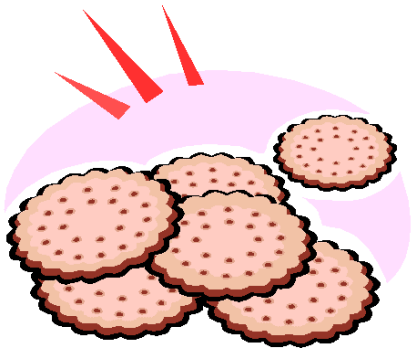
Max W. MOSING

Cookies and Log Files

The “Transparent Internet User” or Data Protection on the Internet in the EU ?!



January 2003

1 Introduction

In the every day life on the Internet data of the user are stored by several entities. The technical possibilities of storing data on the Internet (and especially on the World Wide Web (www)) are multifaceted and in most cases the user does not even know that, what, and from whom (his) data are processed. Unfortunately, governments (secret services), companies and private entities (data spies, …) are already using the opportunity for data-mining for all kinds of purposes: The danger of the "(uninformed) transparent Internet user" is obvious.

The scope of this paper is to evaluate the legal background of the two most common examples for data processing/storing on the Internet, cookies and log files. It is not new that "[t]he Internet is not a legal vacuum",[1] but although the EU has been dealing with the issue of data protection for years and the national data protection laws of the Member-States are being based on the EU Data Protection Directive,[2] the regulations across the EU are less than crystal clear. This fact combined with the main legal issue of the Internet - the disappearance of borders – lead to an inconsistent evaluation of data processing on the Internet. This work focuses on the legal guidelines of the EU and brief excurses on their transposition in the Member-States (mainly the UK and Austria).[3] Finally the Directive 2002/58/EC on privacy and electronic communications (E-Communication Directive),[4] which has to be transposed till the 31st of October 2003, will lead to new regulations on cookies and log files but raises also new issues.

One finding of this work can be antedated: The EU is on the way to guarantee the right to privacy and expands therefore the importance of the data protection regulations to the right to privacy: Information and not only personal data will be the object of protection

[1] European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, "Working document: Processing of Personal Data on the Internet", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp16en.htm (1/20/2003).
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal 1995 L 281, 31.
[3] In the US there have been already some actions because of cookies (eg vs Doubleclick – cp beneath), but these cases cannot be easily compared with the situation in the EU.
[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 2002/201, 37.

in connection with the e-communication. As it will be shown beneath, this fact will change the every day life on the Internet/www: The need for consent will lead to a “pop-up jungle” and longer (and therefore even more unreadable) general terms and conditions of providers.

2 Technical Background

2.1 Definitions

Before appearances on the Internet can be evaluated legally, it is essential to understand at least basics of the technical background – otherwise the lawyer is in a permanent danger to "judge worldly innocent".

2.1.1 Cookies

Cookies are used by web servers on the www:

> "Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, to allow users to participate in WWW-wide contests (but only once!), and to store shopping lists of items a user has selected while browsing through a virtual shopping mall."[5]

> "A cookie is a piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it. The pieces of information are stored as name-value pairs."[6]

Cookies base on a two-stage process:

- The cookie is stored by the web server in the user's computer in a special file called a "cookie list".
- The web server gain access to "its'" cookies whenever the user establishes a connection to it.

In most cases the storage of the information into a cookie in the computer of the user, and access to it, is not noticed by the user, unless he uses a browser-setting or a firewall that block cookies.

---

[5] Viktor Mayer-Schönberger, "The Cookie Concept", http://www.cookiecentral.com/content.phtml?area=2&id=1 (1/10/2003).

[6] Brain Marshall, "How Internet Cookies Work", http://www.howstuffworks.com/cookie1.htm (1/15/03).

From a technological point of view, cookies have to be distinguished from programs/software (which have to be downloaded by the user more or less actively):[7] Cookies cannot run like programs do; therefore, they cannot gather any information on their own, nor can they collect any personal information about the user from his machine, as long as this information is not already known by the web server (because the browser has sent this information to the web server; some computer languages used on the www, like Java or JavaScript, can be used for gathering and transmitting a huge amount of data from the user's computer to the server: User's settings, web history and so on).

Microsoft's Internet Explorer (MS IE) stores all the cookies (normally) in a directory called "c:\windows\cookies" ("cookies list"). In this context, the EU-Working Party on the Protection of Individuals recommended as early as in 1999 that cookies and other client persistent information should be stored in a standardised way and be easily and selectively erasable at the client's computer.[8] Unfortunately, there has not taken place any standardisation: Opera 7 stores the cookies in a single file "cookies4.dat" and Netscape 7 stores cookies as temporary internet files.

The vast majority of sites store just a piece of information in their cookie (eg session identification) but technically there is no limit: A web server could store infinite name-value pairs. On the other hand, as information are stored in a cookie does not say anything about the data the web server has stored: The information (eg selected goods, visited sites, time, …) can also be stored in the web server's database and the cookie contains only an unique ID to identify the user in the database.

A cookie does not only contain data gathered from the user's computer but also other pieces of information can be stored with the name-value pairs; eg an expiration date (otherwise the browser deletes cookies according to the setting of the system - normally when the user quits the browser). The expiration date can also be set in a way that the

[7] Of another opinion: Jean Hughes / Edward Black / Carolyn Chia, "Data Protection Compliance For Financial Institutions – A UK Perspective", FSB 2002, 2.8(5); unclear: Sarah Gwyndaf-Roberts, "Cookies", PDP 2001, 1.6(4).

[8] European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal data, "Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm (1/20/2003).

cookie is stored forever unless the user deletes it manually; these are called persistent cookies. Furthermore, a path for associating different cookie values with different parts of the website can be stored.

One of the practical issues and data protection is the fact, that all the data in a cookie can be encrypted by the server; so even if the user opens a cookie (with every word processor) he cannot find out what information is really stored in that cookie (cp more beneath).

The above-mentioned possibilities of cookies seem to make them the perfect measure for surveillance for any purpose; but there are several things that make cookies imperfect:

- Shared computers: Any machine that is used in a public area, and many machines used in an office environment or at home, are shared by multiple people. If they do not use different accounts (cookies do not only identify the computer but also the username) the web server can not distinguish between the different persons sitting in front of the computer.
- Cookies can be easily erased: It is easy to delete the cookies, directly in the browser or in the folder "c:\windows\cookies" (MS IE).
- Multiple machines: People often use more than one machine during the day (eg laptop and desktop). Therefore, for the web server a user with multiple machines seems to be different users – profiling becomes harder.
- 20 cookies limit: Each domain (generally speaking, each web server) is only allowed to store 20 cookies on the computer of the user; more cookies are not accepted by the system.

The solution for the problems would be a server based registration (identification) of the user. But in this case the Internet user knows that he is identified; cookies work often without any knowledge of the user. And there is another reason for using them; cookies make it easier to track the user's way through the Internet:

2.1.1.1 Who Can Read the Cookies?

Not every web server can read all the cookies:[9] Only those can be accessed that have been set from the web server's domain.[10] But a domain can be shared by several entities (eg: oe3.orf.at uses the same domain (orf.at) than fm4.orf.at); therefore it is possible that all theses entities can access the cookies of each other.[11]

Companies who provide other websites with data that is retrieved from their web server (eg banners), can set cookies and use them for tracking the movements of the user. "DoubleClick" (www.doubleclick.com/us/) is the most famous example of this method:[12] Many companies use DoubleClick to serve ad banners on their sites. DoubleClick loads with the banner cookies on the machine of the user and can then track the movements across multiple sites where DoubleClick has banners and can even customise banners that are placed on the webpages.[13] Because these cookies are not directly set by the website the user has accessed they are called "third party cookies". With these cookies DoubleClick can form very rich profiles. Most of these profiles are anonymous, but DoubleClick started to link these profiles to name and address information from companies where the user has identified himself before. A US case against this practice failed as the US do not have adequate data protection regulations to protect the individual from that kind of process - the situation would be different under the data protection legislation across the EU-Member-States. Meanwhile DoubleClick has changed its' privacy policy to improve its' image.[14]

2.1.1.2 Need for Cookies?

From a positive point of view "[…] cookies are generally good things – they save you time when surging the web and, on the vendor/marketing side they are a source of

[9] Http://www.cookiecentral.com/content.phtml?area=4&id=11 (1/15/2003).
[10] Gwyndaf-Roberts, PDP 2001, 1.6(4).
[11] Cp Victor Mayer-Schönberger, "The Internet and Privacy Legislation: Cookies for a Treat", http://www.wvu.edu/~wvjolt/Arch/Mayer/Mayer.htm (1/22/2003).
[12] Cp the US case report of Martin H. Samson, "Internet Law – Cookies", http://www.phillipsnizer.com/int-cookies.htm (1/20/2003).
[13] European Commission, "Working Document: Privacy on the Internet – An integrated EU Approach to On-line Data Protection", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf (1/22/2003).
[14] Privacy Policy, http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=& (1/20/2003).

valuable information, although possibly open to abuse at times."[15] Cookies are used in many different ways: For e-commerce solutions (e-trolley), identification (even passwords can be stored in cookies), online databases (for individual settings), and so on. Nearly all these features can also be provided by server based solutions, but the usability of cookies make them so attractive (cp eg with dynamic IP-addresses beneath).

Some years ago, storage space was very expensive and so provider of web services tended toward storing data in the user's computer. Those days are gone and providers use huge databases for user data and use only the cookies to identify the user in the database. This trend has been strengthened by the browser standard, that each domain can only store 20 cookies on the user's machine.

2.1.2 Log Files

A log file is a "[f]ile that records the activity on a Web server."[16] Log files record information such as, which files from a web server are requested, when they are requested, who requested them, and where they were referred from. These data can help to identify trends but also incompatibility and other bugs in a website or a web server. Log file analysis software helps the provider to quickly and easily view high-level trends. Log files are generated on nearly every web server (even if mere conduit of data) and (normally) consist of the following data:

- Computer of the user (IP-address or even URL: Some web servers are set to automatically resolve IP addresses by conducting a "Whois lookup"[17]);
- Date and time of the visit or the transaction;
- Names of the files (or data) that were transmitted;
- Status codes (eg 404: The requested URL was not found on this server);
- From which URL the request has been generated (prior page);
- What system has the user installed;
- What browser has the user installed.

[15] ITLT, Editor's Comment, "Computers and Information Technology", ITLT 2002, 10.4(3).
[16] Http://www.marketingterms.com/dictionary/log_file/ (1/20/2003).
[17] Cp eg http://www.ripe.net/perl/whois (1/24/2003).

2.1.2.1 Who Can Read the Log Files?

Normally only the provider of the web server is able to read the log files but there are rumours that several providers sell their log files to web marketing agencies. With the help of log file analysis software it is then pretty easily to create profiles and even identified profiles of single users (depends on IP-addresses and other available data that can be compared).

2.1.2.2 Need for Log Files?

The access providers often use the log files for billing – unless there is a flat rate. If the user has (only) to pay the time he is connected to the Internet, there are other technical possibilities for the billing (connection-time-billing). Only if the user has to pay the amount of data that are transmitted, there is no other way than to use log files for the billing; but even then, not all the data in log files are necessary (cp beneath the "economy of data"-principle).

2.1.3 IP-Addresses: The Key to the Individual User?

An Internet Protocol-(IP-)address identifies an individual computer (or (virtual) server) on the Internet. The Berkeley Internet Name Deamon (BIND)[18] connects domain names, like it-law.at, to the IP-address 195.230.39.2 and with the IP-address the server where the data of it-law.at are stored, can be identified on the Internet and a connection can be established. After the connection is established with the help of the IP-addresse the computers use the MAC-addresses[19] to address the sent packets. The MAC-address is worldwide unique and identifies an individual network-card. While MAC-addresses are hardware based on the network-card, IPv4-addresses (IP version 4) are assigned (finally[20]) by the access provider: Every computer needs an unique IP-address while connected to a network: There are two different kinds of assignments of IP-addresses:

- Static IP-addresses;
- dynamic IP-addresses.

[18] Cp to the history of BIND: Lawrence Lessig, Future of Ideas (2001) 56.
[19] Short for Media Access Control address, a hardware (network card) address that uniquely identifies each node of a network.
[20] The RIPE Network Coordination Centre (RIPE NCC) is one of 4 Regional Internet Registries (RIR) which exist in the world today and administrates the IP-addresses (mainly) for Europe and assigns IP-address blocks to providers, cp www.ripe.net (1/23/2003).

While static IP-addresses are assigned to the identical computer/connection, dynamic IP-addresses are assigned for every (new) session of the user. What kind of assignment is used, depends on the policy of the access provider (dynamic addresses can be administered in a way that they can be used consecutively by several users). The more popular broadband access with flat rates becomes, the more static IP-addresses are used. Because in this case the user's computer always uses the same IP-address, this data can be used for profiling. Sometimes even dynamic IP-addresses can provide geographical location data, as big providers (eg AOL, T-online) assign dynamic IP-addresses according to the domicile of the user (mostly because of technical reasons); in this case little knowledge is needed to find out what IP-address-block is used in what region (in Germany it is said, that in the T-online-network, IP-addresses lead at least to the town of the user).[21]

The "new generation" of IP-addresses (IPv6) raises even more (new) issues, because it uses "lifelong" unique identifiers for every device.[22] The standards are not crystal clear yet; for that reason, a (legal) evaluation is not possible at the moment.

However, the IP-address leads (at least) to the provider of the user and so (normally) the user's geographical location can be ascertained (easily with the help of special software: Eg: visualroute[23]). With the help of the IP-address the search engine *google.com* seems to identify the location where the user is located and leads the user automatically to the national site of *google*.[24]

[21] Cp Patrich Brauch, "Von wegen Incognito", c't 2002, H 19, 128.
[22] Cp European Commission, "Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp58_en.pdf (1/20/2003).
[23] By http://www.visualware.com (1/22/2003).
[24] The author entered www.google.com and was forwarded to www.google.at while connected to the Internet over his Austrian provider (1/2/2003); cp http://www.wichtig.de/ (Zenoogle) (1/24/2003).

3 Legal Background

On the way to the "information society"[25] the public has been waking up to the issue of privacy: "Knowledge, of itself, is power" became "information, of itself, is power" and is changing to "data, of itself, is power". The European Convention on Human Rights deals with this problem in its' Art 8,[26] which was transposed eg to Schedule 1, Art 8 of the UK Human Rights Act 1998: Cookies and log files are – as shown above – devices for surveillance. Although the Convention and the Human Rights Act are designed to protect individuals from abuse by public bodies, on their base the right to respect for private and family life can be at least enforced against these entities (keywords: e-government, state universities), if cookies or log files of these entities are violating this right.[27]

Aware of the above-mentioned trend and the fact that the legal bases were and still are inconsistent across the EU-Member-States, eg "[…] neither English nor Scots law currently recognises any general right to privacy […]",[28] the EU has tried to bring uniformity in the law of collecting and processing data: The Data Protection Directive 1995[29] was the first important step in this direction.

3.1 Data Protection Directive

The object of the Directive 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. "Personal data" is defined in Art 2, a of the Directive as "[...] any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". The Directive prohibits the

[25] Cp Ian J. Lloyd, Information Technology Law (2000) 1 et sqq.
[26] Http://www.echr.coe.int/Convention/webConvenENG.pdf (1/22/2003).
[27] Gwyndaf-Roberts, PDP 2001, 1.6(4) says: "It is still unsettled whether a business that is not a public body, within the meaning of the Human Rights Act, will come under the application of Article 8."
[28] Lloyd, Information Technology Law 205.
[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal 1995 L 281, 31.

processing of special categories of data, namely sensitive data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life as long as there is no exception available (Art 8).

According to Art 3 of the Directive, the directive shall apply to the processing of personal data wholly or partly by automatic means. Thus, there is no doubt that the Directive is applicable on the processing of personal data on the Internet. Looking at cookies and log files the first issue becomes obvious: Are the data that are stored in cookies or log files "personal data" of a natural person (or can the data even be subsumed under a special category)? Some national law concretise the notion "personal data":

- Section 1 of the UK Data Protection Act 1998 defines "personal data" as data "[…] which relate to a living individual who can be identified […] from those data […] which is in the possession of, or is likely to come into the possession of, the data controller." It is not necessary that the provider really identifies the user but he has to have the possibility to do so (cp even "likely to come into the possession").
- Another example is Sec 4 of the Data Protection Act 2000 in Austria: Data is not "personal data" if the necessary additional information cannot be procured by legal means – again it is not necessary for the applicability that the provider really identifies the user.

Excursus 1: Personal Data – Contradictions with the Directive?!

The Data Protection Directive determines minimum standards; the Member-States can pass national laws with wider protection but are not allowed to restrict it (cp the exceptions in Art 13). Nevertheless, some national laws restrict the applicability of their data protection law by defining personal data too strict – therefore, according to the "effet utile"[30] this restriction are not applicable if the data processor is the state/government: If the state/government runs a website or is a service provider (eg

[30] Cp ECHR, Judgment of the Court (Fifth Chamber) of 15 June 1995; Commission of the European Communities v Grand Duchy of Luxembourg, C-220/94, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=61994J0220&model=guichett (1/20/2003).

universities) for the evaluation the guidelines of the directive have to be consulted. However, the directive cannot directly effect the situation between two private entities,[31] but if a private entity suffers a damage (from another) because the state does not provide an adequate protection, "state liability" can be claimed – the state has to recover the losses.[32]

- The UK Data Protection Act 1998 defines "personal data" only as data "[…] which relate to a living [ecce!] individual […]". This restriction contradicts the Directive which protects "[…] any information relating to an identified or identifiable natural person […]".The consequence is that the protection of the UK Act has to be expanded to all (living or dead) individuals, if the state is the data processor (of the cookies or the log files).
- Sec 1 of the Austrian Data Protection Act 2000 (a Constitutional Provision): "[…] Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection [ecce!]. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject. […]"[33] This restriction contradicts the Directive and the regulation has to be read without the requirement of "an interest deserving such protection". The restriction can obviously effect the evaluation of cookies or log files, but is not legally allowed according to the Community Law; thus, this restriction is irrelevant if the state/government is the data processor (of the cookies or the log files).

Recapitulating, the evaluation of cookies and log files has to be done by consulting the national data protection laws, apart from the case, when the obligations of the directive, which were not fulfilled and the state/government is the data processor.

[31] Cp European Court of Justice, Case C-91/92, Faccini Dori.
[32] Cp European Court of Justice, Cases C-6/90 and 9/90, Francovich.
[33] Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000), http://www.bka.gv.at/datenschutz/dsg2000e.pdf (1/20/2003).

3.1.1 Cookies and Personal Data

The web server "amazon.co.uk" stored the following cookie on the author's computer and named it "max@amazon.co[1].txt":

"session-id 026-8096756-7202866 amazon.co.uk/1024 886571008 29540777 853117440 29539485 * session-id-time 1043193600 amazon.co.uk/ 1024 886571008 29540777 853117440 29539485 * ubid-acbuk 432-7682679-2483237 amazon.co.uk/ 1024 2679150208 31961202 858617440 29539485 *".

Prima facie these data are cryptical numbers without any relation to an identifiable natural person (the author). And here starts the obvious problem for the legal evaluation of cookies: As it is up to the web server to create the name-value pairs and even to encrypt it, it can only be said by a case-by-case evaluation (sometimes only with the help of the provider)[34] if a cookie contains personal data. However, if the identification number (cp Art 2, a Data Protection Directive) in the cookie refers to personal data, like a customer list, the cookie contains personal data (cp sec 1 (1) UK Data Protection Act 1998): Eg the cookie of amazon.co.uk contains personals data after the author has identified himself (otherwise he would not get the ordered goods), if these data are combined. Because cookies are named "username@creating-web-server.txt" the web server at least knows the (system)-username of the user, which also could lead to an identification (eg if the username is firstname.surename). (Persistent) cookies allow permanent and unique identifier to be sent systematically with every information request; so it can be "waited" until the user identifies himself somehow and then analyse the collected (till then anonymous) data. IP addresses in contrast – as mentioned above – remain relatively weak identifier: They can be dynamic, be hidden behind proxy servers or be used by several users. The big advantage of cookies is their usability (for the provider) and that they allow a much better personalisation than eg IP-addresses.[35]

Recapitulating, cookies contain personal data if there is the possibility to combine them with other data, which make it possible to identify the user.[36] The main problem for the legal evaluation of cookies are their intransparency; although cookies are stored and are readable on the computer of the user, they are incomprehensible, because the

[34] Cp Art 10 of the Directive.
[35] Cp European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal data, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm.
[36] It is not necessary that the combination is really done – according to the wording of the Directive, the possibility is enough ("identifiable").

name/valid pairs are "encrypted" (cp beneath, the information obligation of the controller).

3.1.2 Log Files and Personal Data

Beneath a log file from the (virtual) server "it-law.at" as an example:

"130.159.254.2 - [20/Jan/2003:00:35:33 0000] "GET /main.htm HTTP/1.1" 200 11631 "http://www.univie.ac.at/lg-informationsrecht/profil/index.htm" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"".[37]

Here is a brief explanation what the entries mean:

- "130.159.254.2": The IP-address of the user (a "Whois lookup"[38] shows that the visitor came from the network of the University of Strathclyde – netname: STRATH);
- "20/Jan/2003:00:35:33": Date and Time of the entry;
- "0000": Time difference to Greenwich Mean Time (GMT - Universal Time);
- "GET": The action that was requested by the user (here: To see/get the webpage);
- "main.htm HTTP/1.1": Object-retrieve the page main.htm with the Hyper Text Transfer Protocol 1.1;
- "200": Status code (200 means the task has been completed);
- "11631": Size of (the transferred) object, in bytes;
- "http://www.univie.ac.at/lg-informationsrecht/profil/index.htm": The referring URL (this particular page was accessed from the website of the "LL.M. Universitätslehrgangs für Informationsrecht und Rechtsinformation in Vienna");
- "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)": Is the browser / version and platform of the user (the user was using Microsoft Internet Explorer 5.5 and the Windows 2000 operating system).

Prima vista log files only store computer-based data. As mentioned above, every web server logs the traffic and requests and sometimes servers, more precisely the providers, can connect the computer-based data to an individual person (eg the access provider of the user by using the customer list). If the content provider and the access provider is

[37] Note that some of these entries may be in a different order in other log files.
[38] Eg: http://www.ripe.net/perl/whois (1/20/2003).

identical, he can find out the individual user very easily. And if the user has individualized himself (eg with username and password and domicile – eg at amazon.co.uk to order goods) the content provider can use the log files to analyse the movements of the individual user with the help of the IP-address.

Recapitulating it cannot be generalized that every log file contains personal data but in the case of the access provider it is obvious. Again only an evaluation on a case-by-case base can be made.

3.1.3 Criteria for Making Data Processing Legitimate

As Art 7 of the Data Protection Directive determines, the processing of personal data is prohibited as long as there is no exception ("[…] personal data may be processed only if […]"). Even if one of the exceptions is available, data must be collected for specified, explicit and legitimate purposes and must not be processed further in a way incompatible with those purposes. The data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and furthermore, it must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified (Art 6).

So there has to be a check in two/three steps:

- Are the processed data, personal data?
- Is a criteria available that make the processing legitimate?
- Are the legal circumstances for keeping the data stored (the way they are) present?

3.1.3.1 Cookies

If the data of the cookie can identify a natural person (data subject), the provider of the web server needs a legitimation for processing the data:

- The Data Protection Directives follow the idea of the "informational self-determination"[39] and determines that personal data can be processed if "the data subject has unambiguously given his consent;" (Art 7, a). Only because the browser accepts (every kind of) cookie stored on the user's computer, that does not mean that the user has unambiguously given his consent: The consent is defined in Art 2, h of the Directive: "[T]he data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." Even if there is a cookie-warning by the browser, the information provided ("xyz wants to store a cookie on your computer") is in the author's point of view not enough for an "informed consent" in terms of the directive. Even by looking at the cookie-file (cp the above-shown one) the content and the consequences of its' processing are less than clear. So only if the provider of the web server presents the details (eg on the Website) before (ecce!) storing the cookie, the data subject's consent is legally possible (cp beneath for the circumstances of providing the information).
- Another criteria for making data processing legitimate is that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Art 7, b). Again it is not possible to generalize: Some data of cookies may be necessary for the performance of the contract: Eg the storage in the "e-trolley" is allowed (cp the obligation of sending an acknowledgement according to Art 11 E-Commerce Directive[40]). Nevertheless, because of the "economy of data"-principle the data (and the details which sites have been visited) must be deleted as soon as possible, so at least after completing the order.

Under the UK Data Protection Act 1998 the key provisions are that the personal data must be processed fairly and lawfully and that the data subject must be aware of the purpose for which the data is being used. For the fair and lawful processing the user's consent is needed (Schedule 2, 1) or the processing is necessary for the performance of

[39] Cp Llyod, Information Technology Law 83.
[40] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal L 2000/178, 1.

a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract (schedule 2, 2). According to the guidelines of the Data Protection Directive (Art 7: "[…] may be processed only if: (a) the data subject has unambiguously given his consent; […]") and the Schedule 1 of the UK Data Protection Act ("[…] shall not be processed unless – […]") the user has to opt-in for the use of a cookie, if personal data is processed. The opt-in-system means that the use of cookies is illegal as long as there is no (implicit) consent.[41] *Mercer* argues that a "positive consent" (with the meaning of explicit?) for the download of a cookie is necessary.[42] The Directive and the UK Act only claim an (informed) consent, as long as there is no sensitive personal data processed, where an explicit consent is necessary (Art 8 of the Directive; Schedule 2 of the UK Act). As in most Member-State the consent is a deed poll / unilateral declaration of intention, it depends on the legal requirements for such declarations, how the consent come into existence: Eg in the UK and Austria the (informed) consent can also be given implicit; the processing is lawfully if there is no doubt that the user wants the cookie stored even if he has not given his explicit consent.

As mentioned above, it is possible that cookies contain special categories of data (sensitive data) in the terms of Art 8 of the Directive resp sec 2 of the UK Data Protection Act; eg data stored from a search for a catholic church; from a booking of a flight and ordering kosher food; from a order of books on sexual or political views; from a visit on medical websites; and so on. The provider needs in this cases the explicit consent of the user to store the cookie.

3.1.3.2 Log Files

If the data of the log file can identify a natural person (data subject), the provider of the web server needs a legitimation for processing the data in the log file:

- He needs the consent of the user or
- the data processing is necessary for fulfilling a contract; as mentioned above, log files could be necessary for the billing – but in this case there are special

[41] Cp the discussion about the opt-in and opt-out approach: Llyod, Information Technology Law 112.
[42] Colin Mercer, "Overview", Corp Briefing 2002, 16.3(1).

regulations in the ISDN-Directive and the E-Communication Directive which has to be transposed until the 31st of October 2003 (cp beneath).

Log files can contain special categories of data (sensitive data - cp the examples above). Because it is (nearly) unpredictable if sensitive data will be stored in log files, every provider should get the explicit consent of the user for storing the log files.

3.1.3.3 Obligations Even If Legitimate Processing

The provider of the web server who stores cookies with personal data as well as the provider who stores personal data in log files are data controllers in the terms of the data protection regulations. The "controller" is defined in Art 2, h of the Data Protection Directive 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 controller has to fulfil several obligations: He has to provide information (Art 10); has to follow several rights of the data subject (Art 12 et sqq); has to implement appropriate technical and organizational measures to protect data (Art 17); and has to notify the supervisory authority (Art 18). These guidelines were transposed into national laws of the Member States. Thus, in the case of processing personal data in cookies or log files

- the provider is considered "data controller" in the terms of the UK Data Protection Act 1998. Therefore, he has to file a notification with the Information Commissioner, who maintains a public register of data controllers. The notification has to contain a general description of the data processing (should be identical with the information provided to the user for the consent). The controller has to pay an annual fee of GBP 35.- and it is a criminal offence not to notify.[43]
- the provider has to comply with the Seventh Principle to provide appropriate measures for ensuring the safety of the processed data (eg encrypting the data; but this measure makes it more difficult to distinguish personal from non-personal data).
- the provider has to fulfil the obligations to inform the data subject. "The speed of data flows on the Internet cannot be used as an excuse for not fulfilling the

[43] Cp Gwyndaf-Roberts, PDP 2001, 1.6(4).

obligations […]"[44] According to Schedule 1, Part II, sec 2 of the Data Protection Act the provider has to inform the user that personal data is processed, about the identity of the data controller (can be different from the provider of the website, cp DoubleClick), the purpose for which the data are processed (even if the cookie is necessary for technical reasons), and further information (what data is stored, who can read it, for how long it is stored, disclosure of data to third parties, …) before (ecce!) the cookie resp the log files are stored.

- and he has to follow the "economy of data" principle:

3.1.4 "Economy of Data"-Principle

According to the "economy of data principle" (Art 6 para 1, e of the Data Protection Directive) personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The named principle can be found in most national laws in the EU: Cp sec 6 of the Austrian Data Protection Act 2000, which requires to delete data which are no longer necessary for the legitimate purpose or cp the fifth principle of the UK Data Protection Act 1998; according to this principle personal data shall not be processed / kept for longer than is necessary for the (legitimate) purpose of the processing.

3.1.4.1 Cookies

It could be argued, that a stored cookie is not kept by the controller and not processed as long as the user does not visit the web server again. But the controller (when the cookie is created and stored) has the control over the expiring date (which makes a processing necessary: The expiring date has to be compared with the actual date) and "stays" therefore a controller.

(Session) cookies, which are stored for technical reasons (without consent) have to be deleted as they are not necessary anymore, normally at the end of the visit. But it can be argued that they have to be kept till the user quits the browser. Even if the user has given his consent, he must be aware of how long the cookie will be stored.

---

[44] European Commission, "Working Document: Privacy on the Internet", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf.

3.1.4.2 Log Files

Unless the user has given his consent, the "economy of data"-principle leads for log files to the consequence that only these data can be and as long be stored as they are necessary: Data which provide no "special" information (eg for the conduit of the data; for the billing) have to be deleted or made anonymous immediately.

3.1.5 Applicable Law

The really new issue of legal evaluating appearances on the Internet is the disappearance of national boarders. It is essential to have at least an EU-wide approach to the issues of cookies and log files. Art 4 of the Data Protection Directive determines for the application of national law that

> "1. [e]ach 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."

3.1.5.1 Cookies

According to Art 4 of the directive the provider which stores cookies has to obey his national data protection law if he has his domicile in the EU (if several domiciles, he has to abide by every law of each such domicile). According to the directive even for providers that are not domiciled in a Member-State, the national law of the Member-state (also applicable for EEA States) of the user shall be applicable, because the provider "makes use of equiment" – the computer of the user – when he stores a cookie: The text file is installed on the hard drive of the user and his computer receives, stores and sends back information to the server. This raises the next issue, which can only be mentioned in this paper: The Transfer of personal data to third countries (Art 25 et sqq of the Directive; the eighth principle of the UK Data Protection Act 1998; sec 12 et sqq of the Austrian Data Protection Act 2000).

In sec 5 of the UK Data Protection Act 1998 the guidelines of the Directive are transposed; it determines that the Act is also applicable for data controllers neither established in the UK nor in any other EEA State but using equipment in the UK for processing the data otherwise than for the purpose of transit through the UK. So every provider who stores cookies which contain personal data in the UK has to obey the Act and if he is not established in the UK, in the terms of sec 5, he has to nominate for the purposes of the Act a representative established in the UK. Nearly no provider fulfils the last obligation – one point where the Act seems to be unenforceable in the reality (on the Internet).

The Austrian Data Protection Act 2000 determines in sec 3 (1) that "[t]he provisions of this Federal Act shall be applied to the use of personal data in Austria." The "use" is defined in sec 4, no 8 as "all kinds of operations with Data of a Data Application, meaning both processing of data (sub-para 9) and transmission of Data (sub-para12);" and sub-para 9 defines "processing of data" as "the collection, recording, storing, sorting, comparing, modification, interlinkeage, reproduction, consultation, output, use, committing (No. 11), blocking, erasure or destruction or any other kind of operation with data of a data application by the controller or processor except the transmission of Data (sub-para. 12)". Again the collection of the data and the storing of the cookies on the computer of the user in Austria leads to the application of the Austrian Data

Protection Act, unless the data controller has no domicile in Austria but is established in another EU-Member-State; then the law of the origin is applicable. According to sec 6 (3) of the Austrian Act a controller who does not reside in the EU has to name a representative residing in Austria who can be held responsible in place of the controller, without prejudice to the possibility of legal measures against the controller himself. However, in practice, this obligation is not fulfilled on the Internet.

3.1.5.2 Log Files

Log files and the data stored in it are created on the web server; thus, the domicile of the user is not important for the applicable law. The provider has to obey the national law of his domicile: if he is not established in the EU but uses a web server that is located in a Member-State, the law of this Member-State is applicable (cp above).

3.2 ISDN-Directive 97/66/EC

In the last years of the last century the EU had to face the "new generation" of telecommunication: The digital services. Processing of transmitted data became much easier with ISDN[45] (and the Internet) and needed regulation; on the other hand, the limitation of the Data Protection Directive seemed to be too restrictive on certain procedures. The ISDN-Directive (or Telecommunications Privacy Directive)[46] should solve these issues. Even if the directive refers to the telecommunication sector in general and uses terms such as "calls", which allude to traditional and ISDN telephony, the European Commission sees the directive applicable to the Internet: "Nevertheless, it is usually possible to include Internet services within the scope of application of the directive although […] some difficulties have to be faced."[47]

The directive determines in Art 5 (Confidentiality of the communications) that

[45] ISDN = Integrated Services Digital Network.
[46] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector Official Journal 1998 L 24, 1.
[47] European Commission, "Working Document: Privacy on the Internet", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf.

> "1. Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. […]"

So independently, if an access provider runs a "public telecommunications network" in the terms of Art 2, c of the directive (the question of providing infrastructure), he provides a "'telecommunications service", a service whose provision consists wholly or partly in the transmission and routing of signals on "telecommunications networks" (Art 2, d). The content provider and a provider storing cookies (normally) does not provide a telecommunication service in terms of the directive, as a Working Paper of the European Commission points out: "It is unclear whether the core activities of Doubleclick, Engage and other advisers can be regarded as a telecommunications service or not. It appears that they do not transmit and route signals […]. They provide content information to be placed on the requested webpage, making use of the available telecommunication infrastructure and networks." So for providers who use cookies the following regulations of the ISDN-Directive are not applicable – but applicable to those who store traffic data and process log files:

> "[…] In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14 (1).
>
> 2. Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication."

So access/interconnection providers are allowed to store data (in log files) which are needed for billing. Nevertheless, they have to mind Art 6 about traffic and billing data:

> "1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a […] publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.
>
> 2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex[48] may be processed. Such processing is permissible

[48] Data containing the:

only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

[…]"

Even if the access provider offers his service with a flat rate, it can be argued that he needs the log files to prove that the service was available for the user ("bill may lawfully be challenged or payment may be pursued"). In the author's point of view, this argument contradicts the scope of the Directive (cp Art 1); therefore, log file data must be deleted or made anonymous as soon as technically possible, unless the user has given his (informed) consent.

Excursus 2: Cookies – Trespassing?

Gwyndaf-Roberts argues that the use of cookies without a user's consent could amount to trespass to property; on the other hand she points out that in order to prove trespass, the claimant must be able to show that there had been a direct interference with property, which could be difficult to establish in the case of cookies. Especially in Scotland an action based on trespassing would not be successful: The delict of trespass relates almost exclusively to the use without permission of heritage (land and buildings).[49]

3.3 E-Communication Directive 2002/58/EC

As the Internet had become more and more important as an economic factor and the political scope across the globe was to enforce e-commerce and the trust in it, there was the need to ensure a EU-wide level of protection of the right to privacy, with respect to

- number or identification of the subscriber station,
- address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,
- type, starting time and duration of the calls made and/or the data volume transmitted,
- date of the call/service,
- other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.

[49] Lilian Edwards, "Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail?", http://www.law.ed.ac.uk/script/spam.htm (12/19/2002).

the processing of personal data in the electronic communication. This need should be satisfied by the E-Communication Directive that repeals the ISDN-Directive (cp Art 19 of the E-Communication Directive) and has to be transposed by the 31st of October 2003. The directive provides for the first time regulations that are directly focused on cookies and log files (on the Internet):

3.3.1 Cookies

Art 5 para 3 determines that the use of electronic communications networks to store information (to store the cookie in the computer) or to gain access to information stored in the terminal equipment of a user (to read the cookie) is only allowed on condition that the user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This regulation does not distinguish information (data) from personal data – cp the above mentioned issue of the applicability of the data protection regulations. Therefore, the provider of web services needs the informed consent (in terms of Art 2, h Data Protection Directive) independently if the processed data is personal data or not. Scope of the regulation is the protection of the private sphere of the users according to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Recital 24 names explicit as a danger for the private sphere (and not only data) spyware, web bugs, hidden identifiers and other similar devices that should be allowed only for legitimate purposes with the knowledge of the user. But, as the recital 25 points out, such devices, eg "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in online transactions. So according to the E-Communication Directive the above-mentioned regulation shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the user.

The fundamental idea of all regulations in the field of data protection, and communication generally, is to find solutions that are independent of the concrete used technology. This means for cookies, that it is possible that the provider has also to obey

the regulations according "traffic data". As mentioned above, the web server can store all kinds of data in the cookie; so it is possible that a cookies also contains traffic data in the terms of the E-Communication Directive (cp beneath). In this case Art 6 of the directive is applicable and the provider has to give the user the possibility to withdraw his consent for the processing of traffic data at any time (cp beneath).

Recapitulating, the main change the E-Communication Directive makes for cookies is that for the legitimate storage of all (ecce!) data the consent or a technical reason must be available. In the author's point of view, this will lead in the practice to an extensive interpretation of the "need for technical reasons". Nevertheless, the importance of the consent (as needed for the opt-in-system) will increase (cp beneath).

3.3.2 Log Files

Although potentially log files can store every kind of data (even the transmitted content), normally "only" traffic data is stored. According to Art 2 of the E-Communication Directive traffic data "means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". Recital 15 says that traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network. Subsequently, the E-Communication Directive focuses in Art 5 (also) on log files on the Internet while following the wording the Art 5 of the ISDN-Directive (cp above). But the directive introduces a new exception in para 1:

> "[…] This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality."

This exception could again lead to an extensive interpretation of "technical needs". For the use of traffic data the E-Communication Directive adopts the Art 6 of the ISDN-Directive, but changes the guidelines concerning the use of data for the purpose of marketing:

> "[…]

> 3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.
> 4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.
> […]"

According to the new guidelines, the provider can use traffic data for the purpose of marketing for any (ecce!) electronic communications service and not only the own one. The informed (cp para 4) consent must be able to withdraw at any time.

Para 4 deals obviously with the above mentioned issue of the different systems for a legitimate processing (opt-in or opt-out). In the author's point of view this guideline leads to more confusion than clarification: The Data Protection Directive determines an opt-in-system with the need of an informed (ecce!) consent. So the data controller always has to inform the user before the user can give his consent (so para 4 does not provide any new regulation).

That the provider has to give the user the possibility to withdraw his consent for the processing of traffic data for the purpose of marketing at any time, raises an issue in the whole system of consent: What consequences can there be, if the user withdraws? Can the provider cancel his service (cp for providers of telephone service: Art 5 of the ONP Directive[50])? Must the provider offer his service although the user does not give his consent from the beginning? Cp beneath more about the opportunity to refuse.

[50] Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment, Official Journal L 1998/101, 24.

Recapitulating, generally providers need the consent of the user to store log files unless the data is necessary for technical reasons or billing (cp above the ISDN-Directive). Even if the storage of the data is technically necessary, according to the "data economy"-principle, the data has to be deleted or made anonymous as soon as possible.

3.3.3 Unambiguously Given and Informed Consent

The E-Communication Directive determines that the consent of the user is necessary for cookies and log files as long as there are no technical or billing reasons for storing the data. Art 2 of the directive refers for the definition of the "consent" to the Data Protection Directive (cp above). The "unambiguously given and informed consent" presumes the provision of the necessary information. Recital 25 of the E-Communication Directive says that the methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible even though the information may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

"As user-friendly as possible" means that the information cannot be "hidden" in general terms and conditions (somewhere on the website) but that the user has to be aware of the circumstances before the cookie or the log file are stored. As a result for cookies, the information has to be provided on the homepage of the website or even in an extra pop-up-window. Of course this main information can refer to more detailed information eg in the privacy policy or in the general terms and conditions but the "first information" has to specify, in generally understandable language, which information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie.[51] There is the fear that especially "third party cookies" will lead to a "pop-up jungle": The third party, as the data controller, has to provide the information and in rare cases this third party will have influence on the content of the website; therefore the third party will provide a pop-up-window which is loaded from his web server. The

[51] Cp European Commission, "Recommendation 1/99", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm.

"pop-up-jungle" will make it impossible to browse the web quickly anymore. Another fear is that this regulation is the first step of the EU to regulate the architecture of the Internet and this will slow down of the invention of new services.

The consequence for (access) providers will be much longer privacy policy clauses in their contracts. Because it is possible that even sensitive data is stored in log files, providers will try to get explicit consent to a large extent.

3.3.4 User Bans Cookies / Opportunity to Refuse

According to Art 5 no 3 of the E-Communication Directive the user has to have the opportunity to refuse every cookie (independently, if it consists personal data or not). But as mentioned above, there are already several (technical) possibilities for the user to ban cookies from his computer at the moment: Browser settings, firewalls or special cookie-software[52]. Using this features leads to the following consequences: A lot of websites, eg www.msn.com, refuse the access to the whole or at least some of their functions. Theirfore, the user is "forced"[53] to accept the cookies. Recital 25 of the E-Communication Directive deals with this issue and says that the "[a]ccess to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose." The notion "legitimate purpose" makes it less than crystal clear, when the blocking of content is / will be allowed: The "informational self-determination" (as generally the self-determination) is a principle of (every) democratic society; on the other hand, the (freely given) consent is absurd if the user has no other possibility to use the Internet (in the worst case as a whole) unless he gives his consent. This leads to the question if "freely given" has to be interpreted as "independently from providing the service". According to the interpreted scope of the regulation, the provider is not allowed to refuse the whole (ecce!) service, if the user does not give his consent – another uncertainty how the Member-States will deal with this topic. This will also have practical effects on the Internet: A lot of the content on the www is free, because the user gives his (valuable) data to the provider; if the provider will be forced to provide the service without getting the data, the intention of the EU to help the e-commerce could lead to the opposite.

[52] Eg the shareware: Cache, Cookie & Windows Cleaner 7.7.01, available over www.tucows.com (1/22/2003).
[53] Cp Gwyndaf-Roberts, PDP 2001, 1.6(4).

The E-Communication Directive determines in Art 6 para 3 that an explicit possibility for users to withdraw their consent for the processing of traffic data for the purpose of marketing at any time has to be provided. It could be argued that this explicit right leads to the effect that the consent (in the terms of the Data Protection Directive and the E Communication Directive) cannot be withdrawn. This argument could raise inconsistency in connection with the “freely given consent” and the “rights of the data subject” according to the Data Protection Directive. In the author’s point of view, it is a principle of the EU data protection regulations, that any consent can be withdrawn at any time.

Independently of the above raised issues, the refuse of service could also raise competition law issues.

4 Evaluation

Although it can be argued that "[t]he problem, however, is not so much the technology. The TCP/IP protocols are essentially neutral […]",[54] cookies and log files – as originally purely technological features – have become a (political) issue; they are seen as a danger for the trust in e-commerce. Even if the Data Protection Directive (and its' transposition to the national laws of the Member-States) is already protecting the users in connection with the use of cookies and log files, the applicability of the regulations is not crystal clear; it depends on the evaluation if the cookies and log files contain personal data or not; and this can only be answered on a case-by-case evaluation, which leads in the practice to nebulosity if the processing of cookies and log files is legitimate in the particular case. The E-Communication Directive has (therefore) a much broader approach: Independently if the data is personal data or not, the use in cookies and log files is restricted: The processing is only allowed if, inter alia, it is technologically necessary or the user has given his consent (if they are sensitive data, even his explicit consent is necessary).

While according to *Singleton* the UK Direct Marketing Association welcomed the decision that cookies can be placed on consumers' PCs by website owners, provided consumers are given clear and precise information about the reasons for, and the use of, cookies,[55] the journal *IT Law Today* reports that the Union of Industrial and Employers' Confederations of Europe (Unice) fears that an indiscriminate ban on cookies would shy off consumers and harm business and affect to the contrary the EU's much vaunted plan to get Europe online.[56] And in the author's point of view this fear is not totally absurd:

- Many services on the Internet (esp in the www) are for free, because the user gives the provider his (valuable) data; if the consent can be withdrawn at any time, a lot of services could be closed.
- The informed consent for every kind of data will lead to a "pop-up-jungle": The user will spend a lot of time reading all kind of information concerning the use of his data – a fact that could annoy and also frighten users.

[54] Llyod, Information Technology Law 32.
[55] Susan Singleton, "A Legal Guide to Advertising On The Web", ITLT 2002, 10.6(9).
[56] ITLT, "EU Cookies Law Criticised", ITLT 2002, 10.4(5).

On the other hand, as more and more people spend nearly all their (working-)day and even spare-time in front of the computer connected to the Internet, there is a need for clear regulations of processing of their data – even if it is not personal data in the terms of the data protection regulations. The convergence of technology (telephone, mobile and the Internet) and the mass of processed data, which cannot be handled on a case-by-case bases, if they are personal or not anymore, and the obvious importance of the trust of the consumer and the businesses in e-commerce, made the E-Communication Directive necessary. Although the directive raises several (new) issues (not only) in the connection with cookies and log files, it is an important EU-wide step towards the protection of the private sphere in the context of electronic communication.

The E-Communication Directive will prohibit at least one issue in connection with cookies (and log files): The "uninformed (ecce!) transparent Internet user"; even if the consequences will be a "pop-up-jungle".

5 Bibliography

Patrich Brauch, "Von wegen Incognito", c't 2002, H 19, 128.

Michael Chissick, "Data Protection In The Electronic Commerce Era", CTLR 1999, 5(4).

European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, "Working document: Processing of Personal Data on the Internet", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp16en.htm (1/20/2003).

European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal data, "Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm (1/20/2003).

European Commission, "Working Document: Privacy on the Internet – An integrated EU Approach to On-line Data Protection", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf (1/22/2003).

European Commission, "Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6", http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp58_en.pdf (1/20/2003).

Lilian Edwards, "Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail?", http://www.law.ed.ac.uk/script/spam.htm (12/19/2002).

Sarah Gwyndaf-Roberts, "Cookies", PDP 2001, 1.6(4).

Jean Hughes / Edward Black / Carolyn Chia, "Data Protection Compliance For Financial Institutions – A UK Perspective", FSB 2002, 2.8(5);

ITLT, Editor's Comment, "Computers and Information Technology", ITLT 2002, 10.4(3).

ITLT, "EU Cookies Law Criticised", ITLT 2002, 10.4(5).

Lawrence Lessig, Future of Ideas (2001)

Ian J. Lloyd, Information Technology Law (2000)

Viktor Mayer-Schönberger, "The Cookie Concept", http://www.cookiecentral.com/content.phtml?area=2&id=1 (1/10/2003).

Brain Marshall, "How Internet Cookies Work", http://www.howstuffworks.com/cookie1.htm (1/15/03).

Victor Mayer-Schönberger, "The Internet and Privacy Legislation: Cookies for a Treat",

http://www.wvu.edu/~wvjolt/Arch/Mayer/Mayer.htm (1/22/2003).

Colin Mercer, "Overview", Corp Briefing 2002, 16.3(1).

Martin H. Samson, "Internet Law – Cookies", http://www.phillipsnizer.com/int-cookies.htm (1/20/2003

Susan Singleton, "A Legal Guide to Advertising On The Web", ITLT 2002, 10.6(9).

Websites:

http://www.bka.gv.at/datenschutz/dsg2000e.pdf (1/20/2003).

Http://www.cookiecentral.com/content.phtml?area=4&id=11 (1/15/2003).

http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=& (1/20/2003).

Http://www.echr.coe.int/Convention/webConvenENG.pdf (1/22/2003).

http://google.com (1/19/2003).

Http://www.marketingterms.com/dictionary/log_file/ (1/20/2003).

http://www.ripe.net/perl/whois (1/24/2003).

http://www.visualware.com (1/22/2003).

http://www.wichtig.de/ (Zenoogle) (1/24/2003).

Case-Law

ECHR, Judgment of the Court (Fifth Chamber) of 15 June 1995; Commission of the European Communities v Grand Duchy of Luxembourg, C-220/94, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=61994J0220&model=guichett (1/20/2003).

European Court of Justice, Case C-91/92, Faccini Dori.

European Court of Justice, Cases C-6/90 and 9/90, Francovich.