The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?

FREDERIC DEBUSSERE*

One day in June 1994, Lou Montulli sat down at his keyboard to fix one of the biggest problems facing the fledging World Wide Web – and, as so often happens in the world of technology, he created another one.¹

1 Introduction

The development of the information society is characterized by the introduction of new electronic services available through different types of technologies and devices. Publicly available electronic communications services create new possibilities for users, governments and businesses. However, at the same time, these services have large capacities and possibilities for processing personal data. For instance, one of the technologies that are crucial in the functioning of the Internet, so-called ‘cookies’, are used to track an individual’s movements on a website and even among different websites, and can be used to store information that the individual supplies to another website including his name, address, credit card number, etc. This is of course of great advantage to advertisers who can create profiles of an individual and target their advertisements to match...
the individual’s interests, but it is problematic in light of the fundamental right to privacy.

In the United States (‘US’), there have already been some lawsuits against companies and organizations that used cookies to gather information about Internet users. The most notorious example of such a case involved the Delaware-based advertising company DoubleClick, Inc.² This company’s marketing niche is its promise to advertisers to place their ads in front of persons most likely to respond to them. To this end, DoubleClick collects and analyses an extensive amount of information about Internet users. It accomplishes this by invisibly placing a cookie on the hard drive of individuals who visit one of the 11,000 ‘DoubleClick-affiliated’ websites, which enables DoubleClick to track those individuals’ clickstream data. The collected information is then compiled into detailed profiles of Internet users. DoubleClick currently has a stockpile of more than 100 million such profiles.³

In June 1999, DoubleClick caused a public outcry when it purchased Abacus Direct Corp. for more than one billion dollars. Abacus was a direct-marketing services company that maintained a vast database of names, addresses, telephone numbers, retail purchasing habits and other personal information on approximately ninety percent of American households, which it sold to direct marketing companies. Through the purchase, DoubleClick intended to combine its massive database of largely anonymous online profiles with Abacus’ personally identifiable offline data, so that DoubleClick would be able to create a super database capable of matching individuals’ online activities with their names and addresses. In March 2000, after a Federal Trade Commission investigation into whether DoubleClick’s consumer data policies constituted unfair or deceptive trade practices, several state and federal consumer class actions raising a variety of statutory and common law tort claims and an investigation by some States, DoubleClick’s CEO announced that he had made a ‘mistake’ by planning to merge both companies databases and stated that DoubleClick would not undertake such merger until it reached an agreement with the US government and Internet industry regarding privacy standards. It agreed to postpone linking personally


identifiable information to anonymous user activity until the government and the industry could agree upon standards.4

Since the successful development of information society services is partly dependent on the confidence of users that their privacy will not be at risk, a legal framework is needed to protect individuals’ fundamental right to privacy and their personal data, while at the same time paying attention to legitimate interests of governments and businesses.

In this respect, on 12 July 2002, the European Parliament and the Council of the European Union (‘EU’) adopted Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (‘Directive 2002/58’).5 This Directive is part of a package of five new Directives that aim to reform the legal and regulatory framework of electronic communications services in the EU,6 and it repealed and replaced 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 (‘Directive 97/66’).7 The latter Directive aimed to translate the general personal data protection principles laid down in 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 (‘Directive 95/46’),8 into specific rules for the telecommunications sector. However, Directive 97/66 was already outdated at the moment of its adoption in 1997: it had been drawn up in the first half of the nineties and – as its title and terminology suggest – it applied only to the ‘telecommunications’ sector, whereas by 1997, the Internet and electronic communications had already begun to be used with regular frequency.9

---

4 In re DoubleClick, Inc. Privacy Litigation, supra note 2, at 505.
5 EU Official Journal 31 July 2002, L 201/37. The procedure file of the Directive, including all its preparatory documents, is available at http://wwwhl.europarl.eu.int/oeil/oeil_ViewDNL.ProcedureView?lang=2&procid=4483 (all websites referred to in this article were last visited on 31 July 2004).
9 The European Commission’s initial proposal dates from 1990 (COM(1990)314final) EU Official Journal 5 November 1990, C 277/12.)
Although the EU Article 29 Data Protection Working Party was of the opinion that this Directive also applied to the Internet and e-mails,\(^{10}\) it was still uncertain whether this was indeed the case, and the EU wanted to remove this uncertainty by adopting a new Directive.

Directive 2002/58 had to be implemented in national law by the EU Member States by 31 October 2003.\(^{11}\) However, nine Member States – Belgium, Germany, Greece, Finland, France, Luxembourg, the Netherlands, Portugal and Sweden – failed to do so, and in the beginning of December 2003, the European Commission opened infringement proceedings against them.\(^{12}\)

One of the innovative provisions of Directive 2002/58 is Article 5(3), as clarified by Recitals 24 and 25, which sets out a legal framework for the use of devices for storing or retrieving information, such as cookies.

This article aims to analyse this new EU legal framework for the use of cookies. First, it is described what cookies are, what types of cookies there are and what they can be used for. Second, it is explained why their use can be problematic in the light of privacy and personal data protection. Third, a critical analysis is made of the new European rules for the use of cookies.

### 2 Cookie Technology in a Nutshell

If an individual wants to visit a website or navigate from webpage to webpage within a website, then his webbrowser (for instance, Microsoft Internet Explorer or Netscape Navigator) sends a request to the server that operates the website. Upon receiving the request, the server then transmits to the individual’s webbrowser the information that constitutes the requested website or webpage. The communication between the individual’s webbrowser and the server that operates the website occurs by means of a protocol called HyperText Transfer Protocol (‘HTTP’). The file sent by the server to the webbrowser is preceded by an HTTP header, which is a set of ASCII strings following a special language called HyperText Markup Language (‘HTML’) and containing information about the server and the document being sent.\(^{13}\)

---


\(^{12}\) See http://europa.eu.int/rapid/start/cgi/guesten.ksh;p_action=getfile=g&doc=IP/03/16630&AGED&lg=EN&type=PDF.

HTTP differs from other protocols such as the File Transport Protocol (‘FTP’) in that it is a ‘stateless’ protocol, which means that each visit to a website and even each click within a website is seen by the website’s server as the first visit by the individual. Consequently, the server ‘forgets’ everything after each request, unless it can ‘mark’ a visitor to help remember it. It is at this point that cookies come into the picture: their technical purpose is to ‘maintain state’ between stateless HTTP communications. In other words, they help a server to remember an individual’s activities on the website(s) concerned.

As mentioned above, the cookie technology was invented in the mid-nineties by Lou Montulli, at that time a programmer at Netscape Communications. The term ‘cookies’ comes from the computer science term ‘magic cookie’ used by Unix programmers.14

A cookie is a text file of typically less than four kilobytes of memory that the server which operates the visited website places on the individual’s hard drive by means of an additional line added to the HTTP header. Contrary to some newspaper reports and US court opinions, a cookie is thus not an executable computer program or code and cannot function like a program.15 The syntax of the additional line in the HTTP header of an HTML document is as follows: ‘Set-Cookie: NAME=VALUE; expires=DATE; path=PATH; domain=DOMAIN_NAME; secure’.

NAME=VALUE is the name of the cookie and its value. This is the only required attribute in the Set-Cookie header; the others are optional.16 This is the globally unique identifier (‘GUID’) that the server specifically assigns to an individual and is the main component in the cookie’s tracking system; it is through this number that companies are able to identify exactly which websites or webpages an individual has visited before. In other words, it is the data that the website’s server wants passed back to it when a browser requests another page. It is this GUID that DoubleClick uses to target individual Web surfers and ensure that they do not see the same advertisement banner over and over again.17

14 A. Stuwart, ‘Mysteries About the Internet. Where Cookie Come From’, available at http://www.domino.power.com/issues/issue200207/cookie001.html. See also http://www.montulli.com/lou. A ‘magic cookie’ is defined as: ‘Something passed between routines or programs that enables the receiver to perform some operation; a capability ticket or opaque identifier. Especially used of small data objects that contain data encoded in a strange or intrinsically machine-dependent way. […] The phrase “it hands you a magic cookie” means it returns a result whose contents are not defined but which can be passed back to the same or some other program later.’ (see http://computing-dictionary.thefreedictionary.com/magic%20cookie).

15 See M. Brain, ‘How Internet Cookies Work’, HowStuffWorks, available at http://computer.howstuffworks.com/cookie1.htm. See, e.g., In re DoubleClick, Inc. Privacy Litigation, supra note 2, 502–03 (‘Cookies are computer programs commonly used by Web sites to store useful information […]’ (emphasis added)).


DATE is an attribute that determines how long the cookie persists on the individual’s hard drive. Its format is: ‘Wdy, DD-Mon-YYYY HH:MM:SS GMT’.\footnote{See Netscape Support Documentation, supra note 16.} If there is no expiration date, then the cookie is stored in memory only and is automatically erased when the individual unloads or closes his webbrowser; the cookie is then called a ‘session’ (or ‘transient’) cookie. Session cookies only store information in the form of a session identification and do thus not store any personally identifiable information.\footnote{Webopedia Computer Dictionary, available at http://www.webopedia.com/TERM/S/session_cookie.html.} However, if the DATE attribute refers to a date in the future, then the cookie is a so-called ‘persistent’ (or ‘permanent’ or ‘stored’) cookie and is saved in a file. Only such persistent cookies can be used to track an individual at several visits of one or more websites or webpages.\footnote{Webopedia Computer Dictionary, available at http://www.webopedia.com/TERM/P/persistent_cookie.html.} Setting the date for an existing cookie to be some day in the past deletes the cookie.

DOMAIN\_NAME is an attribute that contains the address of the server that sent the cookie and that will receive a copy of the cookie when the webbrowser requests a file from that server. It defaults to the server that set the cookie if it is not explicitly set in the ‘Set-Cookie:’ line. This attribute may be set to equal the subdomain that contains the server so that multiple servers in the same subdomain will receive the cookie from the webbrowser. This allows larger websites to coordinate multiple servers in the same subdomain. For instance, if the DOMAIN\_NAME equals www.company.com, then machines named one.company.com, two.company.com and three.company.com all receive the cookie from the webbrowser. The value of DOMAIN\_NAME is limited such that only hosts within the indicated subdomain may set a cookie for that subdomain.

PATH is an attribute that is used to further refine when a cookie is sent back to a server. When the PATH attribute is set, a cookie is only sent back to the server if both the DOMAIN\_NAME and the PATH match for the requested file.

‘Secure’ is an attribute that specifies that the cookie is only sent if a secure HTTP (‘HTTPS’) is being used. Since most websites do not require secure connections, this attribute defaults to false.\footnote{U.S. Department of Energy – Computer Incident Advisory Capability, ‘Information Bulletin. I-034: Internet Cookies’ (1998), available at http://www.ciac.org/ciac/bulletins/i-034.shtml.}

When applying the above to surfing to, for instance, the URL http://www.google.com, then the HTTP header (in HTML) of the response that Google’s server sends to the individual’s webbrowser may look like this:

```
HTTP/1.1 200 OK
Content-Length: 3059
Server: GWS/2.0
```
Once a cookie is installed on an individual’s hard drive for a particular website, then each time that individual surfs to and navigates through that website and requests a different webpage, the website’s server gains access to the current cookie. The information stored in the cookie is attached to every subsequent request from the web browser to the website’s server for a different webpage. After receiving the cookie’s information attached to the web browser’s request, the server may modify that information to reflect new or updated information. Together with the new webpage the individual requested, the server sends a revised cookie that replaces the old one. Thus, once installed on an individual’s hard drive, cookies facilitate a flow of communication back and forth between that hard drive and the website’s server.

3 Why Do Cookies Threaten Privacy?

The technical purpose of cookies is thus to make it possible that the server which operates a website can ‘remember’ that an individual visited that website or a webpage before; cookies allow websites to ‘tag’ their visitors with unique identifiers so that they can be identified each time they visit the website or webpage. In this way, cookies can be very useful things. For instance, if an individual wants to check his e-mail box via the World Wide Web, then the username and password that have to be typed, can be stored in a cookie, so that these data are automatically filled out the subsequent occasions the individual wants to check his e-mail and that he thus only has to type them once. In the case of electronic commerce, cookies can be used to retain a record of the items that one has ordered the previous time, so that one can view one’s shopping basket over a certain period of time. Cookies can also be used to personalize a website; for

---

23 See M.R. Siebecker, supra note 2, at 898.
24 It is important to note that cookies do not ‘gather’ information; the only data available in cookies is information that users themselves provide to websites and the server of the website then stores in cookies.
instance when an individual visits a multi-language website, a cookie can be used to remember the individual’s language preference.

In this context, it is important to distinguish between two separate types of information that can be stored in cookies: personally identifiable information and non-personally identifiable information. Personally identifiable information consists of data that is used to identify an individual and is mostly provided to the website by the individual himself, for instance in the context of electronic commerce. Such information, also called ‘transaction generated information’, can include, for instance, an individual’s name, address, phone number, e-mail address, credit card number, age, gender, income, marital status, number of children, health, political affiliation, social security number, occupation, lifestyle dimensions, leisure activities, type of car, Internet Protocol address, etc. Non-personally identifiable information is not linked to any particular personal information and typically consists of so-called ‘clickstream data’, for instance the number of times that an individual clicks on an online advertisement (‘banner’).

The potential harm of cookies does not lie in the information stored on the user’s computer itself, but in what companies can do with the information. It is a fact that a company that retrieves some personally identifiable information via cookies, for instance via electronic commerce, may have some knowledge of some characteristics of individuals. This is a legitimate concern, but in most cases the individual has provided the information himself and has consented to giving the information. In addition, since most websites have only the limited capability to read cookies from an individual’s hard drive that that website itself sent on a previous visit, it is hard for single information collecting companies to come to a real ‘dossier effect’. The real danger rather lies in so-called ‘online profiling’ by means of data mining. This consists of recording an individual’s online behaviour through the accumulation of clickstream and other forms of data into vast databases and the subsequent construction of ‘profiles’ of individuals based upon that record. In this context, a third party, usually an advertising agent, places cookies on individuals’

---


hard drives from its own servers. The clickstream data collected by such third parties is in some ways more comprehensive than those of single website owners because third parties serve material on a number of different websites. If company A, company B and company C all enter into an agreement with third party D to place advertisements on each of their respective websites, then third party D can use the same cookie irrespective of which of the three websites an individual is visiting. In other words, whereas companies A, B and C only know what individuals do when they are on their respective websites, third party D can link behaviour of a given individual on any of these websites to that individual’s behaviour on any of the other websites.29 In this way, third party D can associate non-personally identifiable information retrieved from a cookie of company A’s website with personally identifiable information retrieved from a cookie of company B’s website.

This cookie-facilitated interaction for advertising purposes, such as that of DoubleClick, works as follows. When an individual visits website X, then the HTML code underlying the webpage at website X tells the individual’s webbrowser that it needs to display several advertisements on the webpage, and it refers the individual’s browser to server Y, i.e. the server of the advertising placement service’s website. When the request from the individual’s webbrowser arrives at server Y, the latter determines whether or not the individual has one of Y’s cookies (or one of Y’s network of associates). If there is no such cookie, then server Y installs a cookie on the individual’s hard drive. If there is already such a cookie on the individual’s hard drive, then server Y accesses it, analyses the stored clickstream data, combines that data with data about the individual previously retrieved and finds out what kind of advertisement the individual should be interested in. Server Y then responds to the request from the individual’s webbrowser by filling the advertising space on website X’s webpage with advertisement banners targeted to the individual’s profile. The owner of website X is paid for displaying the banner ads (each view is called a ‘hit’) and receives more revenue if the individual clicks through on the banner to the sponsor’s website (a ‘click’). The owner of server Y earns money from the advertisers for placing the targeted banner advertisements on the requested webpage.30

In addition, it has to be pointed out that the scope and penetration of data-profiling activities will probably increase with a new technology initiative aimed at facilitating the sharing of data among several businesses. It is

30 L. Jenab, supra note 28, at 545–46.
currently rather difficult for companies to exchange customer data, because there is no uniform standard method for compiling and collecting such data, so that a company can share such data with another company only if it first transforms the data into a form that the other company can read. The creation of the Customer Profile Exchange (‘CPEX’) and the advent of Extensible Markup Language (‘XML’) will make this possible. CPEX, formed in 1999, is an alliance of technology companies dedicated to developing ‘a vendor-neutral, open standard for facilitating the privacy-enabled interchange of customer information across disparate enterprise applications and applications’.\(^\text{31}\) To achieve this goal, CPEX is developing a common language based on XML that will allow different companies to exchange data more easily. XML is similar to HTML, but unlike HTML, XML has a greater capacity for facilitating the sharing of data. HTML currently allows website owners to use only a limited array of tags to designate whether Web text should be, for example, a certain font, size or colour. A characteristic of HTML tags is that they identify whether the text is a name, zip code or e-mail address. XML, in contrast, can attach identifying tags to any type of text, allowing it to be recognized. Because anyone can define XML tags, XML cannot by itself facilitate exchanges of customer data among companies; a standard format must exist for the tags. CPEX wants to develop common specifications of XML so that companies collecting customer data can quickly transfer that data to other companies.\(^\text{32}\)

There are several possible self-help measures against the installing of cookies. First, webbrowsers permit their users to set their ‘preferences’ to accept or reject cookies, to notify the user before accepting a cookie or to accept only cookies that will be returned to the originating website. A second possibility is to manually delete all cookies installed in the ‘cookie jar’ after having finished surfing the World Wide Web.\(^\text{33}\) Third, there is also software for examining, editing, blocking or eradicating cookies, such as Cookie Pal, Cookie Master 2, Cookie Crusher, Crumbler 97, Cookie Cutter, etc.\(^\text{34}\) However, it is perceived that self-help does not seem to be sufficient and that there should also be a legal framework with respect to the use of cookies. Below, we turn to an analysis of the new EU legal framework for the use of cookies.

---

31 See http://www.cpexchange.org/about/mission.asp.
32 A.J. McClurg, supra note 3, at 85–86.
4 The EU Legal Framework for the Use of Cookies

The new EU legal framework for the use of cookies is laid down in Article 5(3) of Directive 2002/58, which provides the following: ‘Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or 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 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 subscriber or user.’ Article 5(3) is further clarified by Recitals 24 and 25 of the Directive.

This new legal framework was not included in the European Commission’s initial proposal,35 but has been introduced by the European Parliament’s amendments to the proposal,36 which were later modified by the Council of the EU.37 The European Parliament’s intention was to prohibit the use of cookies without the Internet users’ prior, explicit consent. It proposed the following provision: ‘Member States shall prohibit the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user without the prior, explicit consent of the subscriber or user concerned. This 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.’38 However, as will be explained below, the Council later replaced the Parliament’s intended prohibition to use cookies unless prior, explicit consent by a permission to use cookies on the condition that information and a right to refuse the cookie are provided.

Before analysing Article 5(3) and its related Recitals, it is necessary to examine the legal framework’s material and territorial scope.

38 Amendment 26, supra note 36, at C 140E/128.
4.1 Assessment of the Scope

4.1.1 Interaction between Directives 95/46 and 2002/58: Two Interpretations

The interaction between Directive 95/46 and Directive 2002/58 is important for determining the exact scope of Directive 2002/58 and its provision about cookies. One is spontaneously inclined to think that, since Directive 2002/58 is intended to be a *lex specialis* vis-à-vis Directive 95/46, the former prevails over the latter in case of a conflict between provisions, so that an examination of their interaction seems superfluous. However, the provisions of Directive 2002/58 that set out its scope are written in an enigmatic way so that the interaction between both Directives is rather unclear. For instance, whereas Article 1 of Directive 2002/58 provides that the provisions of Directive 2002/58 ‘particularize and complement’ those of Directive 95/46, Directive 2002/58 seems to retain different criteria as regards its territorial scope, laid down in Article 3: Although Directive 95/46’s main criterion for determining its territorial application is the location of the controller of the processing of personal data, this location criterion is not taken into account in Article 3 of Directive 2002/58.39

The text of Directive 2002/58 not being clear, there are two possible interpretations of the interaction between both Directives.

The first possible interpretation is based on the purpose of Directive 2002/58, set forth in Article 1(2) and clarified by Recital 10, and the opinion of the Article 29 Data Protection Working Party. Article 1(2) provides that ‘[t]he provisions of this Directive particularize and complement Directive 95/46/EC for the purposes mentioned in paragraph 1.’ Recital 10 provides that ‘[i]n the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.’ In 2000, the Article 29 Data Protection Working Party issued an opinion on the repealed Directive 97/66, in which it said that, ‘[i]t should […] not be forgotten that the specific directive 97/66/EC only complements the general directive 95/46/EC by establishing specific legal and technical provisions. When revising the specific directive, it will be necessary to take into account, respect and be coherent with the provisions of the general data protection directive 95/46/EC, that applies to any processing of personal data falling under its scope, irrespective of the technical means used.’40

---

These provisions and the Working Party’s opinion imply that both Directives apply cumulatively: Directive 95/46, being neutral with regard to its material scope, is the *lex generalis* for the processing of personal data, and Directive 2002/58, the material scope of which is specific for the electronic communications sector, is the *lex specialis* for the processing of personal data in the context of electronic communications, and both Directives interact according to the principle *lex specialis derogat legi generali*. There would, however, be one exception to this cumulative application: Directive 95/46 applies to natural persons only, whereas Article 1(2) – as explained by Recital 12\(^{41}\) – of Directive 2002/58 provides that this Directive also protects ‘the legitimate interests of subscribers who are legal persons’.

Consequently, under this interpretation, except for the provisions with respect to legal persons, the scope of Directive 2002/58 is determined by the same criteria as those that determine the scope of Directive 95/46.

The second possible interpretation is based on the terminology used in Directive 2002/58 and the fact that it is not explicitly provided in Directive 2002/58 that its scope is determined by the same criteria as that of Directive 95/46. For instance, Article 3 of Directive 2002/58 does not seem to rely on the same criterion of territorial attachment as that of Directive 95/46 (*see infra*). In addition, some provisions do not seem to exclusively deal with the processing of personal data, for instance Article 5(3) about cookies (*see infra*). One could thus infer from this that Directive 2002/58, of course, deals with the processing of personal data in the framework of network and electronic communications services, but that it nevertheless does not have the same scope of territorial application as Directive 95/46 or even that it does not exclusively deal with the processing of personal data as is the case with Directive 95/46.\(^{42}\)

Below, it will be demonstrated that following the first or the second interpretation directly influences the determination of the precise scope of Directive 2002/58.

### 4.1.2 Material Scope: Cookies and Other Little Brothers

Article 5(3) of Directive 2002/58 is vague as regards its material scope. It aims at regulating the use of electronic communications networks to store information or to gain access to information stored in the terminal

---

\(^{41}\) Recital 12 provides: ‘Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.’

equipment of a subscriber or user, but it neither refers to any specific technologies nor to any types of information that it covers.

As regards the technologies, this vagueness undoubtedly corresponds to the intention to remain as technology-neutral as possible. One source of interpretation is Recital 24, which provides some examples of technologies other than cookies that are covered: ‘spyware, web bugs, hidden identifiers or other similar devices [that] can enter the user’s terminal equipment without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user.’

The absence of an explanation of the term ‘information’ can lead to two possible interpretations of the types of information that are covered, depending on whether one sticks to the purpose of Directive 2002/58 – which is to regulate the processing of personal data – or whether one thinks that the terminology used in Article 5(3) is aimed to be more neutral and silently departs from the Directive’s purpose. If one emphasizes the purpose of Directive 2002/58, which is, according to Article 1(1), to ‘ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector’, then the information covered is limited to ‘personal data’ within the meaning of Article 2(a) of Directive 95/46. Consequently, under this interpretation, Article 5(3) only applies to cookies that store or gain access to data that is related to a natural person who is or can be identified. If, however, one stresses the difference in terminology between both Directives, i.e. the use of the term ‘personal data’ in Directive 95/46 and the use of the term ‘information’ in Directive 2002/58, then Article 5(3) applies to any information stored in the terminal equipment of a subscriber or user, whether or not this information consists of ‘personal data’. It is clear that the scope under this interpretation is tremendously broader. One can find some support for this second interpretation in Recital 24 of Directive 2002/58, which provides that ‘[(t)erminal equipment of users of electronic communications networks and any information stored on such computer equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.’ This Recital thus clearly says that information stored on terminal computer equipment is by definition part of the private sphere and seems to imply that Directive 2002/58 applies to such information and not only to information that is ‘personal

---

43 J. Dhont & K. Rosier, supra note 42, at 31–32.
44 This Article defines ‘personal data’ as ‘any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.’
data’ as defined in Directive 95/46. This interpretation is followed by the United Kingdom (‘UK’) Information Commissioner, who has explicitly stated that the UK Regulations (that implement Directive 2002/58) ‘apply to all uses of such devices, not just those involving the processing of personal data’ (emphasis added).46

It has to be pointed out that Article 5(3) does not pay any attention to the purpose of the intrusion. It can be inferred from this that it applies no matter what the purpose is of the person or company that stores or accesses information.

4.1.3 Territorial Scope: Worldwide Application

One of the most relevant issues in practice is the question of when installing a cookie is subject to the rules set forth in Directive 2002/58. For instance, does the Directive apply to the situation in which a cookie is installed on an individual’s hard drive which is located in the EU by an individual or a company located outside the Union, for instance in the US? Since the territorial scope of legal rules in the context of communications networks is usually complex, it is surprising that it can be inferred from the preparatory documents of Directive 2002/58 that its territorial scope was never discussed in any significant way during the drafting process.

The territorial scope of Directive 2002/58 is laid down in Articles 1(1) and 3(1). Article 1(1) provides that ‘[t]his Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.’ (emphasis added). Article 3(1) provides that ‘[t]his Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community.’ (emphasis added). According to these provisions, the criterion for determining whether the Directive territorially applies seems to be the fact that the personal data are processed in the framework of electronic communications services provided in public communications networks in the Community. The wording ‘in the Community’ does not only refer to ‘public communications networks’ but also to ‘services’, since a communication service is necessarily linked to a communications network;47 in addition,


47 J. Dhont & K. Rosier, supra note 42, at 22.
the European legislature confirms in Article 1(1) that it intends to regulate ‘electronic communication services in the Community’. As a result, Directive 2002/58 would thus apply to a service provider established outside the EU offering electronic communication services to individuals situated in the EU.

At first sight, this constitutes a different scope from that of Directive 95/46, for the latter Directive’s territorial point of attachment, set forth in its Article 4(1),48 is the establishment of the controller of the processing of personal data on the territory of an EU Member State, or, in the absence of such an establishment, the use of equipment, automated or otherwise, situated in an EU Member State. It thus seems that the territorial scope of Directive 2002/58, which follows the ‘country of destination’ principle, is much wider than that of Directive 95/46, which in principle does not apply to the processing of personal data conducted by a controller established outside the EU. This difference would be contrary to Article 1(2) of Directive 2002/58, which provides that this Directive ‘particularizes and complements’ Directive 95/46 and can thus not have a wider territorial scope than the latter Directive.

However, it seems that, with regard to cookies, relying on the territorial point of attachment of Directive 95/46 does in fact not lead to a solution different from that resulting from Directive 95/46. The Article 29 Data Protection Working Party has indicated that, under its Article 4(1)(c),49 Directive 95/46 territorially applies if the controller of the processing (1) uses equipment over which he exercises at least partial control, and (2) has the intention to process personal data.50 In other words, the service provider thus has to have the intention to process personal data by means of the equipment, situated in an EU Member State, that is at its disposal. Accordingly, the simple act of using a publicly available communication network on the territory of the EU without the said intention does not suffice to justify the application of Directive 95/46. Applying this reasoning to cookies, the Working Party is of the opinion that Directive 95/46 applies to the installation of cookies on a computer located on the territory of the EU from outside the EU, since (1) a user’s computer can be

48 Article 4(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 obligation 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.’

49 See supra note 48.

viewed as ‘equipment’ within the meaning of Article 4(1)(c) of Directive 95/46, (2) the installer of the cookie ‘makes use’ of that equipment when installing a cookie, and (3) ‘the controller decided to use this equipment for the purposes 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.’ The Working Party has consequently stated that the national law of the Member State where the user’s computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard drive.51

Since the EU Member States’ legislation implementing Directive 95/46 and Directive 2002/58 thus applies to persons and legal entities outside the Union (for instance those located in the US) installing cookies on a computer located on an EU Member State’s territory, the European legal framework for the use of cookies has a tremendous extra-territorial application.

4.2 Assessment of the Legal Rules

The new legal framework for the use of cookies, laid down in Article 5(3) of Directive 2002/58, consists of two parts: (1) two substantive obligations, and (2) two exceptions to these obligations. It must be pointed out, however, that one must also comply with the rights and obligations set forth in Directive 95/46.

4.2.1 Two Substantive Obligations

Article 5(3) allows the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user on the condition that the subscriber or the user (1) is provided with clear and comprehensive information in accordance with Directive 95/46, inter alia about the purposes of the processing, and (2) is offered the right to refuse such processing by the data controller. In other words, installing a cookie is subject to (a) an obligation to provide information, and (b) an obligation to offer a right to refuse.

Obligation to Provide Information

The first condition set forth in Article 5(3) is that the user or subscriber is provided with clear and comprehensive information in accordance with Directive 95/46, inter alia about the purposes of the processing.

The fact that Article 5(3) provides that information has to be provided ‘in accordance with Directive 95/46’ implies that the person placing the cookie must comply with the obligation to inform laid down in Article 10

51 Id., at 11.
of Directive 95/46. This information includes (1) the identity of the controller of the processing and of its representative, if any, (2) the purposes of the processing for which the personal data are intended, and (3) any further information such as (a) the recipients or categories of recipients of the personal data, (b) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and (c) the existence of the right of access to and the right to rectify the personal data. In all probability, the information about whether replies to the questions are obligatory or voluntary and about the consequences of failure to reply can be transposed to the cookie context into information about whether allowing a cookie to be placed is required or not to visit the website or make use of its service and about the consequences of not allowing a cookie to be placed. In this respect, Recital 25 of Directive 2002/58 provides that ‘[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.’ In other words, a legitimate consequence of not allowing a cookie may be that the individual cannot visit the website or make use of certain services.

It thus seems that Directive 2002/58 does not entail a new obligation to inform that is different from that set forth in Directive 95/46. Consequently, the question arises as to what the added value is of repeating the obligation to inform; the obligation to inform under Directive 95/46 applies anyway, since Recital 10 of Directive 2002/58 provides that ‘[i]n the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals’ (emphasis added).

A possible interpretation is that repeating the obligation to inform in Directive 2002/58 aims to – in the context of cookies – no longer distinguish between data of natural persons and data of legal persons. It could be argued that, since Article 1(2) of Directive 2002/58 provides that its provisions ‘provide for protection of the legitimate interests of subscribers who are legal persons’, the purpose of repeating the obligation to inform is that also subscribers who are legal persons have to be informed, and this in contrast with Directive 95/46, under which only natural persons have to be informed (since this Directive does not apply to data of legal persons). However, this interpretation would run counter to Recital 12 of Directive 2002/58, which provides that ‘[t]his Directive does not entail an obligation for Member States to extend the application of Directive 95/46 to the protection of the legitimate interests of legal persons’. It is unclear whether this then implies that there is no obligation to inform if the subscriber is a legal person.

52 O. Hermanns, supra note 45, at 55, 58.
Another – and the most plausible – interpretation is that repeating the obligation to inform in Directive 2002/58 aims to – in the context of cookies – no longer distinguish between ‘personal data’ (as defined in Article 2(a) of Directive 95/46) and ‘non-personal data’. It could be argued that a person installing a cookie still has to provide information, even if that cookie processes data that do not identify a natural person or allow such person to be identified. This interpretation is in accordance with our assessment of the material scope of Article 5(3).

A consequence of explicitly referring to the obligation to inform about the purposes of the processing in accordance with Directive 95/46 is that Article 5(3) imposes another obligation, i.e. the obligation to comply with the requirement that the purposes of the processing be legitimate, as set forth in Articles 6 and 7 of Directive 95/46. This requirement is confirmed in Recital 24 of Directive 2002/58, which provides that ‘[t]he use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.’ In this context, Recital 25 of Directive 2002/58 provides that ‘such devices, for instance so-called ‘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 on-line transactions.’ It has to be pointed out that this again raises the question of whether or not this requirement applies with regard to data about legal persons.

Obligation to Offer a Right to Refuse

The second condition set forth in Article 5(3) of Directive 2002/58 is the offering of a ‘right to refuse’ the cookies. This terminology seems rather inappropriate, since the notion of refusal comes close to the notion of consent, which implies that the user would have only one single opportunity to deal with the cookie: If he does not refuse it the first time, then he can no longer withdraw his consent, for – according to Recital 25 (see infra) – the right to refuse can be offered once and cover any future use of the cookie during subsequent connections, which would thus deprive the user of any remedy during subsequent connections. It would undoubtedly have been better to use the term ‘right to object’, which is used in Directive 95/46 with regard to the processing of personal data for direct marketing purposes. The right to object can be exercised at any time, also during subsequent connections. In this respect, it has to be pointed out that, as mentioned above, technical solutions make it possible to suppress cookies at any time. The use of the right to object would have overcome the problem of multiple users of one terminal equipment, a problem which is explicitly addressed in Recital 25: ‘Users should have the opportunity to refuse to have a cookies or similar device stored on their terminal equipment. This is particularly important where users other than the original user

---

53 Article 14 of Directive 95/46.
have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment.\textsuperscript{54}

An odd, circular problem of the rule that the offering of a right to refuse can cover subsequent connections is that, if the user or subscriber refuses the cookie, it is not clear how the service provider will be able to ‘remember’ this, since the provider is not allowed to install a cookie that contains the information that the user exercised his right to refuse. Maybe this may qualify as an example of the first exception to the obligation to provide information and a right to refuse (\textit{see infra}).

Although the user or subscriber has a right to refuse cookies, he nevertheless has to bear the consequences of his refusal for further visiting the website or using a service, for – as already mentioned above in the context of the obligation to inform – Recital 25 of Directive 2002/58 provides that ‘\textit{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.}’\textsuperscript{55}

This seems to imply that a service provider can refuse to give access to a service although the cookie installed on the computer is not necessary for the supply of the service. The existence of a legitimate purpose that justifies the use of a cookie suffices to permit the service provider to make the service conditional on the acceptance of the cookie.

\textbf{Who Has to Comply With the Obligations?}

Article 5(1) of Directive 2002/58 does not specify who has to comply with the obligations to provide information and to offer the right to refuse, which seems to imply that it is the person or company that uses the cookie concerned. It is worth noting that Recital 25 of the Common Position No 26/2002 on Directive 2002/58 provided that these obligations had to be complied with by ‘\textit{the operator of a website sending such devices or allowing third parties to send them via his website}’.\textsuperscript{55} It is not clear why the latter wording has been deleted in the final version of the Directive, since it is an appropriate point of view. The UK Information Commissioner’s point of view on this issue seems to be based on the Common Position’s wording: ‘\textit{The Regulations} [i.e. the UK legislation implementing Directive 2002/58] do not define who should be responsible for providing the information outlined in Regulation 6(2). Where a person operates an online service and any use of a cookie type device will be for their purposes only, it is clear that that person will be responsible for providing the information in question. We recognize that it is possible for organisations to use cookie type devices on websites seemingly within the control of another organisation, for example through a third party advertisement on a website. In such cases the organization to whom the site primarily refers will be obliged to alert users to the fact that a third party advertiser operates cookies. It will not be

\textsuperscript{54} J. Dhont & K. Rosier, \textit{supra} note 42, at 34.

\textsuperscript{55} See \textit{supra} note 37.
sufficient for that organization to provide a statement to the effect that they cannot be held responsible for any use of such devices employed by other persons they allow to place content on their websites. In addition, the third party would also have a responsibility to provide the user with the relevant information. \(^{56}\)

**When and How Must the Obligations be Complied With?**

Recital 25 of Directive 2002/58 provides more guidelines as regards when and how the obligations to provide information and to offer a right to refuse must be complied with: ‘Information and the right to refuse 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. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible.’

As regards the moment to comply with the obligations, this provision seems to require a website to provide information and offer the right to refuse at the moment that the connection is made.

It is, however, not clear how the obligations have to be complied with. The text of Article 5(3) of Directive 2002/58 provides that the subscriber or user has to be ‘provided with’ the information and must be ‘offered’ a right to refuse. Similarly, Recital 25 merely provides that users ‘should have the opportunity to refuse’ (emphasis added). It is not clear whether or not this means that the information and the right to refuse expressly have to be brought to the individual’s attention by means of an actively directed communication, for instance in the form of a pop-up window. Recital 25 does not explicitly prescribe that a pop-up window be used, but specifies that ‘[t]he methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible.’ This terminology seems to imply that there has to be a specific communication addressed to the user or subscriber and that it does not suffice for the person who has to comply with the obligations to have recourse to a simple technical ‘possibility’ for the subscriber or user to access the information and exercise the right to refuse the cookies. This interpretation finds support in Recital 25, which provides that the information and the right to refuse may be offered once covering any further use that may be made of cookies during subsequent connections; if the information only has to be accessible to the user, then this concession would be of no practical interest.\(^{57}\)

The UK Information Commissioner seems to share this opinion, by saying that ‘[t]he requirement that the user or subscriber should be ‘given the opportunity to refuse’ the use of the cookie type device may be subject to differing interpretation. At the very least, however, the user or subscriber should be given a

---

\(^{56}\) UK Information Commissioner, *supra* note 46, at 5–6.

clear choice as to whether or not they wish to allow a service provider to engage in the continued storage of information on the terminal in question. (original emphasis). *The fact that an ‘opportunity to refuse’ such storage or access must be provided imposes a greater obligation on the relevant party than that they should simply make such a refusal a possibility.* (emphasis added).58 In translating this into practice, however, the Commissioner takes a rather pragmatic view: ‘The mechanism by which a subscriber or user may exercise their right to refuse continued storage should, therefore, be prominent, intelligible and readily available to all, not just the most literate or technically aware. Where the relevant information is to be included in a privacy policy, for example, the policy should be clearly signposted at least on those pages where a user may enter a website. The relevant information should appear in the policy in a way that is suitably prominent and accessible and it should be worded so that all users and subscribers are capable of understanding and acting upon it, without difficulty. […] Although a standard approach would be beneficial, whether service providers choose to make their own switch off facilities available or else explain to the user or subscriber how they can use the facilities specific to their browser type is less important than that the mechanism is uncomplicated, easy to understand and accessible to all. There is, in addition, nothing to prevent service providers from requiring users to ‘opt in’ to receipt of the cookie as opposed to providing them with the opportunity to ‘opt out’.59‘ The Information Commissioner thus seems to be of the opinion that it might suffice to provide the information and offer the right to refuse in a privacy policy visibly posted on the website.

As regards the obligation to offer a right to refuse, this opinion would then boil down to explaining in the privacy policy how the webbrowser can be used to refuse cookies. However, as regards the right to refuse, the Commissioner’s statements seems to be inherently contradictory, since it is not clear what the difference is between simply making a refusal a possibility (which the Commissioner says is insufficient) and merely explaining in a privacy policy how a webbrowser can be used to refuse cookies (which the Commissioner says is sufficient). In any event, it would be logical that, unless an exception applies (see infra), a cookie may not be installed at the moment itself that an individual visits a website, since he then would not have had the opportunity to refuse the cookie. As regards the obligation to inform, it is worth mentioning in this respect that in the Common Position version of Directive 2002/58, Article 5(3) provided that the user had to ‘receive in advance’ the information, and Recital 25 provided that ‘clear and precise prior information’ had to be provided (emphasis added). The fact that in the Directive’s final version the wording ‘in advance’ in Article 5(3) and ‘prior’ in Recital 25 has been deleted and that the term ‘receive’ in Article 5(3) has been replaced by

58 UK Information Commissioner, supra note 46, at 5.
59 UK Information Commissioner, supra note 46, at 5–6.
‘provide with’, may be an argument for contending that providing information in a privacy policy (which is, as opposed to a pop-up window, a ‘passive’ way of communicating) is sufficient. However, this argument is not valid for offering the right to refuse.

4.2.2 Two Exceptions

The second sentence of Article 5(3) of Directive 2002/58 contains a – rather enigmatic – exception to this general regime: ‘This 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 subscriber or user.’

The use of the wording ‘this shall not prevent’ does not make it easy to assess the exact scope of this exception. Does it aim to waive the obligation to provide information and/or to offer a right to refuse? Or does it allow the person or company that has to comply with the obligations to inform and offer the right to refuse to ignore the user’s refusal? The Recitals do not provide any guidelines for answering this question. It may be useful to examine whether the national laws implementing Directive 2002/58 shed light on this matter. In the UK, for instance, Article 6(1) of the implementing Regulations provides that ‘[s]ubject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.’ Paragraph 2 contains the obligations to inform and offer the opportunity to refuse. Paragraph 4 then provides that ‘[p]aragraph (1) shall not apply to the technical storage of, or access to, information for [. . .] the above-mentioned exceptions’ (emphasis added). The wording ‘shall not apply’ seems to imply that, in such cases, the service provider does not have the obligation to provide information and offer a right to refuse.

The Directive’s exception regime applies only in the event of a ‘technical storage or access’ for one or two possible purposes. It is not clear what such ‘technical storage or access’ exactly means. A plausible interpretation may be that the required ‘technical’ nature of the storage or access implies that there may not be any processing of personal data for the exception regime to apply.

A first situation in which a technical storage or access qualifies as an exception is if it is ‘for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network’. It is not really clear what this exception exactly means, but it seems to intend to allow the use of mere session cookies.60 This interpretation is based on the Recital that the European Parliament proposed when it amended the

---

60 In the same sense: O. Hermanns, supra note 45, at 55, 58.
European Commission’s initial proposal with a provision about cookies. This proposed Recital referred to session cookies in general terms: ‘The prohibition of storage of communications [...] by persons other than the users without the users’ consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission [...]’ (emphasis added). Although the European Parliament’s proposal for a prohibition of cookies was replaced by a permission to install cookies in combination with an obligation to provide information and to offer a right to refuse, this first exception (although slightly rewordered) was maintained in the Directive’s final version, so that the Parliament’s proposal is a solid basis for interpretation.

In any event, it is clear that the purpose of carrying out or facilitating the transmission of a communication has to be the sole purpose; if there is another, concurrent purpose, then the exception does not apply.

A second situation in which a technical storage or access qualifies as an exception is if it is ‘as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user’. The term ‘information society services’ is not defined in Directive 2002/58 but in Article 1(a) of Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, as explicitly referred to by Article 2(a) of the EU E-Commerce Directive. It means ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’. Directive 98/34 does not explicitly explain what ‘normally provided for remuneration’ exactly means, but it is generally accepted that this means that the service has to be an economic activity. According to the case law of the European Court of Justice, an economic activity does not necessarily require that the beneficiary of the service pays for the service; the fact that a third party pays the provider of the service is sufficient (for instance a service provider which offers certain online services for free, which is

---

61 Amendment 9, supra note 36, at C 140E/124.
64 In this respect, ‘at a distance’ means that ‘the service is provided without the parties being simultaneously present’, ‘by electronic means’ means that ‘the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means’, and ‘at the individual request of a recipient of services’ means that ‘the service is provided through the transmission of data on individual request’. This concept has already been the object of many studies, so that it will not be further examined in this article.
made possible by revenue coming from advertisement fees paid by third parties).

Does this second exception imply that, if an individual has requested an information society service that involves collecting information regarding usage, it follows that he does not have to be informed and does not have a right to refuse the cookies concerned? It is hard to answer this question in abstracto; it will depend on whether the use of the cookie corresponds to a ‘technical storage or access’ (as mentioned above, it is not clear what this exactly means) and whether the cookie is ‘strictly necessary’. The Directive does not give any information about how the wording ‘as strictly necessary’ should be interpreted. Something to hold on to can be found in the UK Information Commissioner’s Guidelines, which provide that ‘[t]he term ‘strictly necessary’ means that such storage of or access to information should be essential, as opposed to reasonably necessary, for this exemption to apply. It will also, however, be restricted to what is essential for the provision of the service requested by the user, rather than what might be essential for any other uses the service provider might wish to make of that data. It will also include what is required for compliance with any other legislation to which the service provider might be subject, for example, the security requirements of the seventh data protection principle’ [65] [. . .]. Where the use of a cookie type device is deemed ‘important’ as opposed to ‘strictly necessary’ the user of the device is still obliged to provide information about the device to the potential service recipient so that they can decide whether or not they wish to proceed. The information provided to the user about the uses the collector intends to make of that data should be of sufficient clarity to enable the user to make a truly informed decision.’ [66]

4.2.3 Other Obligations under Directive 95/46 Remain Applicable

Since Recital 10 of Directive 2002/58 provides that Directive 95/46 applies to all matters which are not specifically covered by the provisions of Directive 2002/58, including the obligations on the controller and the rights of individuals, persons and companies that place cookies have to comply with all provisions of Directive 95/46, such as the obligation to notify the national supervisory authority (provided in its Article 18) or the data subject’s right of access to the personal data (provided in its Article 12), but only on the condition that the application criteria of Directive 95/46 are met. Amongst other things, this means that other obligations under Directive 95/46 apply only in the event that via the cookie ‘personal data’, as defined in its Article 2(a), are processed; these obligations do not apply if data related to legal persons or ‘non-personal data’ related to

---


[66] UK Information Commissioner, supra note 46, at 6–7.
natural persons (for instance, data that do not identify or allow to identify a natural person)\textsuperscript{67} are processed.

The UK Information Commissioner is of the same opinion, saying that '[w]here the use of a cookie type device does involve the processing of personal data, service providers will be required to ensure that they comply with the additional requirements of the Data Protection Act 1988 [which implemented Directive 95/46]. This includes the requirements of the third data protection principle which states that data controllers shall not process personal data that is excessive […]'. Where personal data is collected, the data controller should consider the extent to which that data can be effectively processed anonymously. This is likely to be of particular relevance where the data is to be processed for a purpose other than the provision of the service directly requested by the user, for example the counting of visitors to a website.\textsuperscript{68}

A provision of Directive 95/46 that does not apply is Article 7. This Article, which enumerates the few situations in which personal data may be processed,\textsuperscript{69} is overridden by Article 5(3) of Directive 2002/46: One is allowed to process personal data via cookies in any situation, also situations that are not enumerated in Article 7, provided that the obligations to provide information and offer a right to refuse are complied with.

One of the far-reaching consequences of the extra-territorial application of Directives 95/46 and 2002/58 to service providers established outside the EU placing cookies on hard drives of computers situated in the EU, is that these service providers, when processing personal data via such cookies, have to comply with Article 18 of Directive 95/46, which provides that they have to notify the supervisory authority of the EU Member States before placing any such cookie. An important issue in this respect is that Member States are allowed to provide certain exemptions from notification, which implies that a service provider placing such cookies may have to be obliged to notify the supervisory authority of one Member State while it may be exempted from notification in another Member State.

Such ‘foreign’ service providers also have to comply with Article 25 of Directive 95/46, which provides that the transfer of personal data from

\textsuperscript{67} In this context, the question arises as to whether or not an Internet Protocol address is a ‘personal data.’ This issue is not further discussed in this article.

\textsuperscript{68} UK Information Commissioner, supra note 46, at 4.

\textsuperscript{69} Article 7: ‘Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) 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; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’
an EU Member State to a country outside the EU is allowed only if that country has an adequate level of protection of personal data. Article 25 applies since personal data are collected on the territory of an EU Member State, i.e. on the hard drives of computers located on that territory, and are subsequently electronically transferred outside the EU.

If a country has an adequate level of protection, then such transfer is allowed. As regards a service provider established in the US, this means that it is allowed to perform such transfers via cookies if it has adhered to the US Safe Harbor Principles.\textsuperscript{70}

According to Article 26 of Directive 95/46, other relevant grounds on which such transfers are allowed – even if the country to which the personal data are transferred does not have an adequate level of protection – are (1) the fact that the data subject has given his unambiguous consent to the transfer, (2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request (for instance, in the context of electronic commerce), and (3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.

If, however, the service provider is established in a country that has no adequate level of protection (for instance, an American company that has not adhered to the US Safe Harbor Principles) or cannot rely on one of the situations set forth in Article 26, then it is not allowed to transfer personal data via cookies outside the EU. This is again an example of the far-reaching consequences of the extra-territorial application of Directive 2002/58.

5 Conclusion

Directive 2002/58 is probably the first statutory legal framework in the world that specifically deals with the use of cookies. In principle, it should be widely applauded because it explicitly recognizes that the use of cookies gives rise to privacy and data protection problems and it constitutes an attempt to protect the fundamental right of privacy while at the same time recognizing that cookies can be used for legitimate purposes and thus preserving legitimate interests of businesses. It is to be hoped that the Directive may therefore be an incentive for other countries to pay more attention to the use of cookies from a privacy point of view.

However, it has been made clear above that Directive 2002/58 in general and its provisions about cookies in particular are not masterpieces of logic and clear legislative art. With regard to the Directive itself, one of

\textsuperscript{70} More information about the US Safe Harbor Principles can be found on http://www.export.gov/safeharbor.
the most far-reaching gaps is the lack of a clear description of the exact interaction between Directive 2002/58 and its mother Directive 95/46. There are two valid interpretations on this point: the first one is based on the purpose of Directive 2002/58, i.e. to ‘particularize and complement’ Directive 95/46, and provides that the scope of Directive 2002/58 is determined by the same criteria as those that determine the scope of Directive 95/46; the second one is based on the different terminology in both Directives and the fact that it is not explicitly stated in Directive 2002/58 that its scope is determined by the same criteria as those that determine the scope of Directive 95/46, and provides that Directive 2002/58 can have a different scope.

This general hiatus directly influences the scope of the provisions that specifically deal with the use of cookies. For instance, as regards the material scope, it is not completely clear whether or not these provisions apply to information processed via cookies that cannot be qualified as ‘personal data’ within the meaning of Directive 95/46, for example information related to legal persons. On the other hand, it has been explained that, as regards the use of cookies, both Directives have the same, tremendously extra-territorial scope: they not only bind service providers established on the territory of an EU Member State, but also those established outside the EU, for instance in the US.

There are also other ‘bugs’ in the cookie-related provisions, which may result from the fact that the Directive’s first draft versions did not contain any rules on the use of cookies and that the final cookie-related provisions have been inserted in a hurry without thorough analysis. For instance, the introduction of the new concept of the right to ‘refuse’ raises several questions, for example as regards its relationship with the right to ‘object’ which is used in Directive 95/46. Another gap is the fact that there is no concrete guidance as to how the obligations to provide information and offer a right to refuse must be complied with. It is also not entirely clear what types of cookie uses are covered by the two exceptions.

In conclusion, the question can be raised whether the new EU legal framework that regulates the Cookie Monster is not a monster itself...