a US company uses a server located in the EU to host its web site, the Directive would apply, even if no data of EU nationals are processed. Although the location of the processing is not relevant under the establishment test of Article 4 (1) (a), it is relevant under the "use of equipment" test of Article 4 (1) (c). Furthermore, under this broad interpretation, the rules concerning transfer of personal data to third countries would be rendered superfluous, since the Directive would apply fully to every controller from the moment the information is collected over the internet. This would be so, because cables or interconnection materials located in the EU are needed to realize the connection between a PC situated in the EU and a web site outside the EU. The broad interpretation of "use of equipment" is therefore inconsistent with the Directive's transfer regime. A teleological interpretation of Article 4 (1) (c) of the Directive would avoid this inconsistency.[82] Pursuant to this interpretation, this provision is aimed at protecting EU data subject against circumvention the Directive's regime by moving the processing outside the EU.[83] Without the use of equipment test, processing would fall outside the Directive's scope. Conversely, if there is no circumvention of the Directive's regime by EU firms, a non-EU company operating a web site outside the EU does not fall under the Directive, even if EU nationals submit personal data

to the web site. In this case, the company is a mere passive recipient of information, and the transfer of personal data is effected solely by the data subject. However, if a non-EU controller actively gathers data in the EU, he might fall under the Directive, if the data so gathered indeed constitute personal data (see Section 3 above).[84]

Unfortunately, the EU Privacy Working Party's report on internet privacy does not adequately clarify the geographical scope of the Directive with respect to online applications. In respect of the "use of equipment" requirement, the report states that "(w)hile the interpretation of the notion of "equipment" or "means" has given rise to debate about their extent, *some examples* undoubtedly fall within the scope of application of Article 4." (emphasis supplied). This would be the case, the Working Party opines, when personal information is actively collected by a non-EU controller, making use of the cookie mechanism. As explained in Section 3, above, cookies do not necessarily contain personal data. In the preliminary conclusions section, the Working Party's report provides without further clarification that "[t]he European data protection legislation has to be applied to data collected using automated or other equipment located in the territory of the EU/EEA."[85] It thus remains unclear whether and when the Directive applies in a cross-border internet context, and the Working Party seems to endorse an ad-hoc approach.

National laws implementing the Directive are inconsistent in their application of the Directive to the internet. In the Netherlands and Italy, it appears that the national data protection laws would not apply to the processing of data submitted by EC nationals to non-EU based companies over the internet.[86] In the United Kingdom and France, however, it is unclear whether this situation would be covered by the data protection legislation. In France, recent decisions of the data protection authority suggest that the French data protection laws apply to anyone collecting personal data from France, including the submission of personal data by an internet user in France.[87] Under the United Kingdom Data Protection Act, it is not clear whether the equipment used by the internet user (i.e. the computer, telephone lines, etc.) will be treated as equipment used in the United Kingdom for processing data.[88]

Telecommunications Directive

As noted in the Introduction, Directive 97/66, which supplements the general data protection Directive[89], establishes specific legal and technical provisions for the telecommunications sector.[90] Since the internet is deemed to be a "network of computers open to all," thus forming "part of the telecommunications sector," Directive 97/66 applies to the processing of personal data over the internet. In particular, as regards unsolicited commercial communications, which includes electronic mailing, this Directive leaves Member States the choice

as to whether unsolicited e-mails for purposes of direct marketing should be subject to the consent of subscribers of the telecommunications service (so-called opt-in rule) or should not be allowed only in respect of those subscribers who have indicated that they do not wish to receive unsolicited e-mails (so-called opt-out rule).

As noted in Section 8, above, to address specific privacy matters arising from the internet and other forms of electronic data transfer, the Commission has proposed a new Directive intended to replace the existing Telecommunication Privacy Directive.[91] The new Directive would set forth technologically neutral privacy legislation for all electronic communications. Specifically, it would cover publicly available electronic communications services in public communication networks throughout the Community, including the internet.[92] Personal data processing in private networks (e.g. an intranet) would fall outside the new Directive and be covered solely by the general Data Protection Directive. The new Directive would apply to "traffic data," even if they do not constitute personal data under the data protection Directive, and thus have a broader scope of application.[93]

The proposed Directive would apply to "electronic communications services," which is not further defined. Recital 7 of the proposed Directive states that "it is necessary to separate the regulation of transmission from the regulation of content." This suggests that only access and network providers would fall within the scope of the draft Directive. Internet service providers would appear to be covered by the proposed Directive only insofar as they act also as access providers. They would fall under the general data protection Directive if they operate merely as content service providers.

Under the new Directive, the provider would be required to erase or anonymize traffic data[94] relating to subscribers and users upon completion of the transmission. However, traffic data that are necessary for the purposes of subscriber billing and interconnection payments may be processed up to the end of the period during which the bill may lawfully be challenged or payment pursued. Traffic data may be used for the marketing of the provider's own electronic communications services, without the individual's consent. The proposal would permit also that they be used for the provision of value added services, if the subscriber's consent has been obtained. It imposes a specific obligation to inform. In addition, it imposes security requirements, which may vary in function of the state of the art and the cost of implementation. Finally, it would ensure confidentiality of communications, especially in the context of internet-telephony.

Electronic Commerce Directive

The EU recently adopted a Directive on certain legal aspects of electronic commerce in the legal market, known as the Electronic Commerce Directive.[95]

With regard to data protection issues related to e-commerce, this Directive expressly clarifies that the general Data Protection Directive, and the specific Directive 97/66 on data privacy in the telecommunications sector, are fully applicable to Information Society services (i.e. internet services, shopping, electronic mailing, etc.)[96] This means that the implementation of the E-commerce Directive must be in line with data protection law and principles. In particular, as far as data protection is concerned, the national law applicable to a company responsible for the processing of personal data will continue to be that of the country of establishment. Also, the e-commerce Directive does not prevent Member States from requiring companies to seek prior consent for commercial communications.

EU Working Party Report on Internet Privacy

In November 2000, the EU Privacy Working Party issued a report on online privacy. This report is aimed at providing an integrated approach to online privacy, and interprets and applies the relevant provisions of the Directive, the Telecommunication Privacy Directive, and the previous Working Party opinions. The Working Party aims at creating a base for harmonized policy standards, and offering guidance for the interpretation of the relevant EU directives. The Privacy Working Party points to the growing amount of personal data processed over the internet, mainly for direct marketing objectives. It asserts that internet users are not sufficiently aware of the invisible processing of their personal data, which would affect the fair balance between the privacy of the internet user and the economic interests of the sellers. The report emphasizes also the responsibility of the software industry, and calls for privacy-friendly products.

In its report, the Working Party makes a number of recommendations with respect to on-line privacy policy. First, the Working Party stresses that "adequate means are [to be] put into place in order to ensure that the user gets all the information he/she needs to make an informed choice." Further, it opines that "although having a privacy policy posted on the web site is a good way of providing general information to the public, it is necessary to provide information to the data subject from which the data are being collected, in a simple and accessible way *each time* that data are collected, e.g. in the same screen where he/she has to fill in his/her data or through a box prompt."[97] (emphasis supplied) Many on-line service providers indeed will want to implement fair information policies, but does fairness require that the data subject be informed *each time* data are collected, even if he already consented to regular collection of his data? Once data subjects are adequately informed, "(i)t is then up to the individual to make use of the means that are available to him/her to ensure the respect of his/her rights, and possibly to make clear that he/she will not accept services or products that are not in compliance with the

existing legal framework."[98] Although this recommendation is badly worded, the Working Party seems to suggest that the data subject's consent alone would suffice, which is an excellent recommendation, but it is inconsistent with the Directive's legitimate processing and other requirements.

Second, the report observes that compliance with the data protection legislation can be guaranteed only if "data controllers can rely on a coherent and co-ordinated interpretation and application of the European data protection rules."[99] A consistent and coherent interpretation and application of the Directive indeed is essential. But the Working Party's report does not help to achieve this objective. It sets forth overbroad and often vague guidelines for interpretation and application, and fails to state reasons for its positions. Accordingly, it is unlikely that the report will be of much help to data controllers or national authorities.

Third, the Working Party recommends that use be made of privacy compliant, privacy friendly and privacy enhancing technologies. The report states that "[t]hose involved in the design and development of(. . .) technical tools are encouraged to consult the national Data Protection Authorities about the existing data protection legal requirements."[100] New privacy enhancing technology is being developed by entrepreneurs, and will likely be able to address many privacy concerns. To encourage these developments, the government should provide clear and unambiguous interpretations of the law. The Working Party's recommendation that a system of certification marks be set up for privacy compliant products should be taken up by the EU. Relatedly, to encourage the development of innovative privacy enhancing schemes, government authorities should treat appropriate contractual privacy guarantees (e.g. anonymization of data by encoding, where the encoder agrees not to decode) on a equal footing with technical protection measures.

In addition to these recommendations, the Working Party's report suggests that effective means of enforcement of legal and technical requirements (e.g. P3P, PET's, etc.) be guaranteed. It suggests also that national authorities set up self-monitoring schemes to encourage self-regulation. They are advised also to promote privacy labeling schemes. In respect of the latter, the Working Party announces that it "intends to take action in this field in order to ensure in particular that privacy labels are granted to web sites which are in line with European data protection legislation."[101] If participation in an approved scheme is treated as an irrebuttable presumption of compliance with the data protection law, this would help to reduce the legal uncertainty that currently surrounds the Directive. Approval by one national authority should permit a data controller to operate the approved scheme throughout the EU without having to verify compliance with each country's national law.

International Law on Extra-Territorial Jurisdiction

Under international law, the scope of a state's jurisdiction[102] over persons or events outside its geographic boundaries is a heavily debated issue. In the *Lotus Case*, the Permanent Court of International Justice held that territorial jurisdiction is a fundamental element in the international legal system and that a State "should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty."[103] The Court in *Lotus* recognized the "objective territoriality" principle by ruling that acts of criminal negligence occurring on a French ship on the high seas could be adjudicated and punished under Turkish law as such negligence had effects within the Turkish jurisdiction. In the US, the Court in *United States v. Aluminum Co. of America*[104] (hereinafter referred to as "Alcoa") adopted the objective territoriality principle of the *Lotus Case* and made the "effects test" part of US law. In *Alcoa*, Judge Learned Hand held that the Sherman Act (antitrust) applied to a foreign agreement that was intended to affect US trade and did so, even though such agreement was between foreign companies and was performed entirely on foreign soil. The *Alcoa* "effects test" raises the question under international law whether any, even insignificant or negligible, effects suffice. In the EU, the ECJ held in the *Woodpulp Case* that the "effect of the agreements and practices on prices announced and/or charged to customers on resale of pulp within the EEC was therefore not only *substantial but intended*, and was the primary and direct result of the agreements and the practices (emphasis added)."[105] Therefore, the EU would appear to require that the effects be substantial.

In the US, to establish personal jurisdiction in internet cases, courts have used the minimum contacts test, which requires "certain minimum contacts" or ties with the state of the forum "such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice."[106] Thus far, although courts are split as to whether the operation of a World Wide Web server is enough to subject a person to personal jurisdiction, courts have rejected the proposition that the operation of a web site subjects a person to personal jurisdiction.[107]

If the effects test were applied by the ECJ or national courts to determine whether the Directive is applicable to data processed on World Wide Web Servers in the US, the result would be unpredictable. Some courts might take the view that a World Wide Web Server is passive and merely provides the information to internet users that visit it, and other courts might argue that such server directs its information worldwide, and therefore, would subject itself to the application of the Directive when a data subject in Europe connects to such server. As discussed above, the Working Party[108] is apparently of the opinion that sufficient contact occurs between the data subject and a World Wide Web Server as it takes the view that the Directive is applicable to data

processing over the internet. The Working Party bases its view on the fact that the data controller "uses equipment" such as computers and phone lines, on the territory of a Member State when a data subject accesses a World Wide Web server. As discussed in Section 12, a broad interpretation of this term is inconsistent with the Directive's transfer regime. In addition, it would likely not be deemed to meet the international law standard of sufficient contact, nor the substantial effects test, which has also been adopted by the European Court of Justice. In the case of web sites operated from outside the EU, both contacts and effects should be regarded as *de minimis*.

13. Remedies and Sanctions

Under the Directive, without prejudice to any administrative remedy before the data protection authorities of the Member State, Member States must provide each person with the right to a judicial remedy for any breach of his rights pursuant to the data protection laws of the relevant member state. Each Member State must also provide that (1) any person who has incurred damages as a result of an unlawful processing operation or any act in violation of the data protection laws of Member States is entitled to compensation from the controller for the damages incurred, and (2) the controller is exempt from such liability, in whole or in part, if he is not responsible for the event giving rise to the damage.

In addition, the Member States must determine the sanctions that will be applicable in the event provisions of the data protection laws are violated. Most Member States' laws impose administrative and criminal sanctions for violations of the national legislation implementing the Directive.

14. Final Observations

With the Data Protection Directive, the EU has adopted a complicated regime for the protection of privacy. The Directive has a broad scope of application, both in terms of subject matter and geographically. Virtually all data relating to a person are subject to this regime. The key definitions of personal data, controller, and processing raise numerous issues when applied to real life situations. The EU Privacy Working Party's attempts to clarify the interpretation and application of the data protection law in the context of the internet have not been successful. In addition to substantive requirements, the Directive also provides for procedures, such as prior notification to the government, and requires agencies to oversee compliance. However, even before the Directive has been implemented by the Member States, it became apparent to the EU that the Directive may not work well in the information age and additional legislation has been proposed to deal with electronic communications. The

cost of the privacy protection regimes thus enacted is significant and this problem is further exacerbated by ignoring cost considerations in implementation and not permitting controllers to charge the full cost to data subjects who invoke their rights. It remains unclear whether this expensive and restrictive regime meets the privacy demands of more than a small minority of citizens.

The Data Protection Directive is believed to be the implementation of the EU citizen's right to "informational self-determination." Although consent is often a necessary condition for lawful data processing, it is not sufficient and additional, non-waivable requirements are imposed. Broad and vague open-ended standards necessitate a balancing of the controller's and data subject's interests in each individual case, even if the data subject's consent has been obtained. Consequently, data controllers are confronted with serious legal uncertainty, and find themselves exposed to the broad discretionary powers of national data protection authorities. The EU Working Party's report on internet privacy at best marginally reduces the government's discretionary power. The discretion granted to the privacy agencies results in ad-hoc regulation that violates the legality principle (i.e. the prohibition on retroactive effect) and is questionable from a viewpoint of democratic principles. Thus, the EU pays lip service to individual autonomy, but in fact empowers government authorities to decide whether data processing should be permitted. Judicial review of such decisions may not be available or be meaningless, where courts are inclined to agree with the agencies determinations in such "technical" matters.

When it comes to the application to the internet, neither the Directive nor the Working Party's report on internet privacy adequately address the pertinent issues and fail to provide reasonable guidance, which further reduces legal certainty in cyberspace. The territorial scope is particularly problematic. Data protection authorities have suggested that the Directive applies to any web site operated by any service provider anywhere in the world, using a server anywhere in the world, if the web site receives data from EU nationals. It applies also to individuals anywhere in the world if there is "use of equipment" in the EU's territory, even if no data of EU residents but only data of non-EU residents are concerned. The EU has not tried to justify this globalist, extraterritorial approach, which is inconsistent with EU and international law. In addition, due to the tendency to interpret the concept of personal data broadly, anonymous web site traffic data may well be deemed "virtual" personal data. This approach is counterproductive because it effectively turns anonymous data into personal data, thus increasing privacy risks. Increased privacy risks arise from the mere increase of the volume of personal data and increased processing of data (e.g. in the context of the data subject's access right) that result directly from the Directive's application.

The basic assumption on which the Directive is based is that ruthless capitalists have an interest in harming the privacy of the consumer, and only

the government is able to protect consumers against these threats. The reality, however, is that businesses are interested in having adequate means to service customers and develop the market at reasonable costs, *and* meet consumers' privacy expectations. Both consumers and business want legal certainty, and autonomy. Vague and inflexible legislation raises costs significantly, has perverse effects, and consequently does not even protect the consumer. Consumers indeed are harmed positively where they are required to purchase, included in the price of goods and services they acquire, a privacy protection regime that they do not want. On the internet, reasonable contractual safeguards and a fair privacy policy agreed between the parties involved are not only the most effective way to enhance privacy, they are also the only way to meet consumers' diverging demands for privacy protection. Initiatives such as P3P should therefore be strongly encouraged by the government. A market-based approach will result in an optimal balance between privacy and other interests in the information age.

Notes

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, COM (2000) 385 final, 2000/0189 (COD).

2. In June 1999 in Cologne, the European Council decided to draw up a charter of fundamental rights of the European Union. A group of ex-political and academic leaders has been entrusted by the European Council with the task of drafting this charter.
3. The right to privacy is worked out in more detail in Recommendations of the Committee of Ministers of the Council of Europe. See, for example, Rec. R(99)5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet – Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways (adopted on February 23, 1999, at the 660th meeting of the Ministers' Deputies).
4. See Section 10.
5. Data Protection News on the http://europa.eu.int/comm/dg15/en/media/dataprot/news/2k-10.htm web site. In all these countries, however, draft legislation implementing the Directive is currently either being discussed within the government or pending before the Parliament. In Recommendation 1/2000, of February 3, 2000, the European Commission's Working Party on the Protection of individuals with regard to the processing of personal data has expressed its regret that not all the Member States have implemented the Directive in time, as existing divergent regimes imply legal uncertainty. Therefore, the Working Party recommends these Member States to take urgently the necessary measures for implementing the Directive.
6. Marleasing SA v. La Commercial Internationale de Alimentacion SA, C-106/89, 1990.
7. Marshall v. South-West Hampshire Area Health Authority, C-152/84, 1986.
8. Wagner Miret, C-334/92, 1993; Dori v. Recreb Srl, C-91/92, 1994.
9. Francovich & Bonifaci v. Italy, C-6/90 and C-9/90, 1991. Pursuant to Francovich, Member States are liable if the following three conditions are satisfied: (a) the directive must grant rights to private parties; (b) the content of such rights must be inferable from the directive's provisions; and (c) there must be a causal link between the damage suffered by private individuals and the Member State's failure to take action.
10. BverfG., EUGRZ, 1983, p. 588.
11. Art. 4 of the former French Data Protection Act sets forth such a test : "Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale."
12. Strictly speaking, the Directive does not apply to "anonymous" data, but the term anonymous is interpreted restrictively. There is a continuum between clearly personal data and anonymous, non-traceable data; many categories of data fall in between these two extremes. A Belgian draft Royal decree distinguishes explicitly between personal data, "coded data," and anonymous data. "Coded data" are personal data that is rendered anonymous (e.g. by an intermediary), but not in an irreversible way. The Belgian Data Protection Act applies also to coded data.
13. The ability to relink the data to specific individual will often be necessary, e.g. in case of longitudinal research. Evidently, a broad interpretation of the notion of "personal data" may make such research programs more cumbersome and more expensive.
14. See Recitals 14 and 15, Directive.
15. The Explanatory Memorandum to Recommendation (97)5 of the Committee of Ministers of the Council of Europe suggests that cost "should not be taken into account to determine identifiability, since informatics are evolving rapidly."
16. The EU Privacy Working Party has opined that in case a false identity is provided by an internet user, indirect identification is possible via the IAP logbook. It is doubtful whether this would often be the case; it would be impossible where access is granted free of charge, a user does not log in via a telephone line, and no personal data has been obtained by the free access provider. Moreover, this interpretation may not respect the 'likely reasonable means' requirement of the Directive's Recital 26. EU Privacy Working Party, Working Document "Privacy on the Internet - An Integrated EU Approach to Online Data Protection" adopted November 21, 2000, p. 12.
17. EU Privacy Working Party, Working Document adopted November 21, 2000, p. 20.
18. The EU Privacy Working Party suggests, however, that in such a case indirect identification would be possible by reasonable means. Working Document, adopted on November 21, 2000, p. 9.
19. "Chattering" refers to the data sent by the user's browser to the web site he visits. Such data may include the software used to communicate, the computer programs that the user has installed on his computer, the referring page, and the language of the user.
20. See Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the internet Performed by Software and Hardware, Adopted by the Working Party on February 23, 1999.
21. Cf. footnote no. 16.
22. Some authors consider a bank account number, a shopping profile, a holiday reservation, or fingerprints 'personal data.' See Cullen International, A Business Guide to Changes in European Data Protection Legislation, Kluwer International, 1999, p. 26.
23. Article 2(d) of the Directive.
24. In some situations, not involving the internet, the definition of "controller" also raises difficulties. When one person determines the purposes and another determines the means, who is controller? For instance, a parent company may decide on purposes but leave the means decision to its subsidiaries. The authorities tend to treat both as controllers in such a case.

25. International Working Group on Data Protection in Telecommunications, "Data Protection on the Internet: Report and Guidance", adopted at the 20th meeting in Berlin, November 19, 1997.
26. Article 6, Directive 97/66/EC, determines the conditions under which traffic and billing data may be processed.
27. Article 6 (b), Directive 95/46/EC.
28. For instance, Article 4 of the Belgian Data Protection Act does not specify the purposes that are deemed legitimate. See also Article 9 of the Italian Data Protection Act and Article 7 of the Dutch Data Protection Act.
29. Depoorter, W.F., De Vulder, K., Schrans, G. and Vergotte, M., Telecom & Internet – recht in beweging, Mys & Breesch, Gent.
30. The Open Profiling Standard is intended to provide for secure transmission of a standard profile of personal data.
31. Dinant, J.M., Platform for Privacy Preferences (P3P): How for can P3P Guarantee the Respect of the Data Protection Directive Requirements?, jmdinant@fundp.ac.be.
32. Opinion 1/98, adopted by the EU Working Party on June 16, 1998.
33. Ibid.
34. Cfr. Article 9 of the Directive.
35. As noted in the Introduction, the processing of personal data via telephone, fax, e-mail or internet is regulated also by the specific Directive 97/66 on the protection of privacy and personal data in the telecommunications sectors, which supplements the Directive. Directive 97/66 will be briefly discussed in part 13, in relation to its application to data processing over the internet.
36. De Terwangne, C. and Louveaux, S., Data Protection and Online Networks, MMR, 1998, p. 451 et seq.
37. Dickie, J., "Internet and Electronic Commerce Law in the European Union, Oxford Hart Publishing, Oxford – Portland Oregon, 1999, p. 58.
38. Rigaux, F., La protection de la vie privée et des autres biens de la personnalité, Bruxelles, Bruylant, 1990; Poullet, Y., Thunis, X., and Leonard, Th., La vie privée – une liberté parmi les autres, Travaux de la faculté de droit de Namur, Tome 17, Bruxelles, Larcier, pp. 231–277.
39. Law No. 675/96.
40. Ley Organica No. 15/99, in force since January 14, 2000.
41. However, the data subject must be granted the possibility to object to such processing, as discussed in paragraph 8.
42. See Recital no. 32.
43. "Sensitive data" includes "personal data revealing racial or ethnic origin, political opinions, religious beliefs, trade-union membership, and the processing of data concerning health or sex life."
44. Member States may, for reasons of "substantial public interest," provide exemptions, in addition to the ones set forth above, from the prohibition of processing sensitive data. If they do so, they must notify the Commission of the additional exemptions. In addition, Member States may determine conditions under which a national identification number or any other identifier of general application may be processed.
45. According to one group of authors, "a person's personal data cannot be processed for any hidden or secret reason. The data subject must be made aware of the uses of data relating to him, either when the data is collected, or when it is recorded, or when it is first disclosed", A Business Guide to Changes in European Data Protection Legislation, ed. Cullen International, Kluwer Law International, 1999, p. 41 This would follow from the "fair processing" requirement set forth in Article 6 (1) (a) of the Directive.

46. These techniques allegedly violate the fairness requirement. In the US, two federal class actions have been filed claiming that online advertisement companies violate federal laws by tracking consumers' browsing habits without prior consent. Such practices would constitute a violation of the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. It, however, is unclear whether the ECPA applies to the internet, since it was intended to protect spoken conversations. See www.thestandard.com.
47. The web site of the Commission Nationale de l'Informatique et des Libertés (CNIL) explicitly discloses what data of a user are collected. See, www.cnil.fr.
48. Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, adopted by the Working Party on February 23, 1999. In this document, the Working Party provides for some examples of proper information practices: (1) In the case of browser software, on establishing a connection with a web server (sending a request or receiving a Web page) the user is informed of what information is intended to be transferred and for what purposes. (2) In the case of hyperlinks sent by a web site to a user, the user's browser should reveal the hyperlinking to the user. (3) In the case of cookies, the user should be informed when a cookie is intended to be placed, stored or sent by the internet software. The message should specify, in understandable language, which information is intended to be stored in the cookie and, for what purpose, as well as the duration of the cookie.
49. Some Member States have adopted a fixed fee regime. See, e.g. for Belgium, Royal Decree no. 4, September 7, 1993 fixing the amount and conditions of a prior access charge.
50. See also Prins, J.E.J. and Berkvens, J.M.A., Privacyregulering in theorie en praktijk, Kluwer, 2000, p. 285. In Belgium, no specific right is granted to employees and the law merely reiterates the Directive's general provision without any further specification (Article 14, Belgian Data Protection Act).
51. A Business Guide to Changes in European Data Protection Legislation, op.cit., p. 71.
52. Directive 1997/66/EC, art. 12.
53. Proposal for a Directive of the European Parliament and of the Council, COM (2000) 385 final, 2000/0189 (COD).
54. Article 7, Directive 2000/31/EC.
55. It would enable software or other devices to filter out commercial communications. These techniques are believed to work properly only if the address of the sender is known.
56. Article 7, 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, Official Journal L178, July 17, 2000, pp. 1–16.
57. Recommendation R (97)5 of the Committee of Ministers to Member States on the Protection of Medical Data, adopted by the Committee of Ministers on February 13, 1997 at the 584th meeting of the Ministers' Deputies.
58. CLUSIB is an acronym for "Club de la Sécurité Informatique Belge."
59. Article 23 of the Directive provides that "(1)Member States shall provide for that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. (2) The controller may be exempted from his liability, in whole or in part, if he proves he is not responsible for the event giving raise to the damage." It is not clear whether this article intends to shift the burden of proof to the controller. A Business Guide to Changes in European Data Protection Legislation, op. cit, p. 91.

60. See Article 7 of Law No. 675/96.
61. Letter, dated November 15, 1999, from US Ambassador David L. Aaron to US organizations requesting comments on the newly posted draft Safe Harbor Principles.
62. Commission Decision of July 28, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issues by the US Department of Commerce, C (2000) 2441.
63. Personal information gathered for publication, broadcast or other forms of public communication of journalistic material, and information found in previously published material disseminated from media archives, is not subject to the Principles.
64. Note that organizations are not required to apply the Safe Harbor Principles to personal information in manually processed filing systems.
65. Opinion 7/99 of December 3, 1999, http://www.ita.doc.gov/td/ecom/Euletter27JulyHeader.htm.
66. FAQ's DOC nr. 14.
67. Opinion 7/99 on the Level of Data Protection provided by the Safe Harbor Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce, adopted December 3, 1999.
68. Article 31, Vienna Convention on the Law of Treaties, May 23, 1969.
69. The Working Party has opined that choice can a basis for legitimate processing only if it is based on adequate information. Opinion 7/99, adopted on December 3, 1999.
70. See, http://www.ita.doc.gov/td/ecom/menu.html.
71. Failure to cooperate with the EU data protection authorities and failure to comply with the Principles will be actionable as a deceptive practice under Section 5 of the FCT Act or other similar statute.
72. This term is defined under letter (a) of the Safe Harbor Enforcement Principle as "readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide."
73. In Opinion 7/99 of December 3, 1999, the EU Privacy Working Party stressed that to ensure legal certainty and non-discrimination in respect of other adequacy findings, it is recommendable that more precise criteria for, and concrete examples of, such exceptions and limitations be provided and that their impact be given proper consideration. The Working Party recommended a distinction between options and obligations: adherence to the principles should only be limited to the extent necessary to comply with statutory or regulatory obligations, but not as a result of options available under US law, since this would result in a serious weakening of the principles.
74. See, for example, the EFPIA Code of Conduct for the Pharmaceutical Industry on the Processing of Personal Data in Research and Development. See also the "Privacy and Confidentiality" requirements of the Dutch Model Code of Conduct for Electronic Commerce, www.ecp.nl. For a discussion, see Docter N. and Van Bellen, A., Model Code of Conduct for Electronic Commerce, EDI Law Review, 1999, pp. 198–200.
75. A seminar on the role of standardization in data privacy was held on March 23/24, 2000, under the umbrella of European standardization bodies CEN/ISSS.
76. A standardized mechanism for data protection, for example, is applied in Canada.
77. The survey of was based on a list of the busiest U.S. commercial sites on the World Wide Web. The groups of sites studied were (1) a random sample of 335 Web sites and (2) 91 of the 100 busiest sites (the "Most Popular Group").
78. These principles were described in the FTC's 1998 Report Privacy Online.
79. See Working Document on the processing of personal data over the internet of the Commission's Working Party on the Protection of individuals with regard to the processing of personal data (the "Working Party"), February 23, 2000.
80. Recital 19, Directive 95/46/EC.
81. According to unofficial sources, the Commission considers the interaction to occur between the hard disk and the cookies produced as a result of the internet user's visit to the web site.
82. Terwangne, C. and Louveaux, S., op. cit., p. 455. This view is confirmed by the EU Privacy Working Party. Working Document, adopted on November 21, 2000, p. 27.
83. Explanatory Memorandum, COM (92) 422 final – SYN 287, p. 13.
84. Terwangne, C. and Louveaux, S., op. cit., p. 455.
85. Working Document of the EU Data Protection Party, adopted on November 21, 2000, pp. 27–28.
86. Italian Law No. 675/96, which implements the Directive, clearly defines its scope of application to the processing of personal data carried out on Italian territory. Therefore, one could argue that the processing of personal data submitted via internet by individuals located in Italy to companies located outside Italy takes place outside Italy and, as a consequence, falls outside the scope of Law No. 675/96. Similarly, the Dutch proposed act which would implement the Directive, would appear to apply only to companies with a presence in the Netherlands, and the processing is done "in the context" of the activities of that presence.
87. See CNIL, 17th Activity Report 1996, p. 106.
88. Data Protection Act, 1998.
89. Directive 97/66/EC is a *lex specialis* that takes precedence over the general data protection Directive 95/46/EC.
90. The Commission issued a Working Document for revision of Directive 97/66. Such revision may address data protection relating to internet and e-commerce.
91. 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, COM (2000)385 final, 2000/0189 (COD).
92. In Opinion 7/2000, the EU Privacy Working Party rejects this exception on the ground that private networks are gaining an increasing importance in every day life and communications, e.g. in the context of work. Processing of personal data in connection with the delivery of services using public communication services and networks, such as the content of broadcasting transmission and information society services, is also not covered by the proposed new Directive. Opinion 7/2000 on the European Commission 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 sector of July 12, 2000 COM (2000) 385, adopted November 2, 2000.
93. The definition of "traffic data" is "*any data processed in the course of or for the purpose of the transmission of a communication over an electronic communication network.*" Traffic data is personal data if it can be related to an identified or identifiable person (e.g. via the intermediary, the access or network provider). In addition, Recital 15 of the proposed Directive suggests that the *right to correspondence* should be protected when subscribers are processing data within electronic communication networks. The right to correspondence does not fully cover the same substance as the right to privacy. The right to correspondence reflects the level of trust in a certain medium. Both rights are protected by article 8 §1 of the European Human Rights Convention. Traffic and personal data are deemed to be worthy of protection, since content and medium in a digital network are entangled in a complex manner. The distinction between the right to correspondence (medium) and the right to privacy (content) may explain why legal

entities also fall under the scope of the Telecommunication Privacy Directive.

94. As noted, "traffic data" means any data processed in the course of, or for the purpose of, the transmission of a communication over an electronic communications network. This term includes location data generated during the transmission of a communication, as well as "navigation data" (URLs), which might reveal an individual's personal interest (see EU Privacy Working Party, Opinion 7/2000, adopted on December 3, 1999).
95. The European Parliament in second reading did not propose any amendment to the common position adopted by the Council on February 28, 2000. Accordingly, in accordance with the co-decision procedure, the Directive is definitively adopted. Member states will have 18 months to implement the Directive following its publication in the EU Official Journal, which is expected shortly.
96. Recital 6(a), Electronic Commerce Directive.
97. EU Privacy Working Party, Working Document, November 21, 2000, p. 89.
98. Ibid., p. 90.
99. EU Privacy Working Party, Working Document, adopted on November 21, 2000, p. 90.
100. Ibid., p. 90.
101. Ibid., p. 91.
102. With respect to extra-territorial enforcement measures, controversy has arisen in the field of economic regulation, especially antitrust regulation. The US effects doctrine (as described above in *Alcoa*) provoked strong reactions from a large number of foreign governments as the enforcement jurisdiction of a US court went beyond the application of the objective territorial principle by allowing US courts to take action when activity abroad has consequences or effects within the US which are contrary to local legislation. Brownlie, Ian, Principles of Public International Law (1990).
103. France v. Turkey, 1927 PCIJ, ser.A, no. 10.
104. 148 F.2d 416 (2d Cir. 1945).
105. According to an EU commentator, under the "effects test" applied in the EU, the following conditions must be satisfied: (1) the effects produced must be substantial; (2) the effect must be direct; (3) it must be foreseeable that the agreement or the performance of such agreement will have effects in the territory of the state; (4) it is not necessary that the parties intended to have effects on the territory, except where the object of the contract is anti-competitiveness (irrespective of its eventual effects), and (5) it is not necessary that the agreement or the performance of such agreement be held invalid (*condamné*) by the jurisdiction in which it was entered into or performed.
106. International Shoe Co. v. State of Washington et al., 326 US 310, 316.
107. Wille, D., Personal Jurisdiction and the Internet Proposed Limits on State Jurisdiction over Data Communications in Tort Cases, Kentucky Law Journal, 87 Ky. L.J. 95, 102.
108. The Working Party is an advisory body which consists of (1) a representative of the national data protection authorities of Member States responsible for monitoring and enforcing the application of the national data protection legislation, (2) a representative of the authority(ies) for Community institutions or bodies, and (3) a representative of the Commission. The Working Party was created by Article 29 of the Directive.