EU DATA PROTECTION REGULATION AND AUTOMATIC PROCESSING OF INFORMATION ON THE INTERNET

Thomas Olsen

University of Southampton, 2001/2002
Faculty of Law

A dissertation submitted in partial fulfilment of the requirements for LLM (European Law) by instructional course

Preface

This dissertation constitutes the final requirement for the LLM degree in European Law by the University of Southampton for the academic year of 2001/ 2002. The paper was written during four hectic summer months from June to September 2002. The word limit of a dissertation makes it difficult to find the balance between depth and width, and my feeling is that I only have scratched the surface in this complex field. However, I hope my approach in this paper is able to illustrate some of the emerging issues of data protection in the information society. The paper is as far as possible updated to September 2002. I would like to thank my supervisor, Dr. Stephen Saxby, for a great year in Southampton and for his guidance and suggestions when writing my dissertation. I would also like to thank Snorre Grimsby and Espen Wahlstrøm for fruitful discussions on technical issues related to the paper.

Thomas Olsen
September 2002

Table of contents

1 Introduction

This paper will assess the EU's initiatives and approach on data protection on the Internet. As the Internet is becoming significant in all aspects of our lives it is of great importance to assess to what extent the EU Directives 95/46/EC[1] and 97/66/EC[2] apply to and are capable of regulating processing of personal data on the Internet. The Directives represent the most significant data protection legislation in the world, and they set a high level of data protection. All around the world states are developing data protection laws and international enterprises are trying to adhere to the different levels of data protection regimes. The next few years will indicate whether EU data protection legislation will be the benchmark for future developments in this area, or whether the EU's ambitious goals will prove too optimistic.

Data protection is considered an increasing priority among policy makers, mainly because the area is regarded as a key element for ensuring respect for the individual's privacy, ensuring a functioning economy and the wish to promote e-commerce. The collapse of the optimistic wave of dot-com companies has partly been explained by customers' lack of confidence in the use of Internet services. However, the concepts of "privacy" and "data protection" are highly debated. The rationale and legal basis for data protection legislation in Europe are not necessarily the same in other parts of the world. Within the EU data protection is regarded as a fundamental human right, which has been strictly regulated through legislation. In the USA, however, there is only sector legislation and its rationale is first of all to protect the citizens from being monitored by the state, not so much by commercial interests.

The paper addresses issues related to automatic processing of information on the Internet. By automatic processing I mean data that are processed automatically when using services on the Internet. This includes first of all transaction data that can be collected by various actors like Telecommunication Operators, Internet Access Providers or Internet Service Providers. Some of the disclosure and collection of transaction data is necessary for the functionality of the Internet. However, transaction data may also be collected and used illegally or illegitimate to build profiles on user's behaviour and preferences. Automatic processing includes such techniques as cookies, browser chattering, spyware, web beacons, etc. Illegitimate automatic processing of data may also take place on the user's machine, e.g. by the use of cookies and spyware. The threat posed by spyware is that it cannot only disclose transactional data, but also report to web servers on use of software or content stored on the user's machine. Characteristic for automatic processing on the Internet is that collection or disclosure of data takes place without the user's knowledge or informed consent. Further, it takes place automatically and may make it possible to monitor use of individual computers (and its users) over time in great detail by collecting a huge amount of transaction data.

Automatic processing of information is challenging the legal regulation of data protection in a number of ways. Instead of assessing a specific topic more thoroughly I have chosen to look into some of the issues that illustrates some of these challenges. It has not been possible to go into specific problems related to national implementation of the Directives. Hence, the main focus here is to analyse the EU Directives on the selected issues. As there is very little case law related to the interpretation of the Directives, the recommendations and opinions of the Working Party on the Protection of Individuals

[1] 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, 24 October 1995, (OJ L 281, 23.11.1995 p. 31).

[2] Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997 (OJ L 24, 30.1.1998, p. 1). A proposed Directive (Directive concerning the processing of personal data and the protection of privacy in the electronic communication sector), COM (2000) 385 is intended to replace Directive 97/66/EC. According to the proposals explanatory memorandum is the proposal not intended to create major changes to the substance of the existing Directive, but merely adapts and updates the existing provisions to new and foreseeable developments in electronic communications services and technologies.

with regard to the Processing of Personal Data (hereinafter "the Art 29 Working Party") will be of great importance. The Art 29 Working Party is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission (Art 29, Directive 95/46/EC). It issues recommendations and opinions on issues relevant to both Directives.[3] The responsibilities of the Art 29 Working Party includes examining questions covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures (Art 30, Directive 95/46/EC). Practice from the national data protection authorities shows that the opinions and recommendations from the Art 29 Working Party are weighted heavily in the authorities own decisions when interpreting the national measures implementing the Directives. Hence, documents adopted by the Art 29 Working Party will also be given much attention and weight in the legal analysis in this paper.

Section 2 will give an assessment of the origin and rationale of data protection laws. This may help explain the main reasons why there have been so much debate and conflicts on data protection laws, especially between the EU and the USA. As explained below, this difference in approach to data protection has a significant impact on the EU data protection scheme and its application on the Internet.

In section 3 I will assess how and where automatic processing takes place on the Internet. Information about the user's computer and his behaviour on the Internet can be logged in a systematic way on the Web server and on the user's computer. Automatic processing can take place without the user's knowledge and informed consent and may allow the creation of "clicktrails" and profiles about the Internet user. The EU Directives apply only to "personal data", thus a core question regarding information collected through automatic processing is whether the information can be linked to an individual.

Section 4 is an analysis on determining the international application of EU data protection. Particularly important is the question on how national data protection law pursuant to the Directives applies to Web pages established outside the EU/EEA. This section will also assess concrete requirements laid down in the Directives and the possibilities of enforcement in cases where rights pursuant to the Directives are not respected.

Section 5 discusses whether standardisation could enhance data protection on the Internet. It is the author's view that standardisation of data protection would make it easier for developers of software and e-commerce companies to comply with different regional and national data protection regimes. The consumer would also benefit from standardisation because most of the privacy enhancing technologies today do not comply with the EU Directives. Further, section 5 assesses the significance of taking the EU Directives into consideration when technical standards, software and privacy enhancing technologies are developed. Finally, the impact and effect of the Directives greatly depend on awareness among consumers about the rights pursuant to the Directives and the possibilities of enforcement.

Outside the scope of this paper are issues on information security. Information security is one of the fundamental principles in all data protection regimes. However, it would be too difficult to give a fair presentation of the subject within the limits of this paper. Neither will important issues on encryption, technologies for authentication and anonymity be assessed in any detail. Developments in these areas are considered as essential for safe and reliable services on the Internet, but would require a broader approach that would lead beyond the limits of this dissertation.

[3] I will in the following refer to the papers issued by the Art 29 Working Party by reference to their number (e.g. WP 37 refers to publication 37). See bibliography for full title and number.

2 Data protection

2.1 The development of data protection laws

The spread of national data protection legislation in the 1980s was fuelled by concerns for the informational privacy rights of individuals and the need to ensure free flow of data for trade. The European Convention on Human Rights and Fundamental Freedoms, adopted by the Council of Europe in 1950, includes a right to respect for the private and family life of individuals, their home and correspondence (Art 8). As computerisation developed there were concerns that the growth of information technology, with its ability to produce extensive data files on individuals and to transmit and match personal data, would undermine the respect for the privacy of individuals upheld by Art 8.[4] As laws protecting individual rights in the face of the new technologies developed in Europe, their growth was accelerated by the passage of two international instruments. In 1980 the Organisation for Economic Co-operation and Development (OECD) adopted Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[5] In the following year the Council of Europe opened the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Treaty 108)[6] for signature by national governments. Countries that wished to ratify Treaty 108 had to have in place national data protection legislation, which met the standards of the Treaty. Many, but not all, of the Member States of the European Community passed data protection legislation.

The differences between the various laws and the absence of legal protection in some countries led to concerns that data protection would present trade barriers and accordingly the European Commission took initiatives to achieve ratification of Treaty 108 by Member States. These did not prove sufficient. The Commission therefore moved to introduce harmonisation measures. Two data protection Directives were passed. The first was a general directive, 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 second was a sector specific Directive which applies in addition to the general directive, Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector.[7]

The Directive 95/46/EC is the most comprehensive and complex international instrument on data protection today. It is also likely to constitute the most important point of departure for new data protection initiatives, both inside and outside the EU, not least because Art 25(1) of the Directive prohibits the transfer of personal data to countries outside EU/EEA if they do not provide “adequate” levels of data protection. The important Safe Harbour agreement between the EU and US is a result of this principle.

Despite the Directive’s adoption, the CoE Convention and OECD Guidelines are still important because they have influenced, and /or embody, the basic principles of most countries’ current data protection laws, along with the EC Directive itself.[8]

[4] Initiative on Privacy Standardization in Europe, final report, 13 February 2002. (IPSE report).
[5] The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter termed “OECD Guidelines”), adopted by the OECD Council on 23.9.1980.
[6] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 28.1.1981. ETS no 108.
[7] Will be replaced by COM (2000) 385. See supra n. 2.
[8] See Bygrave, Lee A., Phd thesis: “Data Protection Law: Approaching its Rationale, Logic and Limits”, 1999 Faculty of Law, University of Oslo, Part I, Chapter 2.

2.2 Background and rationale for EU data protection legislation

2.2.1 Rationale and legal basis of EU data protection laws

According to Art 1, the Directive 95/46/EC's main aim is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data". The recitals emphasise the importance of basic human rights, notably that of privacy, in the face of technological and economical developments.[9] As such, it reflects and reinforces the gradual incorporation of law and doctrine on human rights, particularly as embodied in the ECHR, into the EU legal system. Worth mentioning is also that The European Court of Human Rights (ECHR) and the European Commission of Human Rights (ECommHR) in Strasbourg have over time demonstrated increasing willingness to read basic data protection principles into Art 8 of the ECHR.

On 7 December 2000 the Charter of Fundamental Rights of the European Union was proclaimed. In the Charter, data protection was significantly recognised as an autonomous right, and this achievement can be regarded as the final outcome of the Union's long-standing commitment in this area. Art 8[10] of the Charter has brought about three basic changes that regard the overall institutional framework: firstly, personal data protection has been recognised to be an autonomous, fundamental right of individuals, to be kept separate from the broader right to respect for private and family life referred to in Art 7; secondly, personal data protection cannot be considered solely and/or prevailingly in economic terms, nor may it be overridden by – albeit important – security requirements; thirdly, the role played by independent supervisory authorities has attained "constitutional" importance, it being expressly referred to as a necessary component in Art 8(3) of the Charter.[11]

In addition to this, economic and social development also figures centrally in the aims of the EC Directive. The Directive's recital (especially recitals 3, 5 and 7) register a concern to promote realisation of the EU's Internal Market, in which goods, persons, services, capital and personal data are able to flow freely between Member States. Underlying these economic concerns are the awareness that much of contemporary economic activity is based on the production and exchange of information in a vigorously competitive private sector.

In furtherance of the concern to promote realisation of the Internal Market, the main function of the Directive is to secure, pursuant to Art 95 (formerly 100a) of the EC Treaty, harmonisation of Member States' respective data protection laws. In accordance with the principle of subsidiarity, EU Member States have been allowed a margin for manoeuvre in implementing the EC Directives. [12] It is assumed in recitals 8 and 9 that implementation of the Directive will lead to an "approximation" of national laws, resulting in "equivalent" levels of data protection across the EU. Recital 9 states that the achievement of such equivalency will make it impossible for Member States to restrict the free flow of personal data to other Member States "on grounds relating to protection of the rights and freedoms of individuals, and in particular to the right of privacy". The Directive strives to bring about a "high" level of data protection across the EU.[13]

---

[9] See e.g. recitals 2, 3, 10 and 11.

[10] "1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority. "

[11] See WP 54, preface.

[12] See further Craig, P. and Debúrca, G.(1998), *EU Law: Text, Cases, and Materials*, Oxford: Oxford University Press, 2nd ed, chapter 7.

[13] See recital 10: "…seek to ensure a high level of protection in the Community". See also recital 11: "give substance to" and also "amplify the principles of the CoE Convention"

2.2.2 Fundamental principles

In essence, the Directive set out clear obligations and responsibilities for the treatment of personal data. Personal data must be processed fairly and lawfully, collection and storing of data should be limited to what is necessary (principle of minimality) and collected personal data should only be processed according to their original purpose (purpose specification). A second aim is the maintenance of transparent processing systems for personal data. This is protected by principles of the data subject's participation and control and principles securing data quality. Further, the Directive provides special protection for sensitive personal data and obligations on each Member State to create an independent national supervisory authority with remedies, enforcement rights and responsibility to keep an effective oversight over the treatment of personal information. The Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, e.g. public security, defence, State security etc. (Art 3(2)).

2.3 Comparison with the USA's approach to data protection

The EU and the USA have very different conceptions of privacy and privacy protection underlying their distinctive privacy regimes. Americans tend to be more trusting of the private sector and the free market to protect personal privacy – fearing more the invasion of privacy from the state not the market.[14] The US legal system treats privacy as a personal property right that may be disposed of as one sees best, rather than an unassailable human right. While the European approach is more proactive, American policy making is more reactive, stepping in to regulate only where problems occur and tailoring specific regulatory solutions. The US government frowns upon the too much federal oversight, arguing that the European top-down approach with its "privacy czars and bureaucracies ...would probably be regarded as a violation of privacy rights by many people in the US".[15]

The US data protection regime has been described as "fragmented, ad-hoc, and narrowly targeted to cover specific sectors and concerns".[16] It has been argued that the US especially is lacking the right to review and enforcement mechanisms. There is no privacy oversight agency in the US. Instead the Office of Management and Budget (OMB) and the Federal Trade Commission (FTC) enforce specific privacy laws. The FTC for example, has oversight and enforcement powers for laws protecting consumer credit information and fair trading practices, but it has no authority to enforce privacy rights, other than those arising from fraudulent or deceptive trade practices.[17]

Self regulation is an important element of the American data protection regime. The high tech industry believes that the bureaucracy lacks the capability to deal with the rapid pace of change and innovation of the information economy. The US business community generally supports a "layered" approach to data protection. Under this form of private-public regulation, publicly announced corporate policies and industry codes of conduct are backed by the FTC and state-level enforcement in response to private civil actions for damages or injunction relief.[18]

2.4 Safe Harbour

As the date for the Directive 95/46/EC implementation neared, it became clear that the EU considered the self-regulating practices adopted in the US, particularly the lack of an official avenue for individuals to address or question misuse or misrepresentation of personal data, as failing to meet the

[14] Long, J William and Quek, Marc Pang, "Personal data privacy protection in an age of globalisation: the US EU safe harbour compromise", Journal of European Public Policy, 3 June 2002, vol. 9, p. 331.
[15] Aaron David, Under Secretary of Commerce, cited in Andrews, Edmund L. "European law aims to protect privacy of personal data", New York Times, October 26 1998, p. A1.
[16] Shaffer, Gregory "Globalisation and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards", 2000, *5 Yale J. International Law 1*.
[17] Long, J William and Quek, Marc Pang, supra n.14, p. 332.
[18] Long, J William and Quek, Marc Pang, supra n. 14, p. 333.

"adequacy" standard on personal data transfers required under Art 25 and that US business faced the threat of an "information embargo".[19]

US industry recognised the lack of an enforcement mechanism as the chief concern of EU officials with US self-regulation.[20] In response, the US government and corporate officials began to participate in business-backed programs such as TrustE[21] and BBBOnline[22]. Under these programs, a third-party "seal of approval" is granted to Web sites that comply with industry standards, but would be revoked should the Web site violate its announced privacy policy. These third-party programs, industry claimed, demonstrated their willingness and ability to hold themselves accountable for violations of their own privacy promises.

Negotiations over the Safe Harbour framework occurred through a series of official meetings and exchange of letters. After numerous exchanges, the two parties eventually agreed that all enforcement would be carried out within the United States, subject to very limited exceptions.[23] Under the agreement, organisations within the safe harbour would be regarded as providing "adequate" data protection, and data transfers to these companies from the EU would continue undisrupted.

Due to the uncertainties associated with the safe harbour compromise may attorneys advise European companies against relying on agreement in the conduct of data transfer with US companies. Instead, they recommend that companies transferring data to the United States obtain the US self-certificate supplemented by a legally binding indemnity.[24]

2.5 Conclusion

This short analysis has shown that the EU and the USA have taken a very different approach to data protection. The rationale and legal basis for data protection is very different and the issue remains controversial. The different points of view will most probably cause great difficulties also in the future. The resistance by USA to raise its data protection standards will in my view be one of the main challenges with regard to giving effect to the data protection Directives. The tension between the EU and the USA is also evident in standardisation activity as will be assessed in section 5. My analysis will show that the influence USA's industry has on standardisation and development on the Internet is more significant than many would think. In section 4 I will assess the concrete requirements stated by the Art 29 Working Party with regard to how Web sites shall handle personal data. The requirements may seem optimistic considering that many of the most used Web services are located in the USA.

---

[19] Long, J William and Quek, Marc Pang, supra n. 14, p. 334.

[20] A report by the Federal Trade Commission in 2000 of the 100 most visited Web sites in the USA revealed a very low standard for data protection. The results showed that only 20 percent of the random sample sites were found to have implemented four commonly used "fair information practices". These are "Notice, Choice, Access and Security". And among the most popular group, only 42 percent did so. Even when the report looked at the percentage of sites implementing the two critical practices of Notice and Choice, only 41 percent of the random sample and 60 percent of the most popular sites provided such privacy disclosures. See http://www.ftc.gov/opa/2000/05/privacy2k.htm

[21] http://www.truste.org/.

[22] http://www.bbbonline.org/.

[23] The finalised safe harbour framework is expressed in a collection of documents that include seven privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision, the exchange of letters between the Department and the European Commission, and letters from the Department of Transportation and Federal Trade Commission on their enforcement powers. See http://www.export.gov/safeharbor/sh_documents.html.

[24] Long, J William and Quek, Marc Pang, supra n. 14, p. 337.

3 Automatic processing on the Internet

3.1 Introduction

Chapter 3 will give a technical analysis of the Internet. By describing relatively deeply who is involved in the normal operation of the Internet and how data is generated and disclosed, this will serve as basis for analysing the potential privacy threats posed by normal use of the Internet.
By analysing how data is processed automatically while browsing the WWW, I will try to explore who has access to what data and whether this data can be regarded as personal data in the sense of the Directives. Personal data willingly disclosed by the person using a Web service (e.g. in forms) will be kept outside this analysis.

It should be emphasised that the Directives only applies to the processing of personal data. If the data is not considered as personal data pursuant to the Directives the data protection regulation is of no relevance. The definition of "personal data" is given in Directive 95/46/EC Art 2(a) and states: "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"). The definition applies also to Directive 97/66/EC and the new electronic communications Directive.[25] The core question is what the requirement of information relating to an "identified or identifiable" person means. Directive 95/46/EC Art 2(a) defines an identifiable person as "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". According to recital 26 of Directive 95/46/EC, account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person.

3.2 Basics

3.2.1 History of the TCP/IP network

The Internet is a network of computers communicating with each other on the basis of the Transport Control Protocol/Internet Protocol (TCP/IP). It is an international network of interconnected computers, which enables millions of people to communicate with one another in "cyberspace" and to access vast amounts of information around the world. Historically the ancestor of the Internet is the ARPAnet military network (1969). The basic idea was to build a trans-US digitised network enabling computers operated by the military, defence contractors and universities conducting defence related research to communicate with one another by the redundant channels even if some portions of the network were damaged in the war.

The network later became more and more open to non-academic institutions and to non-US organisations. In 1990, Tim Berners Lee, working at the CERN in Geneva, designed the first browser and implemented the concept of hyperlink, making the World Wide Web some of us take for granted today possible. Since 1990 a variety of new services and functionalities have been continuously added.

On the Internet, every computer is identified by a single numerical IP address of the form A.B.C.D, where A, B, C and D are numbers in the range of 0 to 255 (e.g. 194.178.86.66).[26]

A TCP/IP network is based on the transmission of small packets of information. Each packet includes the IP address of the sender and of the recipient. This network is connectionless. It means that, unlike the telephone network for instance, no preliminary connection between two devices is needed before

[25] See Directive 97/66/EC (and proposal for a Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector COM (2000) 385 final), Art 1, paragraph 2. Note: while the Directive 95/46/EC only applies to natural persons, Directives 97/66/EC and COM (2000) 385 final) also applies to information regarding legal persons

[26] For more information, see Internet Assigned Number Authority (IANA): http://www.iana.org/.

communication can start. It also means that many communications are possible at the same time with many partners, which is very characteristic for how the Internet functions.

3.2.2 The Domain Name System

The DNS (Domain Name System) is a mechanism for assigning names to computers identified by an IP address. Those names are in the form of <names>.top-level domain, where <names> is a string constituted by one or many sub strings separated by a dot. The top-level domain can be a generic domain like "com" for commercial Web sites or "org" for non-profit organisations, or a geographical domain like "no" for Norway. DNS has to be paid for and companies or individuals wanting a domain name have to identify themselves. Some public tools on the Internet make it possible to retrieve the link between the domain name and the company as well as between the IP address and the domain name. A domain name is not in itself necessary for connecting a computer to the Internet. Domain names are dynamic. One single Internet computer can have one or many domain names – or even none at all – but one specific domain name always refers to one particular IP address.[27]

The current Internet Protocol version 4 (IPv4) is expected to run out of IP addresses as more wireless devices are expected to go on-line.[28] The IP addresses are assigned in Europe through an international procedure to Internet Access Providers who then reassign them to their clients, organisations or individuals.[29] By using a publicly available tool like, for instance, http://www.ripe.net/perl/whois it is possible to identify the party responsible for a particular IP address allocation. Typically, this will be:

1) The manager of a Local Area Network linked to the Internet (e.g. a Small or medium enterprise (SME) or a public administration). In this case, he/she will probably use a fixed IP addressing scheme and keep a list of correspondence between people's computers and IP addresses. If this person is using the Dynamic Host Configuration Protocol (DHCP[30]), the DHCP program will typically keep a logbook containing the Ethernet card number. This unique worldwide number identifies a particular computer in the LAN.

2) An Internet Access Provider (IAP) which has a contract with an Internet subscriber. In this case, the IAP will typically keep a log file with the allocated IP address, the subscriber's ID, date, time and duration of the address allocation. Registering of the number called (and date, time and duration) takes place by the phone company for billing purposes in cases where the Internet user uses a public telecommunications network (mobile or terrestrial phone). [31]

3) The Domain Name Holder, which might be a company's name, the name of the employee of a company or a private citizen.

In these cases, this means that, with the assistance of a third party responsible for the attribution, an Internet user (i.e. his/her civil identity: name, address, phone number, etc) can be identified by reasonable means.

---

[27] Id.

[28] The European Commission expects the current reserve of addresses is expected to run out in 2005. The IPv4 gives only 4.2 billion addresses. The upgraded version (IPv6) of the IP addressing system is currently being developed based on numbers that are 128 bits long. See News.com, 21 February 2002: http://news.com.com/2100-1033-842718.html.
The implementation of IPv6 may raise new data protection issues as all kinds of devices may be given a unique IP-address, but will not be dealt with in this paper.

[29] See for example the Regional Internet Registry in Europe: RIPE, http://www.ripe.net/ripencc/about/regional/index.html.

[30] The DHCP is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses (http://www.dhcp.org).

[31] See also section 3.3.1.

3.2.3 Routers

A router is an important device, which provides routes for TCP/IP networks. This means that the TCP/IP route is dynamic, depending on the failure or overloading of some routers or links. It can also be used as a firewall between an organisation and the Internet. It can especially guarantee that only authorised IP addresses can originate from a particular ISP.

It is important to note that the speed of transmission is the single most valuable criterion for routing in TCP/IP networks. With information circulating at almost the speed of light, it can be more efficient to route TCP/IP packets form London to Madrid via New York if there is a traffic jam in the network in Paris. Some tools allow the net user to know the route between two points, but this can theoretically change every second, even during the transfer of a single Web page.

3.2.4 Proxy servers

A proxy server is an intermediary server between the user and the Internet. It acts as a Web cache, dramatically improving the rate of display of information (e.g. the display of Web pages). Many large organisations and Internet Access Providers have already implemented this solution. Each page, image or logo downloaded from outside by a member of an organisation is stored in a cache on the proxy server and will be instantaneously available to another member of this organisation. Another use of proxy servers is to use it as intermediary to hide the original IP number of the Internet user. This enables anonymous surfing and anonymous re-mailing.[32]

3.2.5 More sophisticated protocols using TCP/IP

Some protocols are designed to provide certain services in addition to TCP/IP. The most widely used protocols are the HTTP (Hyper Text Transport Protocol) used for surfing on the Web, the FTP (File Transfer Protocol) used to transfer files, the NNTP (News Network Protocol) used to access newsgroups and the SMTP (Simple Mail Transport Protocol) and POP3 protocols (to send and receive e-mails).

These protocols are necessary because the TCP/IP protocol only permits the transmission of bulk information from one computer to another. The computer delivering a service is called a server. The computer using a service is called a client. To provide a technical service, both the client and the server use the same protocol (i.e. the same communication rules). The Internet is often referred to as a client/server network. It is important to note that whatever the service used, the TCP/IP protocol is always used by every service mentioned above. This means that every threat to privacy linked to the TCP/IP protocol will be present when using any service on the Web.

3.3 Actors involved in the Internet

3.3.1 Telecommunications Operator (TO)

In Europe, the telecoms infrastructure used to be de facto the monopoly of traditional telecommunications operators. This situation is however evolving. Furthermore, this monopoly is often reduced to the cables or optical fibres, while for wireless communications and emerging technologies like WAP, UMTS, etc, competition is emerging between national carriers.

The traditional Telecommunications Operator is still, however, an important actor since it provides the data communications between the Internet user and the Internet Access Provider (IAP).

The Telecommunications Operator processes traffic data for billing purposes, such as the calling number and its location (for mobiles), called number, date, time and duration of the communication. Internet traffic packets that are transmitted are “wrapped” in several protocol headers (e.g. TCP-header, IP-header and Ethernet-header). These protocol headers are read in every knot (router) a

[32] See EPIC for a good presentation of PETs and privacy tools: http://www.epic.org/privacy/tools.html.

packet passes through, to decide where the packet is to be sent next.[33] A controversial issue is whether traffic data should be kept for enforcement issues and whether is should be possible and allowed to intercept traffic data.[34] In the proposed Directive COM (2000) 385, which will replace Directive 97/66/EC, confidentiality is secured in Art 5. Further, Art 6 states that traffic data relating to subscribers and users processed for the purpose of the transmission of a communication and stored by the provider of a communication network or service must be erased or made anonymous upon completion of the transmission.

3.3.2 Internet Access Provider (IAP)

The IAP provides, normally on a contractual basis, a TCP/IP connection to individuals and organisations.

Individual subscribers using a modem or a terminal adapter (ISDN) will receive a IP address for the duration of his/her connection and this address will usually change the next time he/she dials up. This is called a *"dynamic"* IP address. In the case of a connection by ADSL or cable modem, the IP address may be *"static"*. "Static" in this relation means that the subscriber keeps the same IP address. To be able to obtain a connection, the individual has to conclude a contract and give his/her name, address and other personal data. Typically the user will receive a user identification name (User ID that may be a pseudonym) and a password so that nobody else can use this subscription. At least for security reasons, IAP usually seem to systematically "log" the date, time, duration and dynamic IP address given to the Internet user in a file. As long as it is possible to link the logbook to the IP address of a user, this IP address should be considered as personal data.[35]

Organisations may use dialup connection or a line leased to the company's office, normally provided by the traditional telecoms operator. The connection can also be established via a satellite line or a terrestrial radio system. The IAP will give the IP addresses to the company and use a router to ensure that the addresses are observed.

3.3.3 Internet Service Provider

The Internet Service Provider (ISP) provides services to individuals and companies on the Web. It owns or hires a permanent TCP/IP connection and uses servers permanently connected to the Internet. It will normally offer Web-hosting (Web pages stored on its Web server), access to newsgroups, access to an FTP servers and electronic mail. This involves one or more servers using HTTP, NNTP, FTP, SMTP and POP3 protocols.

IAPs will frequently offer the services of ISPs. This is why the generic term ISP is often used to include both IAPs and ISPs. But, from a conceptual viewpoint the roles are different. Namely, the IAP, being the gate to the Internet, will route all traffic from the Internet subscriber, while the ISP will only be aware of what happens on its servers.

From a technical point of view, it is the presence of servers equipped with protocols that will be decisive in gathering personal data. In the case of HTTP servers generally, a logbook or log file is systematically created by default and may contain all or some of the data present in the HTTP request header (browser chattering) and the IP address. The logbook is standard practice and is created by each server. A closer assessment of the possibilities of the ISP to log information about Internet users will be given in section 3.4.2.

[33] See WP 37, p. 51.
[34] This is issue touches aspects of law enforcement and national security which will not be assessed in this paper. The Council of Europe's Cyber crime convention is a new significant international instrument in this area.
[35] See WP 37, p. 11.

3.4 Privacy risks

3.4.1 Privacy risks inherent in the use of the TCP/IP protocol

There are two characteristics of the TCP/IP protocol, which appear to constitute a potential invasion of privacy. Both data-processing operations are legitimate and in most cases unavoidable for the smooth operation of the Internet. However, the problem is that most users are not aware of the fact that these operations take place. Neither are they aware of available security measures.

1) The route followed by TCP/IP packets is dynamic and follows the logic of performance. In theory, it may change during the downloading of a Web page or the transmission of an e-mail, but in practice it remains largely static. In telecommunications, performance is linked more to the congestion of the network than to the physical distance between telecommunication nodes (routers). This means that the shortest way between two towns located in the same EU country may pass through a non-EU country, which may or may not have adequate data protection.[36] The average Internet user has no reasonable means of changing this route, even if he/she knows which route is followed at a particular moment.

2) Due to the fact that the translation between the Domain Name and the numerical IP address occurs via a DNS server, whose function is to ensure this translation, this DNS server receives, and can keep trace of, all the names of the Internet servers the Internet user has tried to contact. In practice, those DNS servers are mainly maintained by Internet Access Providers.[37]

3.4.2 Privacy risks inherent in the use of high level protocols

HTTP is of strategic importance insofar as it is the main protocol used on the Web and can offer services like electronic mail and discussion forum, which has usually been provided by specialised high-level protocols such as POP3, SMTP or NNTP. The following analysis relates to how ISP can log and monitor the use of services on its servers.[38]

This section focuses on three characteristics which are almost always present because of the way the HTTP protocol is implemented in the most frequently used browsers. A combination of these characteristics can have serious consequences for the privacy of Internet users.

1) Browser chattering
One might think that typing an URL in a browser and pressing enter only transmits information about the IP address of the surfer and the requested page to the current Web server. This is not the case. A lot of information about the users operative system and his installed software is systematically transmitted in the HTTP header while making an HTTP request. This is called automatic browser chattering and is available to the server.[39]

2) Invisible hyperlinks
The use of hyperlinks is the main feature of the Web, which makes it possible to browse from one Web page to another simply by mouse click. What is hidden to the eyes of the common user is that classical browsing software makes it possible for the HTTP request to include a command to download images for inclusion in the HTML page code. These images do not need to be located on the same server as the one that has received the original call for a particular Web page. If a Website includes in its Web page in HTML an invisible link to an image located on the Web site of a cyber marketing company, the latter will know the referring page before sending the advertising banner.

3) Cookies

[36] See WP 37, p. 14.
[37] See WP 37, p. 14.
[38] See comparison between the role of the IAP and the ISP in section 3.3.3.
[39] See the specifications for the HTTP 1.1 protocol: http://www.w3.org/Protocols/rfc2616/rfc2616.html.

Cookies are text files that may be put on the Internet user's hard disk, while a copy may be kept by the Web site. A cookie resides on a user's hard drive and contains information about the individual that can be read back by the Web server that deposited it.[40] A cookie can contain any information the Web site wants to include in it: pages viewed, advertisements clicked, user identification numbers and so on. The cookies can facilitate the surfing of the Internet user since the Web site can identify the user and avoid displaying the same messages more times than necessary. Also, the user will not have to log in more than once. The cookie allows a permanent and unique identifier to be sent systematically with every information request, whereas the IP address remains a relatively weak identifier because proxies can hide it and it is not reliable, due to its dynamic character for Internet users accessing the Internet by modem

These three characteristics must be seen in combination with the fact that when following a retrieved link in a search engine, the keywords typed will be communicated to the Web server hosting the relevant Web page.[41] By combining the browser chattering and invisible hyperlinks, a cyber marketing company can, by default, know all the keywords typed by a particular Internet user into the search engine on which this company is advertising. Through these techniques the company may also know the operative system, software installed, operative system, the user's IP address and the time and duration of HTTP sessions. These data make it possible, if combined with other data available to the company, to infer new data like:[42]
i) The country where the Internet user lives
ii) The Internet domain to which he/she belongs
iii) The sector of activity of the company employing the Internet user
iv) The turnover and size of the employing company
v) The function and position of the surfer within this company
vi) The Internet Access Provider
vii) The typology of Websites currently visited

The combination of browser chattering, invisible hyperlinks and cookies provide the means for invisible profiling of every individual Internet user who uses a browser allowing these functions. This profiling is not "per se" linked to the HTTP protocol, as defined by the W3C.[43] The HTTP 1.1 protocol definition has explicitly drawn the attention of the industry to possible privacy issues while implementing the HTTP protocol.[44]

3.5 Some economic considerations

Direct marketing is one of the major rental activities on the Web. Cyber marketing companies place advertising banners on Web pages, often in such a way that the collection of personal data remains widely invisible to the data subject. Thanks to the use of invisible links in combination with browser chattering and cookies, unknown marketing companies are able to profile Internet users on a one-to-one basis. One single cyber marketing company could send half a billion personalised advertising banners on the Web every day.[45] It is also direct marketing companies that finance many search engines.

By adding an invisible hyperlink to cyber marketing companies on their own Web pages, Web sites (and search engines in particular) will instruct common browsers like Netscape and Internet Explorer to open an independent HTTP connection with the cyber marketing company's Web server.

---

[40] Id.
[41] See WP 37, p. 16.
[42] Id.
[43] The World Wide Web Consortium is a non-profit organisation hosted by Inria (France), MIT (USA) and the University of Keio (Japan). The members of this consortium are notably Microsoft, AOL, Netscape, and Center for Democracy and Technology (http://www.w3.org/Consortium/Member/List). This consortium produces non-mandatory but de facto standardisation intended to guarantee the interoperability of computers on the Internet.
[44] http://www.w3.org/Protocols/rfc2616/rfc2616.html.
[45] See WP 37, p. 18.

The average Internet user is generally unaware of the fact that while typing an URL (Unified Resource Locator), many banners that he/she will see as a result do not originate from the Web site he/she is visiting. Nor are users aware of the fact that, while downloading one ad banner, their browser will systematically transmit a unique ID, IP address, and complete URL of the Web page they are visiting. These data can be merged to build a global profile of an Internet user surfing from one site to another, thanks to the unique ID stored in the cookie.

The capture of user information in on-line environments is considered to have economic and strategic importance. Recent cases confirm the increasing value attached by business to consumer profiles. Lists of customers are being sold or shared, most often through mergers of IT companies which thus increase the detail and number of profiles they can use. Customer data have also been offered for sale when Internet companies go bankrupt.

Additional risks exist when data collected during the surfing activities of Internet users can be linked with other existing information on the same user. The fear of such a connection of personal data concerning Internet users has been very present in the discussion on the merger between Internet advertiser Double Click and market research firm Abacus Direct.[46] 10 States in the USA has recently reach a settlement with Double Click where Double Click promises to make it tracking activities more visible and give consumers access to their online profiles.[47]

3.6 Conclusion

This technical oriented analysis has shown that it is necessary to distinguish between TOs, IAPs and ISPs when exploring potential privacy threats to end users on the Internet. The services offered by these operators are distinct, although some companies provide two or all of them.

A general question, which is relevant to almost all kinds of automatic processing, is whether an IP address can be regarded as personal data pursuant to the Directives. As was described in section 3.2.2, Internet Access Providers and Managers of Local Area Networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically log the date, time, duration and dynamic IP address given to the individual Internet user. If the user logs in on a computer with a personal user name and password there should be little doubt that the use of an IP address can be linked to an individual by reasonable means. However, if more than one person randomly use a computer with a given IP address, e.g. in a household or in an Internet Café, it will obviously be more difficult to link the use of the IP address to one person.

Internet Service Providers (which not acts as IAPs), have not attributed IP addresses to any users and will only be aware of the activity on their servers. In these cases is it more difficult to make a link between an IP address and an individual. It should be noted that it is easier to identify a user using a permanent than a dynamic IP address. But even if the user has a dynamic IP address it is theoretically possible to identify the user. For example through use of advanced techniques like cookies containing a unique identifier[48] and modern data mining systems linked to large databases containing personally-identifiable data on Internet users.[49]

[46] See http://www.epic.org/doubletrouble/.
[47] See press release by NY Attorney General, 26 August 2002: http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html.
[48] E.g. Double Click uses the unique Web browser as an identifier, see http://www.doubleclick.com/.
[49] This is also the general view of the Art 29 WP, see WP 37, p. 21.

4 International application of national data protection legislation

With respect to the Directives' international impact, the attention of most commentators has been directed towards the provisions in Art 25 and Art 26 of the Directive, which attempt to regulate the flow of personal data from States within the EU to other States (so-called third countries).

Nevertheless, as this assessment will show, the rules in Art 4 could have a significant impact on relations between the EU and other countries. By contrast, the drafters of the 1980 OECD Guidelines on data protection were unable to reach agreement on appropriate rules, despite discussing interlegal issues extensively. The same problem appears also to have afflicted the drafters of the 1981 Council of Europe Treaty.[50]

The need to determine whether national law applies to situations with links to several countries is specific neither to data protection, the Internet, nor the EU. It is a general question of international law, which arises in on-line and off-line situations where one or more elements are present that concern more than one country. A decision is required on what national law is to be applied before a solution on substance can be developed.

There are according to Bygrave[51] several complicating factors for determining the relevant national data protection law. Since data protection law straddles the boundaries between public and private law, criminal and civil law it is difficult to firmly place data protection law within any one of the legal categories traditionally employed by the doctrines of private international law. It also complicates attempts to locate and/or assimilate suggested jurisdictional and choice-of-law solutions for the field of data protection within the broader field of interlegal rules. Another complicating factor is the nature of the information systems that data protection law seeks to regulate. As the doctrines of private international law tend to rely on the ability to make link to one geographical location, this has proven more difficult for information systems or for the Internet.

Directive 95/46/EC Art 4 directly addresses this essential question, and reads as follows:

> *National law applicable*
> *1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*
> *(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;*
> *(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;*
>
> *(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.*
>
> *2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.*

[50] Bygrave, L. A., "Determining Applicable Law pursuant to European Data Protection Legislation", *CL & SR*, 2000, volume 16, p. 252-257.
[51] Id.

4.1.1 Principle criterion: the controller established within or outside the Community

The Directive distinguishes between, on the one hand, situations where the cross-frontier elements are confined to EU Member States[52] (or with territories outside the geographical borders of the EU, but where the law of a Member State applies by virtue of international public law[53]) and, on the other hand, situations where the processing involves elements going beyond the borders of the EU[54].

The principal criterion for determining applicable law is the "place of establishment of the data controller", largely irrespective of where the data processing occurs.[55] This is the country of origin principle typically applied in the Internal Market and means that when the processing is carried out in the context of the activities of an establishment of the controller on the territory of one Member State, the data protection law of this Member State applies to the processing. When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down by the respective law of each of the Member States for the processing carried out by them in course of their activities. The justification for the origin principle is that in the Internal Market national data protection laws afford equivalent protection thanks to the harmonisation of data protection rights. Additionally, it is the intention of the Directive's drafters that the problems of applying another Member State' legislation will be obviated by increased cooperation between the various national data protection authorities and increased possibilities for cross-jurisdictional court enforcement of data protection laws.[56]

The situation will be different as regards processing operations, which involves a controller in a third country. The national laws of these third countries are not harmonised, the directive is not applicable in these countries and the protection of individuals with regard to the processing of their personal data may therefore be missing or weak. The country-of-origin principle, which is linked to the establishment of the controller, would not be appropriate to serve the purpose of determining the applicable law.

The EU legislator chose one of the classical connection factors in international law, which is the physical link between the action and the legal system. The directive therefore applies when the controller is not established on Community territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a Member State.

The objective of this provision is that an individual should not be without protection as regards processing taking place within his country solely because the controller is not established on Community territory. This could be simply because the controller is not established on Community territory, but it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law. The directive harmonises Member States' laws on fundamental rights granted to all human beings irrespective of their nationality, it makes no distinction on the basis of nationality or location, and it is not necessary for the individual to be an EU citizen or to be resident in the EU. As emphasised by the Art 29 Working Party, the legislator's decision to submit processing that uses equipment located in the EU to its data protection law thus reflects a true concern to protect individuals on its own territory.[57]

---

[52] Art 4(1)(a).
[53] Art 4(1)(b).
[54] Art 4(1)(c).
[55] WP 56.
[56] See especially Art 28(6) which states that: "Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State. The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."
[57] See WP56.

4.1.2 Determining the place of establishment

Another problem is that, on the Internet, it will often be difficult for a data subject or data protection authority to determine the location of the controller, let alone to work out where the latter is "established". One important issue in this regard is the extent to which a Web site itself may be classified as an establishment pursuant to the Directive. Although it can be argued that "effective and real exercise of activity" (recital 19) can be carried out through a Website (at least if the site is interactive), it would seem difficult to argue that a Web site in itself can satisfy the need for "stable arrangements" (recital 19 again).

The Directive on electronic commerce[58] defines in Art 2(c) an "established service provider" as a service provider who "effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider". Recital 19 in the Directive on electronic commerce state that the place at which a service provider is established should be determined "in conformity with the case-law of the Court of Justice according to which the concept establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period".[59] The recital also states that "the place of establishment of a company providing services via an Internet Web site is 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".

For example: a direct marketing company, which is registered in London and has developed its European wide campaign there, will still be established in London, despite the fact that its Web servers are located in Berlin and Paris.[60]

4.1.3 The term controller

The controller is defined in Art 2(d) as "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". The definition is neutral as regards the point of establishment of the controller. It is comprehensive because all processing must be attributable to one or several controllers.

In cases where controllers are using external expertise to do the processing, the controllers must ensure, through appropriate contractual or other arrangements, that processors[61] carry out their tasks in compliance with the laws enacted pursuant to the Directive (Art 17(2) and (3)). In the event of a processor not complying with such laws, it will be the controller that is primarily liable (Art 23 and 17). Thus, for e-commerce operators, determining which actors are controllers is more important than determining which actors are processors.[62]

4.1.4 Controller "makes use of equipment" in the data subject's Member State

In the case that the controller is not established on the Member States' territory, there is a particular problem in the interpretation of the notion "equipment" in Art 4(c).

The Art 29 Working Party advocates a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. According to the WP[63] the directive's objective is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and

[58] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
[59] Case C-221/89 Factortame [1991] ECR I-3905 §20.
[60] See Art 29 Working Party, supra n. 57 p. 8.
[61] The "processor" is defined in Art 2(e) as a person or organisation engaged in processing personal data "on behalf of" a controller.
[62] See for a more comprehensive analysis: Bygrave, L. A., supra n. 50
[63] WP 56 p. 9.

where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved. The art 29 Working Party is of the opinion that not all interaction between an Internet user in the EU and a Web site based outside the EU leads necessarily to the application of EU data protection law.

The test put forward by the art 29 Working Party is whether the equipment is at the disposal of the controller. The necessary degree of disposal is given if "the controller, by determining how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing".[64]

Further, the art 29 Working Party[65] considers that the concept of "making use" presupposes two elements: some kind of activity undertaken by the controller and the intention of the controller to process data. This implies that not any "use" of "equipment" within the EU leads to the application of the Directive. The power of disposal of the controller should, however, not be confused with property or ownership of the equipment, either of the controller or of the individual. This interpretation has support in recital 20[66] of the Directive, which uses the more general term "means"; it drops the more technical term "equipment".

4.1.5 Practical examples of application of Art 4(1)(c)

Cookies

An example involving cookies is the custom of operators of Web sites to set "cookies" on the computers of those visiting their sites. The question is whether Art 4(1)(c) applies if the computer is situated in an EU/EEA country and the third party using cookies to process personal data is located outside the EU. I will in the following presume that personal data are processed, either because the cookie contains personal identifiable data or because the cookie can be linked to a person more indirectly, e.g. through the computer's IP address.

The user's PC can be viewed as equipment in the sense of Art 4(1)(c), which is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory.

Considering these facts, the Art 29 Working Party is of the opinion that the national law of the Member State where this user's personal computer is located applies to the processing of personal data which occurs when the Web server saves or reads cookies on his hard disk.[67]

JavaScript, advertising banners and spyware

JavaScript is software applications sent by a Web server to a user's computer. It allows remote servers to run applications on a user PC. Depending on the content of the software, JavaScripts can be used in order to display information on a Web page, but also to introduce viruses in the computer (so-called malicious Java) and/or to collect and process personal data stored in the user's computer. Where the

---

[64] Id.
[65] Id.
[66] Recital 20: "Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice".
[67] On the other hand, if personal data are collected in a "visible" way, it might be argued that an individual transferring his own data has given his consent to such transfer, provided that he is properly informed about the risks involved.

controller decides to use these tools, it is the Art 29 Working Party opinion that he makes use of equipment in the sense of the Directive.[68]

The same applies to banner ads that are commonly placed on the requested Web site, for example search engines, via an invisible hyperlink to the advertising company.[69] To provide the customer with the most "adequate" banner ad, the network advertisers create profiles by using cookies set via the invisible hyperlink. The customer's profile is linked to the identification number of the ad company's cookie so that it can be enlarged every time the customer visits a Web site, which has a contract with the advertiser. In this way, additional collection of personal data from the user will take place through his computer and without his intervention every time the Internet user visits a Web site with a hyperlink to the advertiser.

Finally, it is of the Art 29 Working Party's opinion that Art 4(1)(c) will apply to so called spyware.[70] This is pieces of software secretly installed in the individual's computer, for instance when downloading software (e.g. multimedia software), in order to send back personal data related to the data subject (e.g. the music titles the individual tends to listen to). These new monitoring software applications often make use of JavaScript and other similar techniques, and clearly make use of the equipment of the data subject (computer, browser, hard disc and so on) to collect data and send it back to another location.

4.2 Application of the principles governing the collection of personal data

Having concluded that the national data protection law pursuant to the Directive applies to cookies, JavaScript, banners and other similar applications, this section will give a short overview over what obligations the 95/46/EC Directive imposes on the controller's using these tools.

The Art 29 Working Party has issued a few papers on this issue and I will first of all give a presentation of the core requirements proposed there with regard to use of cookies to collect personal data.[71] The WP has particularly focused on transparency and the importance of providing information about what processing is taking place on the individual Web site. The recommendations can be taken as a first initiative to spell out on the European level a "minimum" set of obligations in a way that can be easily followed by controllers operating Web sites, and does not dispense the controllers from their present obligations to check the full range of requirements and conditions set up in the applicable national law in order to make it lawful. In WP 56 it is mentioned that "[i]t should be discussed whether all elements mentioned in WP 43 shall also apply to the on-line collection of data in the EU by controllers established outside the EU". This may be a sign of scepticism to achieving the rather ambitious level of data protection expressed in the documents by the WP to these controllers.

Any collection of personal data from an individual via a Website should only take place after prior supply of information. More particularly, the existence of automatic data collection procedures and the possibility of opposing to the collection should be provided interactively and on the screen before using such a method to collect any data. In fact, the Art 29 Working Party goes as far as to suggest that "if necessary this information could be provided using the technique of a "pop-up" window.[72] For example, if a server wants to place a cookie on the user's computer, information must be provided before it is being sent to the Internet user's hard disk. Regarding invisible hyperlinks, which automatically leads the user to another server to display banners, the information should be given before the browser is triggered to connect to the other server.

The data subject should be informed of the domain name of the site server transmitting the automatic collection procedures, the purpose of these procedures, their period of validity, whether or not

[68] See WP56, supra n. 57, p. 12.
[69] Id.
[70] Id.
[71] See WP 17, WP 37, WP 43 and WP56.
[72] WP 43, p 7.

acceptance of such procedures is necessary to visit the site and the option available to any Internet user to object to their use, as well as the consequences of de-activating such procedures. In cases where other data controllers are involved in collection of personal data, the data subject should be provided with information on the data controller's identity and purposes of processing in relation to each data controller.

More generally the Art 29 Working Party emphasises a few core data protection principles with regard to collecting personal data on-line:[73]

- Data should only be collected as far as necessary in view of achieving the purpose specified;
- Personal data should only be required where necessary for a specific purpose. In other words, without a legitimate reason, personal data cannot be used and the individual remains anonymous (Art 6(1)(b));
- Provide for and promote anonymous consultation of commercial sites without requests for identification of the users by name, first name, e-mail address or other identifying data. Where no legal identification requirement exists, promote and accept the use of pseudonyms, even in the case of certain transactions;[74]
- The right to access and rectify should be ensured, and this right should be possible to exercise both at the physical address of the controller and on-line. Security measures should exist to guarantee that only the data subject has on-line access to the information which concerns him/her;
- Fix a storage period for the data collected. Data can only be kept for as long as this is justified by the purpose of the processing specified and pursued (Art 6 of Directive 95/46/EC and Art 6 of Directive 97/66/EC);
- When transferring information to a third country where adequate protection is not guaranteed, ensure that the transfer of data only takes place if it is in line with one of the derogations provided for in Art 26 of Directive 95/46/EC. In such cases, inform the individual about the adequate guarantees provided in order to make the transfer lawful.

4.3 Procedural aspects

According to Directive 95/46/EC Art 4(2), the controller should designate a representative who is established on the territory of the Member State where the equipment is located.

Further, as regards notification of the intended processing operation (namely the collection) to national data protection authorities, the directive provides for choices. According to Art 18(1) first sentence, the controller or his representative must notify the supervisory authority before carrying out any processing operation or set of operations. Art 19(1)(a) stipulates that the notification shall include amongst other elements the name and address of the controller and his representative.

According to Art 18(2), Member States may provide for a simplification of or exemption from notification. This is the case for categories of processing operations "which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects" (Art 18(2) first indent). The same applies where the controller, in compliance with the national law that governs him, appoints a personal data protection official in accordance with Art 18(2) second indent.

4.4 Enforcement

In an era of extensive trans-border data processing, data subjects are likely to be increasingly forced to seek remedies under foreign law for interferences with their data protection rights.

[73] See WP 43 pp. 4-8.

[74] One example is the use of pseudonym certificates for electronic signatures (see Art 8 of Directive 99/93/EC on a Community framework for electronic signatures).

In a concrete case, where an individual experiences problems with a non-EU Web site, the Art 29 Working Party[75] suggests that the individual should submit his case to the competent national data protection supervisory authority. This authority would determine whether the Directive respectively the national data protection law, applies. If it does, the authority should contact the foreign Web site and try to resolve the problem. If the case is brought before a court in the Member State where the individual is resident, the court will decide whether it has jurisdiction over the case (which according to international procedural law could be so, because the party most concerned is the individual living on the same territory as the court). In the case of having jurisdiction, the court applies the relevant national legislation pursuant to Art 4 of Directive 95/46/EC and may find the foreign Web site is in breach of these rules. Having obtained a judgement, there will still be problems of enforcing it, even though many third countries will recognise and enforce the judgement.

The Art 29 Working Party[76] recognises these problems of enforcing the Directive and expresses that a good level of compliance would require in the first instance to make aware both European and international organisations of the requirements of the Directive as regards collection of data in the European Union. Furthermore, it also suggests technological solutions, "providing a pre-established structure for the collection of personal data, which would incorporate the requirements described into the software tools used for the collection of personal data". An example of this approach would be to require Web browsers to be designed in a way which would guarantee that the Directives are complied with, e.g. by fair handling of cookies and invisible third party hyperlinks. This "designing privacy in" or "privacy by default" approach will be explored more thoroughly in section 5.

The Art 29 Working Party has also discussed the possibility of product authorisation procedures, which would include a check of the respect of legal requirements for the protection of personal data. The Working Party suggests that a European system of labels/Web seals, open also to non-EU Web sites, could be the cornerstone of such action.[77] This issue is assessed further in section 5.2.4.

4.5 Conclusion

Even though Arti 4(2) of the 95/46/EC Directive imposes obligations on the data controller to designate a representative established in the territory of that Member State, data subjects may frequently face difficulties that they would not otherwise experience in seeking remedies pursuant to their own national laws.

Bygrave[78] emphasises the possibility of "regulatory overreaching" by having a rule like Art 4(c) that is expressed so generally and non-discriminatory that it applies prima facie to a large range of activities without having much of a realistic chance of being enforced. He states that: "[t]he strict application of Art 4(1)(c) is likely to create a situation in which large numbers of data controllers outside the EU/EEA are supposed to comply with at least two sets of data protection rules that may not be harmonised (i.e. the rules of the EU/EEA Member State and the rules of the respective countries in which the controllers are established), and in which the duty of compliance with what are for the controllers *foreign* rules can arise on the basis of using relatively common, highly automated data-processing mechanisms".

Since the notion of "equipment" is a loose and disparate one, equipment in one data-processing operation can be dispersed over several countries. If this is the case, controllers might have to comply with a considerable multiplicity of national laws. In its latest working document, WP 56, the Art 29 Working Party put forward a "disposal-test" as presented in 4.1.4. I think this test will prove difficult to apply to new technical developments for controllers, national data protection supervision authorities and national. However, the working document gives valuable guidance and should in my view be

[75] WP 56 pp. 14-15.
[76] Id.
[77] Id.
[78] Supra n. 11.

given much weight to seek uniform practice until authoritative case law or new EU legislation dealing with the issue has been established.

When dealing with a controller established in another Member State, this Member State's national law applies. It is as mentioned in 4.1.1 the intention of the legislators that theses difficulties could be obviated by increased cooperation between the various national data protection authorities and increased possibilities for cross-jurisdictional court enforcement of data protection laws. However, some scholars[79] raises the question of whether this problem could be remedied if applicable law were to be made the law of the State in which a data subject has his/her domicile. It is stated that such a rule would parallel existing European rules on the jurisdiction and choice of law in the case of consumer contracts.[80] They also argue that it deserves a serious consideration, particularly in light of the close relationship between the concerns of data protection law and consumer protection.

[79] See Bygrave, supra n. 62, and Benno, *The "anonymisation" of the transaction and its impact on legal problems*, The IT Law Observatory Report 6/98 (Stockholm, 1998), p. 16.

[80] See the 1968 Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Art 13-15; 1988 Lugano Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters, Art 13-15; 1980 Rome Convention on the Law Applicable to Contractual Obligations, Art 5.

5 Standardisation and regulation of architecture

5.1 What may standards on data protection achieve?

The international aspect of the Internet is clearly the main reason for advocating standards on data protection. The Initiative for Privacy Standardisation in Europe (IPSE) recently published its final report[81] on whether standardisation actions in the broadest sense could benefit the process and implementation of the Directive 95/46/EC. The remit of the group was to concentrate on the potential role of standards work in implementing the Directive in Europe. However, as mentioned many times in the report, a number of merits of standardisation come from outside Europe.[82]

Many large companies in Europe are global companies, and their privacy policies and practices tend to be developed as global company policies with regional variations. Electronic commerce and rapidly dropping telecommunication costs have made global databases and sourcing systems a reality. Companies may have one centralised human resources system, one integrated IT capability for software support and one public interface through the Internet. These practices, closely integrated with the technological infrastructure, are difficult to manage in a manner that respects regional variations, not to mention national law. At the same time, the growing complexity of the Internet and high bandwidth demands have resulted in a global network of mirror sites, often run by intermediaries.[83]

Also consumers may benefit from standardisation of data protection. Most Internet surveys conclude that the general public is confused about how Web sites handle personal data and lacks trust in how Web sites handle their personal data. People are not aware of the processing of personal data taking place and complex privacy policies make it often very hard to find out for what purposes your personal data may be used. Measures that are supposed to enhance the user's control over personal data, like for instance Web seals and privacy enhancing technologies, does not necessarily comply with the EU Directives.[84] Thus, consumer confidence is expected to increase if consumers know that their interests are protected by businesses and administrations adhering to the requirements of an international standard.[85]

Also small- and medium-sized enterprises (SMEs) experience many of the same problems that consumers face.[86] Many of them are under-resourced, and have difficulty devoting the time to participate in standards activity, let alone consortia activity where the price of entry usually precludes their joining. They are consumers of both government services and the products and services of much larger players, where they are usually in a disadvantageous position relative to power and market force. They also face steep hurdles in trying to keep up with the pace of change, both regulatory and technological. Companies, particularly small businesses which do not have sufficient competence in matters of data protection and do not have the resources to seek expensive outside help are often perplexed when they face the issue of compliance to the Directive. This is partly because the Directive (and usually national law) remains at a relatively high level of generality, for example requirements that personal data must be processed "fairly and lawfully" (Art 6).[87]

Also from the developer's point of view there may be advantages of standardisation. New developments take place in a rapidly changing environment of new technologies, competitive markets,

[81] IPSE report, published 13 February 2002
[82] IPSE report, section 3.5.
[83] Id.
[84] See e.g. the critique of P3P by Art 29 Working Party in WP 11.
[85] Blow, Joyce, former chairman of the BSI Consumer Policy Committee, Conformity assessment: "Products and services: the added value of consumer participation in standards development – a personal view" ISO Bulletin volume 32 no. 8 August 2001, p. 15-18.
[86] IPSE report , section 4.9.
[87] IPSE report, section 4.

convergence of networks and globalisation. In a recent communication from the Commission[88] it is pointed out that these challenges are compounded by the fact that the market will tend to under invest in security and thus also data protection. Due to certain market imperfections many security risks remain unsolved or solutions are slow coming to the market. Particularly, investment in security often only pays off if enough people do the same. Thus cooperation to create security solutions is required. But cooperation only works if a critical mass of players participates, which is difficult to achieve as there are "free-rider" profits to be made. Interoperability between products and services will allow for competition between security solutions. However, there are substantial coordination costs involved as global solutions might be required and some players are tempted to impose a proprietary solution to the market. Since a multitude of products and services still uses proprietary solutions there is no advantage to using secure standards which only give extra security if everyone else offers them. The communication[89] states that there is no lack of standardisation efforts, but a great number of competing standards and specifications lead to fragmentation of the market and to non-interoperable solutions.

5.2 Enhancing data protection through indirect regulation

This section will build on the previous ones by assessing the possibilities of safeguarding the rights pursuant to the Directives through standardisation and regulation of other aspects than mentioned above. Until now we have only assessed the difficulties of applying and enforcing rules regarding the actual conduct of processing personal data. However, inspired by the more philosophical approach by inter alia Joel Reidenberg[90] and Lawrence Lessig,[91] the potential of law to indirectly regulate through for example "social norms, markets and architecture" should also be considered. These authors share an emphasis on the importance of the technical infrastructure of cyberspace – whether they call it "code" or "Lex Informatica" or "Net federalism" – as a source of regulation of the Internet.

Law does not only affect individual behaviour directly (e.g. by prohibiting a certain conduct), but also indirectly by seeking to change markets, norms or architectures. One of Lessig's classical examples is that governments can choose to address the barriers faced by disabled people by forbidding discriminatory conduct (directly regulation by law), by requiring educational institutions to teach children to respect the interests of the disabled (law indirectly regulating norms) or by requiring building codes to allow for access ramps and other physical facilities (law indirectly regulating real space "architecture"). In real space, Lessig argues, these indirect regulations are already "the regulatory technique of choice".

There are reasons to believe, as will be illustrated in the following sections, that lack of influence on social norms, the markets and the technical infrastructure of the Internet cause great problems with application and enforcement of the EU Directives.

5.2.1 Regulation and standardisation of software and hardware

In section 3 we analysed how automatic processing is possible due to the use of for example cookies. This tool would not be possible if the browser's default settings automatically blocked third party cookies. In this section I will explore how the EU has positioned it self to the idea of directly regulating the technical equipment that makes this processing possible.

Currently there are security requirements regarding electrical components of a computer, but no requirements as to security of data handled by a computer.[92] In its recommendation 1/99 the Art 29

[88] "Network and Information Security: Proposal for A European Policy Approach", 6.6.2001, COM (2001) 298 final, p. 16.
[89] Id.
[90] Reidenberg, Joel R., "Lex Informatica: The formulation of Information Policy Rules Through Technology", *Texas Law Review*, vol. 76, number 3, February 1998.
[91] Lessig, Lawrence, "The law of the horse: what cyberlaw might teach", *Harvard Law Review*, vol. 113 p. 501, 1999.
[92] See supra n. 88, p. 24.

Working Party addressed the problem of so-called invisible and automatic processing of personal data on the Internet performed by software and hardware. The Working Party found that some of the software, which is necessary for new telecommunications services, such as software used for sending e-mails and browsers used for surfing the Internet, does not comply with data protection rules. In its recommendation the Working Party called on software and hardware industry to develop privacy-compliant products in line with data protection rules of the Directives 95/46/EC and 97/66/EC.

The issue of privacy compliance of software and hardware used for electronic communications services has been raised during the revision of the Directive 97/66/EC. One of the objectives of the 1999 review of the telecommunications regulatory framework was to ensure a consistent, technology neutral application of existing rules and propose amendments where technological neutrality was not guaranteed. Under the revision the possibility to address the matter in the revision of Directive 97/66/EC was also examined.

Under the Directive providers of public telecommunications services and networks are under specific legal obligations to guarantee the security of their networks, to ensure the confidentiality of communications and to delete traffic data. One could say that there is no technological neutrality in a situation where the privacy of the user is protected depending on whether certain functionalities necessary for a telecommunications service are in the network or in the software. However, the option of amending the Directive by extending its coverage from electronic communications services and networks to terminal equipment including software was considered inappropriate. Instead, the Commission stated that it might propose measures under Art 3(3)(c) of Directive 1999/5/EC[93], which explicitly foresees the possibility of requiring manufacturers of terminal equipment to construct their product in such a way that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected. Such measures could therefore be proposed if privacy compliance of software and hardware remains unsatisfactory.[94]

In the Directive 95/46/EC, however, the incorporation of Privacy Enhancing Technologies (PETs) into strategies for privacy receives some encouragement from Art 17, which requires data controllers to implement “appropriate technical and organisational measures” to protect personal data, especially in network transmissions. Recital 46, which augments the meaning of Art 17, highlights the requirement that these measures should be taken “both at the time of the design of the processing system and at the time of the processing itself”. Hence, it indicates that security cannot simply be bolted onto data systems, but must be built into them.

5.2.2 Standardisation bodies and data protection

An interesting recommendation from the IPSE report,[95] is to develop a coherent assessment of the impact of ongoing technological development on the implementation of the Directives, with a view to ensuring a better dialogue between the standards developers and the technical community, and the oversight authorities and consumers. The rationale for the recommendation is that privacy requires a systematic approach in which data protection is designed into systems and operations from the outset. It is also a complex and often contradictory set of issues, “where buy-in to final outcomes increases directly with the degree of participation in the process”.

The initial requirement in such an assessment would be to develop a technical report, based on stakeholder requirements and an analytical framework,[96] which can be used to understand and give

[93] Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, 9 March 1999. (OJ L 91, 7.4.1999, p. 10).
[94] See Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, explanatory memorandum, COM (2000) 0385 final. (OJ C 365 E, 19/12/2000 p 0223-0229).
[95] IPSE report, section 8.
[96] As an example, the International Security, Trust & Privacy Alliance’s (ISTPA) Privacy Framework represents a joint industry and academic research institute effort to construct an analytical framework to guide the

context to the impact of technologies and standards, and the potential for improvement of outcomes through the use of PETs. The report states that a "fundamental disconnect needs to be addressed between the legal regulatory community, society and that of business and innovation". An example is the urgent need for a common P3P policy reflecting (within the limits of actual and practical possibilities) the values of the Directive 95/46/EC.

Another aspect that, according to the IPSE report, should be addressed in the assessment is the standardisation process itself.[97] There is evidence that conventional technology-related standardisation activities do not take sufficient – or any – account of data protection considerations. Standard bodies are developing standards of all kinds with committees that are relatively deficient in privacy expertise. The assessment would describe ongoing activity and flag current standards setting activities that have a potential impact on privacy and could benefit from informed review and comment by data protection experts.

In the longer term, individuals, business, data protection authorities and technologists could benefit from an informed oversight of the impact of technologies on data protection. Technologists need to understand data protection requirements and how they can be built at a systematic level into the technology infrastructure. Data protection authorities need a concise way of keeping up with technological developments, and a voice in the design stage of the process. Law enforcement agencies can be helped to understand the role and contribution of standardisation and provide input to discussions on the impact of technologies on data protection. How this collaboration should take place, however, is not clear and should in my view be regarded as a significant part of the assessment recommended in the IPSE report.

5.2.3 Standardisation and Privacy Enhancing Technologies (PETs)

In applying PETs, the person responsible can choose two strategies: either focus on preventing or reducing identification or focusing on preventing unlawful processing of personal data, in accordance with the Directive. A combination of both is also possible.[98]

However, the application of PETs in old, existing data systems is not always feasible. For example, opening up existing data systems to introduce an identity protector can be very expensive. In addition, the owner of the old data system often lacks the courage and will to carry out such operations as the "spaghetti" usually cannot be disentangled due to the many releases and patches.

The major opportunities for Pets are therefore in the design and implementation of new data systems. The latest data systems do not necessarily completely comply with the requirements set in the Directive or the related national legislation.[99]

P3P[100] illustrates the challenge and significance of agreeing on what level data protection should be set in PETs. The Art 29 Working Party[101] has in its opinion on P3P stated that the P3P vocabulary has not been developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalise lower common standards. Further, the opinion highlights series of problems posed by the implementation of P3P. The Art 29 Working Party argues that a technical

---

development advancement and understanding of privacy tools, technologies and systems designed to address information privacy related issues in the context of security and trust. See: http://www.istpa.org/.

[97] IPSE report, section 8

[98] Borking J and Raab C, "Laws, PETs and Other Technologies for Privacy Protection"', The Journal of Information, Law and Technology, vol 1. 2001.

[99] See WP 17.

[100] Platform for Privacy Preferences (P3P) 1.0, issued by the W3C on the 16 April 2002 as W3C recommendation, representing a cross-industry agreement on an XML-based language for expressing Web site privacy policies. P3P enabled browsers can read this snapshot automatically and compare it to the consumer's own set of privacy preferences. See http://www.w3.org/P3P/.

[101] Art 29 WP "Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), Draft opinion of the Working Party", opinion 1/98, WP 11.

platform for privacy protection will not in itself be sufficient to protect privacy on the Web: “It must be applied within the context of a framework of enforceable data protection rules that provide a minimum and non-negotiable level of privacy protection for all individuals”. Crucial to the decision of whether or not to provide data to Web sites established outside the EEA will, according to the Art 29 Working Party, be to know not only the approximate content of any applicable rules, but also whether there are any sanctions for non-compliance and, most importantly, a simple and effective means of obtaining a remedy if the rules are broken. The Art 29 Working Party agrees that the P3P in theory could be capable of providing such information to users. However, the P3P vocabulary “does not require or even allow for the provision of information about sanctions or remedies to users”.

Further, the opinion states that “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 on-line negotiation. In fact those businesses, organisations and individuals established within the EU and providing services over the Internet will in any case be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process”.[102]

The opinion also touches on the issue of default settings of browsers. Given that most Internet users are unlikely to alter any pre-configured settings on their browser, the “default” position regarding a user’s privacy preferences will have a major impact on the overall level of on-line privacy protection. Therefore, the major browsing software manufactures have a responsibility to implement P3P in a manner that enhances rather than reduces levels of privacy protection.

5.2.4 Consumer awareness

Another recommendation in the IPSE report is to take a more systematic approach to promote and educate consumers in privacy standards. “Realisation of consumer trust and confidence (...) can only be effectively built on a solid information base among citizens and consumers, which promotes greater participation in the process of standards development and deployment”. It is highlighted in the report that the need for this information is not already being adequately addressed by any organisation.

One such instrument to enhance consumer awareness regarding data protection is the use of Web seals. In the last few years there has been a growth of Web seals programmes related to privacy protection levels, many offered globally. This has occurred despite the fact that there is no single global standard for privacy and no generally accepted set of audit standards against which seals can be tested.[103] Consumers cannot be expected to appreciate the differences between the varying seal programmes or understand exactly what level of assurances they offer. This issue has been addressed by the Art 29 Working Party,[104] which has invited the Commission to consider as a matter of urgency the creation of an EU seal system for Internet sites, based on common criteria of data protection assessment that could be determined at the Community level. The IPSE report also supports setting up an EU seal system, but recognises that there are difficulties as some seals currently cover other areas than privacy, some are government sponsored and some, but not all, also apply to off-line activity.[105] Another challenge is that seal programmes are competitive and may not wish to cooperate on work of this nature.

5.3 Conclusion

Even though my analysis in this section has been very superficial it should be clear that the main reasons why the EU Directives are so difficult to apply and enforce is due to what Reidenberg and

[102] According to section 4 in this paper and later publications of the Art 29 WP, this may also apply to controllers established outside the EEA.
[103] IPSE report section 8.
[104] See WP 43, p. 2.
[105] IPSE report section 8.

Lessig would call “architecture”.[106] In my view it will be impossible to achieve a higher level of data protection if not data protection principles are taken into regard when developing technical standards, software and PETs. This will necessitate better dialogue and a closer collaboration between data protection specialists and technologists.

[106] See supra n. 90 and 91.

6 Conclusion

This paper has illustrated that there are many difficulties in applying the data protection Directives to automatic processing on the Internet.

It is very controversial whether clickstream data can be considered to be personal data pursuant to the Directives. Advertisers and heavy users of cookies on the Internet argue that the information is not possible to link to individuals. This may be so in some cases, but my assessment shows that it is a theoretical possibility to link clickstream data to individuals. Lack of transparency and knowledge about business routines makes it difficult to come to a conclusion on this issue.

My conclusion on the international application of national data protection law may be controversial. When the controller is established outside the EU/EEA, the data subject's national law applies to automatic processing where the controller uses common tools like cookies. This interpretation gives a significant effect to national legislation pursuant to the Directive 95/46/EC. This means that controllers all around the world who are using clickstream data to make profiles on their Internet users may be in breach of the Directive. However, the challenges in enforcing the rights pursuant to the Directive will most probably have a chilling effect for those trying to stop non-compliant behaviour abroad. Thus, enforcement is a key word with regard to data protection.

My main point in section 5 is that it will be very hard to enforce rules which do not reflect the common used standards and default settings in browsing software. To be able to give effect to the Directives the EU has to make sure that browsing software, PETs and trust schemes like Web seals are in compliance with the legislation. This means that the EU must be able to have influence on standard setting bodies like W3C and the software industry. My analysis in section 2 shows that data protection is a controversial issue. It is clearly a tension between the EU and the USA and between consumers and e-commerce companies. Neither should the Internet society's ability to refuse to give in to interference by national and regional regulatory authorities be underestimated.

The requirements laid down by the Art 29 Party on Web sites' handling of personal data are in my view quite unrealistic.[107] My analysis in section 4.2 shows that there seems to be some uncertainty as to how information from automatic processing should be regarded in comparison with information collected through other means. The Art 29 Working Party has also raised doubt whether the same requirements should apply to Web sites within and outside EU/EEA.[108] This would in my view be unfortunate and could possible lead to more confusion than simplification.

This paper has shown that there are great difficulties in applying the data protection Directives to processing of information on the Internet. It is also evident that seems to be a great demand for more and consistent guidance on how the Directives should be applied and also enforced. I think we will see a battle on the level of data protection on the Internet in the next few years. This will be a negotiation both between the e-commerce sites and the customers regarding the use personal data, especially with regard to use of "informed" consent to allow lawful processing of personal data. Another type of "battle" will be among e-commerce sites in communicating trust to their customers. It will be difficult for companies to invest in good privacy for their customers when the customers are not able to distinguish between the clever companies and those who do not take privacy seriously. This problem increases as commonly used Internet technologies by default often come in conflict with EU data protection law.

[107] See for example the documents adopted in WP 37, 43 and 56.
[108] WP 56, quoted in section 4.2 of this paper

7 Bibliography

Legislation and action plans

The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter termed "OECD Guidelines"), adopted by the OECD Council on 23.9.1980.
http://europa.eu.int/comm/internal_market/en/dataprot/inter/priv.htm

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 28.1.1981. ETS no 108.
http://conventions.coe.int

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, 24 October 1995, (OJ L 281, 23.11.1995 p. 31).
http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997 (OJ L 24, 30.1.1998, p. 1).
http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, 9 March 1999. (OJ L 91, 7.4.1999, p. 10).

Proposal for a Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM (2000) 385 final. (OJ C 365 E, 19.12.2000, p. 223).
http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

"Network and Information Security: Proposal for A European Policy Approach", 6.6.2001, COM (2001) 298 final.

"eEurope 2002: An information society for all – Action Plan", Brussels, 14.6.2000.

Communication from the Commission: "eEurope 2005: An information society for all", Brussels, 28.5.2002
COM(2002) 263 final.

Publications by Art 29 Working Party

Note, all documents are numbered (WP "number") and are available at URL:
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

"Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard", WP 11, adopted 28 April 1998.

"Processing of personal information on the Internet", Working Document, WP 16, adopted 23 February 1999.

"Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware", recommendation 1/99, WP 17, adopted 23. February 1999.

"Opinion 4/2000 on the level of protection provided by the "Safe Harbour Principles", WP 32, adopted 16 May 2000.

"Privacy on the Internet – A integrated EU approach to On-line Data Protection", Working Document, WP 37, adopted 21 November 2000.

"Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, WP 43, adopted 2/2001.

"Fifth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in Third Countries covering the year 2000", WP 54, adopted 6 March 2002.

"Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based Web sites", WP 56, adopted on 30 May 2002.

"Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe", WP 57, adopted 30 May 2002.

"Working document on functioning of the Safe Harbor Agreement, WP 62, adopted 2 July 2002.

Textbooks

Bygrave, L. A., Phd. thesis, *Data Protection Law: Approaching its Rationale, Logic and Limits*, Faculty of Law, 1999, University of Oslo.

Craig, P. and Debúrca, G., *EU Law: Text, Cases, and Materials*, *Oxford*: Oxford University Press, 1998, 2nd ed.

Smith, G., *Internet law and regulation*, Bird & Bird, 2002.

Articles and reports

Aaron David, Under Secretary of Commerce, cited in Andrews, Edmund L. "European law aims to protect privacy of personal data", New York Times, October 26 1998, p. A1.

Benno, *The "anonymisation" of the transaction and its impact on legal problems*, The IT Law Observatory Report 6/98 (Stockholm, 1998), p. 16.

Borking J and Raab C, "Laws, PETs and Other Technologies for Privacy Protection"', The Journal of Information, Law and Technology, 2001, vol 1.
http://elj.warwick.ac.uk/jilt/01-1/borking.html

Bygrave, L. A., "Determining Applicable Law pursuant to European Data Protection Legislation", *CL & SR*, 2000, volume 16, p. 252-257.

EPIC Report (1999), "Surfer Beware III: Privacy Policies without Privacy Protection",
http://www.epic.org/reports/surfer-beware3.html

EPIC Report (2000), "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy", June 2000,
http://www.epic.org/reports/prettypoorprivacy.html

Initiative on Privacy Standardization in Europe, final report, 13 February 2002.

http://europa.eu.int/comm/enterprise/ict/policy/standards/ipse_finalreport.pdf

Lessig, Lawrence, “The architecture of privacy”, Draft 2 presented at the Taiwan Net 1998 conference, March 1998.

Lessig, Lawrence, “The law of the horse: what cyberlaw might teach”, *Harvard Law Review*, vol. 113 p. 501, 1999.
http://cyber.law.harward.edu/works/lessig/law_horse.pdf

Long, J William and Quek, Marc Pang, “Personal data privacy protection in an age of globalisation: the US EU safe harbour compromise”, Journal of European Public Policy, 3 June 2002, vol. 9, p. 331.
Mayer-Schönberger, V., “The Internet and Privacy Legislation: Cookies for a Treat”, *CL&SR* vol. 14 no. 3, 1998.

Reidenberg, Joel R., “Lex Informatica: The formulation of Information Policy Rules Through Technology”, *Texas Law Review*, vol. 76, number 3, February 1998.

Rotenberg, M., “Data Protection in the United States – A Rising Tide?”, *CL&SR*, Vol. 14 no. 1, 1998.

Shaffer, Gregory “Globalisation and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards”, 2000, *5 Yale J. International Law 1*.

Steinke, Gerhard, “Data privacy approaches from US and EU perspective”, *Telematics and Informatics*, Vol. 19 Issue 2, May 2002, p. 193-200.

US Federal Trade Commission, “Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress” (May 2000)
http://www.ftc.gov/os/2000/05/index.htm#2.