European Commission

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology by:

time.lex

Spark
Legal network and Consultancy ltd

Digital Agenda for Europe

This study was carried out for the European Commission by:

Internal identification

Contract number: 30-CE-0629642/00-85

SMART 2013/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-47439-2

doi:10.2759/411362

Abstract

This Report is the final result of a study of which the objective was threefold:

- First, the study aimed to assist the Commission by gathering evidence on the transposition of the ePrivacy Directive and by conducting an in-depth analysis of the effective implementation and enforcement of key provisions of this Directive in the Member States;
- The second objective was to assess whether the ePrivacy Directive appears to be achieving its intended effects, by identifying and discussing possible gaps, overlaps and diverging transpositions in the Member States;
- Finally the study addressed the interaction between the ePrivacy Directive and the proposed Data Protection Regulation in order to assess how the two instruments will operate together.

The study did not deal with the entire ePrivacy Directive but focused on five topics: (i) Article 3 regarding the geographical and material scope of application; (ii) Article 5.1 on confidentiality of communications; (iii) Article 5.3 on cookies, spyware and the like; (iv) Articles 6 and 9 on traffic and location data respectively; (v) Article 13 on commercial communications.

This report, drafted by Jos Dumortier and Eleni Kosta, contains an analysis of each of these five topics regulated by the ePrivacy Directive, based on the primary observations from the Member States as drawn from the Study's country reports, and an evaluation of the impact, effectiveness and challenges of the relevant provisions of the ePrivacy Directive. These elements form the basis of a series of recommendations from the perspective of a possible revision of the Directive.

Brussels, 31 January 2015

Table of Contents

1. Executive summary

1.1 Introduction

Directive 2002/58/EC – hereafter "the ePrivacy Directive" – aims to protect the privacy and regulate the processing of personal data in the electronic communications sector. As such the Directive complements the Data Protection Directive 95/46/EC. Inter alia, the ePrivacy Directive specifies how some of the principles of Directive 95/46/EC apply to the electronic communications sector.

The ePrivacy Directive is on the other hand part of the Regulatory Framework for Electronic Communications. The Framework was last amended in 2009 and the deadline for transposition of the 2009 amendments was 25 May 2011. By January 2013, all Member States had notified the necessary measures to implement the revised ePrivacy Directive into their national laws.

On 25th January 2012, the Commission adopted a proposal for a reform of the EU legal framework on the protection of personal data. The reform includes a Regulation which lays down a new EU framework for data protection (replacing Directive 95/46/EC). The proposed Regulation also makes a limited number of technical adjustments to the ePrivacy Directive to take account of the transformation of Directive 95/46/EC into a Regulation. The Communication that accompanies the proposed Regulation explains that the substantive legal consequences of the new Regulation and of the new Directive for the ePrivacy Directive will be the object, in due course, of a review by the Commission, taking into account the result of the negotiations on the current proposals with the European Parliament and the Council.

The first objective of this report is to provide evidence on the transposition of the ePrivacy Directive, but also on the effective implementation and enforcement of key provisions of this Directive in the Member States. A second objective is to assess whether the ePrivacy Directive appears to be achieving its intended effects, by identifying and discussing possible gaps, overlaps and diverging transpositions in the Member States, taking into account, in particular, the need to ensure a single market and free movement by avoiding fragmentation along national boundaries. Last but not least, the report addresses the interaction between the ePrivacy Directive and the proposed Data Protection Regulation in order to assess how the two instruments will operate together.

The report does not deal with the entire ePrivacy Directive but is focused on five topics: (i) Articles 1 to 3 regarding the geographical and material scope of application; (ii) Article 5(1) on confidentiality of communications; (iii) Article 5(3) on cookies,

spyware and similar techniques; (iv) Articles 6 and 9 on traffic and location data respectively; (v) Article 13 on unsolicited commercial communications. Topics such as security (Art. 4), itemized billing (Art. 7), calling and connecting line identification (Art. 8 and 10), automatic call forwarding (Art. 11) and subscriber directories (Art. 12) are thus outside the scope of this report.

1.2 Scope of application

The Regulatory Framework for Electronic Communications to which the ePrivacy Directive belongs, applies to providers of "electronic communications networks and services" as defined in Art. 2 of Directive 2002/21/EC (the Framework Directive). More precisely, according to Art. 3 of the ePrivacy Directive, the provisions of this Directive are applicable "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". Consequently only services consisting wholly or mainly in the conveyance of signals – as opposed to e.g. the provision of content – are within the scope of the Directive. However convergence sometimes results in services that are very similar from a functional perspective remaining subject to different legal regimes depending on whether they are provided in the form of an electronic communications service, an information society service, or an audiovisual service. Well-known examples are internet telephony and webmail.

Our survey of the transposition of the ePrivacy Directive into the national legislation of the Member States has demonstrated that the provisions of the Directive are not always transposed in the context of the national legal framework applicable to the electronic communications sector. Several provisions of the Directive have been transposed by Member States in the context of another legal framework, such as the legislative instrument applicable to information society services, the general personal data protection law or the legal framework for consumer protection. As a result, the scope of the national provisions on topics such as cookies, traffic and location data, or unsolicited direct marketing communications, adopted pursuant the ePrivacy Directive, frequently have a different scope of application than the one defined by Art. 3 of the ePrivacy Directive.

Furthermore, the definition of the scope of application of the ePrivacy Directive is ambiguous. The provision refers to "the provision of publicly available electronic communications services in public communications networks" and, according to Art. 2(c) of the Framework Directive the notion of "electronic communications service" does not include information society services, as defined in Article 1 of Directive 98/34/EC and which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

On the other hand, it seems incontestable that certain provisions of the ePrivacy Directive are nevertheless applicable to providers of information society services. The most obvious example is Art. 5(3) dealing with the use of cookies and similar techniques.[1] For other provisions, such as Art. 9 – regulating the processing of location data other than traffic data – the extension of the scope of application to information society service providers is most often excluded.[2] Art. 13 regulating unsolicited direct marketing communications is generally interpreted as being exclusively applicable to messages transmitted via electronic communications.[3]

Moreover, for certain provisions, such as Art. 6 – relating to the processing of traffic data – or Art. 9 – on location data other than traffic data – the narrow scope leads to unacceptable situations of unequal treatment. It is difficult to justify why traffic or location data should receive different legal protection if they are processed in the context of very similar services from a functional perspective. The same observation is valid for the provision of Art. 13(1), prohibiting the use of e-mail without prior consent of the recipient only for messages transmitted via electronic communications and not for messages exchanged via information society services such as social media platforms.

In order to remedy this situation we recommend amending Art. 3 of the ePrivacy Directive to make its provisions applicable to the protection of privacy and the processing of personal data "in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union". The amendment would put an end to the discussion about the applicability of the provisions of the ePrivacy Directive to information society services and other value-added services provided via public electronic communications networks. In addition it would extend the scope of the Directive to private networks that are intentionally made accessible to the public. Such extension has also been suggested by the EDPS in his second opinion of 9 January 2009 on the review of Directive 2002/58/EC.[4]

In the longer term, further convergence will probably trigger a broader debate about the opportunity of a more in-depth revision of the current structure of the European

[1] See e.g. the Article 29 Opinion 2/2010 on online behavioural advertising, p. 9: "The Working Party has already pointed out in WP 29 Opinion 1/2008 that Article 5(3) is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used".

[2] See e.g. the Article 29 Opinion 13/2011 on geolocation services on smart mobile devices, p. 9: ""The e-Privacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network".

[3] See e.g. the Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines, WP 148 (2008), p. 4: .

[4] O.J. C 128 of 6 June 2009, p. 36.

regulatory framework for the online environment. Maintaining a distinct regulatory regime for electronic communications services, information society services or audiovisual services will most probably become less and less relevant in the future. For the time being however, an explicit widening of the scope of application of the ePrivacy Directive can solve, to a large extent, the most urgent issues.

1.3 Confidentiality

Article 5(1) of the ePrivacy Directive protects the confidentiality of communications and the related traffic data. The provision states that "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation" and that "in particular, they (Member States) shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users".

It is evident that, at the moment of the adoption of this provision in 2002, all Member States had already long since introduced legislation protecting the confidentiality of private communications. The transposition of Art. 5.1 did not have a harmonizing effect on these existing national legal provisions. The legal protection of confidentiality of communications in the Member States remains therefore diverse. The diversity is mainly related to definitions, conditions and other modalities but, evidently, also to the exceptions. This is due to the fact that Art. 15.1 of the ePrivacy Directive states that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC".

As a consequence rules with regard to e.g. wiretapping for law enforcement purposes or monitoring electronic communications in an employment context are not harmonized at the European level. This situation will not fundamentally change after the transposition by the Member States of the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (so-called "Law Enforcement Directive"). The scope of this proposed Directive is restricted to the processing of personal data by law enforcement authorities and

doesn't deal with topics such as the interception of electronic communications. Further harmonisation of the rules with regard to these topics would also be difficult to achieve in the short term since they are, in most of the Member States, part of the national criminal procedure rules.

In order to bring the text of Art. 5.1 into line with the proposed widening of the scope of the ePrivacy Directive, we suggest amending it and making it applicable to "confidentiality of communications and the related use of traffic data by means of a public or publicly accessible private communications network". It is further evident that confidentiality of electronic communications should also be protected against "automatic" intrusions without human intervention. This clarification could be added in a Recital to the Directive, noting that automated intrusions are of course always initiated and/or controlled by one or more persons. Finally, the exception of Art. 5(1) for "technical storage which is necessary for the conveyance of a communication" should probably be broadened to "storage as far as necessary for ensuring the functioning of the network or the provision of the service on that network". Such amendment would be a logical consequence of the extension of the scope of Art. 5.1 to e.g. information society services.

Article 5.2 of the ePrivacy Directive stipulates that the protection of confidentiality "shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication". This provision – often designated as the "business exception" - has been interpreted and transposed by Member States in very different ways. National legislators in some of the Member States have restricted the scope of Art. 5.2 to the electronic communications sector. In other Member States the provision is applied to all sectors and is aimed at giving employers some margin to register telephone conversations conducted by employees in the context of, for instance, a call centre. We suggest therefore clarification of the scope of Art. 5.2 in order to obtain a uniform transposition and implementation of this provision throughout the Union. The currrent restriction to "the provision of evidence of a commercial transaction or of any other business transaction" could be widened to other situations in which recording of communications in an employment context seems to be justified, such as quality control or legitimate supervision of work performance. A harmonised legal basis for monitoring communications of employees for such legitimate reasons, and under the condition to respect general data protection rules, is currently missing on the European level. A careful assessment of the impact of such change on stakeholders would be needed to assess its feasibility, taking into account the diversity of rules currently applicable to the processing of personal data in the employment context.

1.4 Cookies and Similar Techniques

Article 5.3 requests the Member States to "ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent (…)". Recital (24) explains that "so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned".

The requirement to collect the users' prior consent in the context of Art. 5.3 is the result of an amendment adopted in 2009 in the context of the Citizen's Rights Directive. Recital (66) of the Citizens' Rights Directive states that "where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application". This part of Recital (66) has been integrated into the text of the law by about ten Member States, including e.g. France, Ireland, Luxembourg, Greece, Poland, Slovakia, Slovenia, Spain and the UK, In other Member States Recital (66) of the Citizen's Rights Directive is referred to in guidance documents issued by national data protection commissioners.

The possibility to express consent via the configuration of browser settings has initially led to uncertainty. The Article 29 Working Party has therefore elaborated the conditions for browser settings to be able to deliver valid and effective consent in its Opinion 2/2010. Several major web browsers, whose default settings often allow all kinds of cookies, do not currently fulfil these conditions. As a consequence – and this should preferably be clearly stated in a Recital of the ePrivacy Directive – only browsers or other applications which by default reject 3d party cookies and which require the user to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites are able to deliver valid and effective consent.

It is further difficult to deny that the introduction of the consent rule in Art. 5.3 did not entirely reach its objective. This is largely due to the fact that the user is currently receiving a warning message with regard to the use of cookies on almost every web site. Obviously the effect of such warning messages would substantially increase if they would only appear if the web site contains 3d party cookies, cookies used for direct marketing purposes and, more generally, all cookies that are not related to the purpose for which the user is navigating on the site.

Article 5.3 currently contains two exceptions where prior consent of the user is not needed: a) for the technical storage of, or the gaining access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the gaining access to information is strictly necessary for the provider. These exceptions should preferably receive a slightly broader formulation, for example, by deleting the condition stating that "the storing of or the gaining access to information (should be) strictly necessary for the provider". In addition we recommend the insertion of additional exceptions, e.g. for cookies which are exclusively used for web site usage statistics. Finally we propose the explicit request of specific, active and prior consent in all cases where cookies or similar techniques are used for direct marketing purposes.

Last but not least, while the current discussion mainly deals with the issue of *how* consent should be given and *how* the relevant information should be furnished to the user or the subscriber, it should also be examined *whether* the choice to make the ePrivacy Directive allow the use of cookies (and similar techniques) based only on the consent of the user or the subscriber is effective and logically plausible. Does the consent of the user justify unlimited tracking of that user's behaviour in the online environment, given the known weaknesses of consent as a mechanism for ensuring legitimacy? This question inevitably leads us to the issue of "profiling", and any solution should take into account the outcome of the discussion in the framework of the proposed general Data Protection Regulation on this very issue.

1.5 Traffic and Location Data

Although Article 6 of the ePrivacy Directive seems to be more or less correctly transposed by the Member States, there are serious problems with regard to the enforcement of some of its provisions. Most problematic is Art. 6(3) which stipulates: "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 or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time."

In practice some mobile operators mention the possibility of processing user and traffic data in their general terms and conditions. Some of these terms and conditions grant the operator a right to process the data for a duration of two years after the end of the contract.

Furthermore, the provisions regarding location data are frequently criticised. The ePrivacy Directive regulates only a fraction of location based services, namely those which rely on the processing of location data other than traffic data offered via a public communications network or in a publicly available electronic communications service. Location based services that are offered to members of a private network are not governed by the provisions of Article 9 of the ePrivacy Directive, even though privacy risks may be the same or even greater. For example, Article 9 does not cover location data that are transmitted via enterprise networks aimed at a private user group, or data collected and transmitted via infrared signals or GPS signals in combination with a private secured wireless LAN.

Moreover, in its Opinion 13/2011 dealing with geolocation services on smart mobile devices the Article 29 Working Party, referring to the strict definition of electronic communications service in Art. 2(c) of the Framework Directive, also stated that "the ePrivacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network" (p. 9).

In line with our proposed amendment to Article 3 of the ePrivacy Directive it is sufficient to slightly modify the wording of Art. 6(1) and Art. 9(1) in order to make the rules with regard to the processing of traffic and location data applicable to all services provided via public or publicly available private communications networks that collect and further process traffic and location data. As a result, the processing of location data in the context of information society services provided via all kinds of mobile apps will be subject to the application of Art. 6 and Art. 9, even if the location data are not resulting from the public electronic communication network or service as such, but via other techniques such as wifi network proximity or IP-address databases.

Additionally, efforts are needed at the Union and the national level to ensure correct transposition of the European rules on the processing of traffic and location data and to enforce their implementation in practice.

1.6 Unsolicited Direct Marketing Communications

In general, Member States have adequately transposed Article 13(1) of the Directive. Thus, they have introduced national provisions ensuring that the use of automated calling and communication systems without human intervention, fax and e-mail for direct marketing is prohibited unless prior consent has been obtained. The term "electronic mail" – being defined in Art. 2(h) of the ePrivacy Directive as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient" – is generally interpreted as being restricted to e-mail via electronic communications and not applicable to messages exchanged via information society

services such as Facebook, LinkedIn, Skype or Twitter, even when the transmission of such messages ultimately occurs over the internet and thus makes use of publicly available electronic communications services provided on public electronic communications networks. This restrictive interpretation seems also be the one adopted by the Article 29 Working Party.

The Directive leaves some discretion to Member States in relation to "other forms of direct marketing", such as person-to-person voice telephony. As they are relatively more costly for direct marketers, Member States are free to choose an opt-in or opt-out consent regime. Some Member States have chosen opt-in, and others opt-out. This distinction is a natural consequence of the margin of policy making left to the national legislators by EU legislation.

In relation to communications made to subscribers who are legal persons, the Directive stops short of specifying what rules should be put in place at Member State level, but provides the broad requirement that the legitimate interests of such subscribers be "sufficiently protected". In general, one of three approaches was adopted in each Member State for this situation: opt-in, opt-out, or no protection for legal persons.

Our main recommendation with regard to Art. 13 is to bring the scope into line with our proposed amendment to Art. 3. This means, in the first place, that the opt-in rule of Art. 13(1) should also apply to e-mail messages transmitted via information society services.

This extension of the scope of Art. 13(1) should not, however, lead to the prohibition without the prior consent of the user of all kinds of personalised online advertising. Therefore the definition of "e-mail" in Art. 2(h) of the Directive needs to be amended.

Article 13(1) would of course only be applicable if e-mail is "used for the purpose of direct marketing". It is irrelevant whether the direct marketing message is part of the message body or attached in a separate document. However direct marketing should be the primary purpose. This is the reason why, for example, a newsletter or a magazine, sent as an attachment to an e-mail will not fall under the scope of Art. 13(1), as long as the newsletter or magazine is primarily sent for a different purpose, other than direct marketing.

For various reasons we recommend maintaining the possibility for Member States to adopt either an opt-in or an opt-out regime for direct marketing message under Article 13(3).

1.7 Relationship with the proposed general Data Protection Regulation

The relationship between the ePrivacy Directive and the proposed general Data Protection Regulation is regulated by Art. 89 of the text proposed by the Commission.

Article 89(1) of the proposed Regulation states that "this Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC". In addition, Recital (135) of the draft Regulation proposed by the Commission states that the Regulation "should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly."

Article 89(2) of the draft Regulation stipulates: "Article 1(2) of Directive 2002/58/EC shall be deleted". Art. 1(2) of the ePrivacy Directive is currently worded as follows: "The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover they provide for protection of the legitimate interests of subscribers who are legal persons."

The objectives of the proposed Article 89(1), further developed in Recital (135) are to delimit the scope of application of both legislative instruments and to ensure that the modified ePrivacy Directive and the Regulation can work together in the future, after the adoption of the General Data Protection Directive. The proposed Regulation will not be applicable in all cases where the ePrivacy Directive contains specific obligations with the same objective. For the provisions examined in our Study this solution is perfectly possible to implement.

However, if, according to the recommendations formulated in this Study, the scope of application of the ePrivacy Directive were to be modified, the text of Article 89(1) should be amended as well. Currently this text refers to "obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union". This should be changed into "obligations on natural and legal persons in relation to the processing of personal data in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union".

The proposed Art. 89(2) is necessary because a directive cannot "particularise" a regulation. According to Art. 288(2) TFEU a regulation has not only general application but is also binding in its entirety and directly applicable in the whole of the Union. Member States can therefore not be requested in a directive to derogate from rules contained in a regulation.

In our view, the Commission should consider transforming the Directive into a regulation for three reasons. First of all, the relationship between the provisions of the two legislative instruments would be considerably less complex if they are at the same level. This would make the announced revision of the ePrivacy Directive a lot easier.[5] In the second place it may considerably facilitate the application of the entire supervisory and enforcement mechanism introduced by the proposed Data Protection Regulation to the topics currently covered by the ePrivacy Directive. Arguably the adoption of this mechanism will be justified once the scope of the Directive (or of a future regulation) would be widened beyond the borders of the electronic communications sector. Last but not least, it would allow the amendment of Art. 89 of the general Data Protection Regulation (once adopted) if this provision was no longer in line with the final text of a future "ePrivacy Regulation".[6]

If the ePrivacy Directive is not transformed into a regulation and remains a directive, it would be necessary to transform it into a self-standing instrument after the adoption of the General Data Protection Directive, following the example of the proposed Law Enforcement Directive. As a result there would be two instruments containing provisions on personal data protection with mirroring provisions but on different levels. Moreover, if the scope of application of the ePrivacy Directive will be widened and include services which do not belong to the electronic communications sector in the strict sense, the ePrivacy Directive will no longer address a separate sector but the entire online environment, which is also one of the main targets of the proposed Data Protection Regulation. This overlap will inevitably create a very complex situation.

[5] The revision would be easier because, not only for many current provisions such as Art. 1(3) – the exclusion of the former second and third pillar from the scope of the ePrivacy Directive -, Art. 4(3) – security breach notification - , Art. 15 (1) – allowing Member States to restrict certain provisions of the Directive –, etc. but also for not explictly regulated issues such as the territorial scope, it will suffice to refer to the corresponding provisions of the general Data Protection Regulation. Notice that many current provisions of the ePrivacy Directive are already formulated in a directly binding form (see e.g. Articles 4, 6, 7, 8, 9, 13(1)).

[6] In this hypothesis it is, for example, no longer necessary to delete Art. 1(2) of the ePrivacy Directive because a future ePrivacy Regulation can perfectly particularise and complement the general Data Protection Regulation. Consequently Art. 89(2) would have to be abrogated again.

2. Introduction

2.1. Background

Directive 2002/58/EC – "the ePrivacy Directive" - replaced Directive 97/66/EC - the Telecommunications Data Protection Directive[7]-, which was part of the 1998 telecommunications regulatory package.[8] The latter Directive focused on "the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN)"[9]. Soon after its adoption, it became obvious that the European telecommunications regulatory framework would rapidly become obsolete given the wide range of "new services which [had] become available and affordable for a wide public".[10] It was therefore repealed and replaced in 2002 by the ePrivacy Directive, which wished to adapt the provision of the Telecommunications Data Protection Directive "to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used".[11]

The ePrivacy Directive aimed at providing for an equivalent level of privacy protection in the electronic communications sector and to ensure the free movement of data collected in such sector and equipment. This was done while at the same time incorporating the principle of technology neutrality into the Directive. This principle is understood as "not to impose, nor discriminate in favour of, the use of a particular type of technology, but to ensure that the same service is regulated in an equivalent

[7] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector ("Telecommunications Data Protection Directive") [1997] OJ L24/01 (30.01.1998).

[8] For a more comprehensive analysis of the developments in the telecommunications sector that led to its full liberalisation in 1998 see: LAROUCHE, Pierre, The Bases of EC Telecommunications Law after Liberalization (Hart Publishing, Oxford 2000; BURRI-NENOVA, Mira, EC electronic communications and competition law (Cameron May, London 2007, Chapter 4 "European Community Communications Law" and especially its section 3 on "European Community Communications Specific Legislation", pp. 185ff.;

[9] Recital 6 Telecommunications Data Protection Directive.

[10] COMMISSION OF THE EUROPEAN COMMUNITIES, 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Towards a new framework for Electronic Communications infrastructure and associated services - The 1999 Communications Review' COM(1999) 539 final, 10 November 1999, p. 45.

[11] Recital 4 ePrivacy Directive.

manner, irrespective of the means by which it is delivered"[12]. Nevertheless, the European regulatory landscape with regard to the online environment after the 2002 reform continued to operate on the basis of the distinction between three different legal concepts (information society services, electronic communications services and audiovisual media services), regulated in three different regulatory frameworks: the E-Commerce Directive, the electronic communications package and the Audiovisual Media Service Directive.[13]

The EU Regulatory Framework on electronic communications services and networks adopted in 2002 was amended in 2009 by two new Directives, the Citizens' Rights Directive[14] and the Better Regulation Directive.[15] These Directives aimed at the attainment of better regulation for competitive electronic communications in the European Union, the completion of the single market in electronic communications and a better connection with European citizens.[16]

The deadline for transposition of the 2009 amendments was 25 May 2011. By January 2013, all Member States had notified the necessary measures to implement the revised ePrivacy Directive into their national laws. With regard to the notification of personal data breaches, Commission Regulation (EU) No 611/2013 of 24 June 2013

[12] COMMISSION OF THE EUROPEAN COMMUNITIES, "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Towards a new framework for Electronic Communications infrastructure and associated services - The 1999 Communications Review" COM(1999) 539 final, 10 November 1999, p. vi. For a detailed analysis on the principle of technology neutrality in the EC telecommunications regulations, see VAN DER HAAR, Ilse, *Principle of technological neutrality in EC telecommunications regulation* (DPhil thesis, Tilburg University, 2008).

[13] SØREN SANDFELD JAKOBSEN, "EU Internet law in the era of convergence: the interplay with EU telecoms and media law", in SAVIN & TRZASKOWSKI (ed.), Research Handbook on EU Internet Law, Edward Elgar, 2014, p. 60

[14] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ("Citizens' Rights Directive") [2009] OJ L337/11 (18.12.2009).

[15] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 2009/140/EC amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services ("Better Regulation Directive") [2009] OJ L337/37 (18.12.2009).

[16] COMMISSION OF THE EUROPEAN COMMUNITIES, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and Summary of the 2007 Reform Proposals' (2007) COM(2007) 696 final, 13(1)1.2007, pp. 3-4.

issued technical implementing measures setting forth the circumstances, formats and procedures applicable to the information and notification requirements referred to in Article 4(3) of the revised ePrivacy Directive. These measures entered into force on the 25th August 2013. Finally, on the 11th September 2013 the Commission published its proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent.[17] Although this new proposal does not amend the ePrivacy Directive, it could, once adopted by the European Parliament and the Council, affect the application of the Directive's provisions in practice because European users would, much more so than today, be empowered to move to electronic communications services provided by an undertaking established in another Member State.

2.2. Relation with the General EU Data Protection Legal Framework

As stated in Article 1(2), the ePrivacy Directive *particularises* and *complements* Directive 95/46/EC[18] on the processing and free movement of data. In other words, for privacy and data protection aspects that have not explicitly been dealt with in the ePrivacy Directive, Directive 95/46/EC remains fully applicable.[19] The collection and processing of data in an electronic communications environment will always have to correspond to the principles set forth under Directive 95/46/EC. For instance, Directive 95/46/EC provides that the collected data shall be processed fairly and lawfully, shall only be collected for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes. The personal data shall furthermore be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data shall be accurate and, where necessary, kept up to date. The personal data shall 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 (Article 6 of Directive 95/46/EC), and so on. These overall principles maintain their entire significance in an electronic communications environment.

This situation is a specific application of the doctrine stating that "a law governing a specific subject matter (*lex specialis*) overrides a law which governs a general matter

[17] COM(2013) 627 final

[18] 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* of November 23, 1995).

[19] Recital 10 ePrivacy Directive clarifies exactly this point: "In 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."

(*lex generalis*)".[20] It should also be noted that the ePrivacy Directive contains provisions aimed at protecting the privacy of users and subscribers also in situations where no personal data are being "processed" as defined by Directive 95/46/EC. There is, in other words, not a complete overlap between the two legislative instruments. Moreover, whereas Directive 95/46/EC only applies to the collection of personal data of natural persons, the ePrivacy Directive also protects the legitimate interests of legal entities.

On 25 January 2012, the European Commission released its proposal for a comprehensive reform of the 1995 data protection rules on personal data processing.[21] On 21 October 2013 the LIBE Committee adopted amendments to the Commission's proposal and the European Parliament adopted a legislative resolution in plenary on 12 March 2014 (EP first reading)[22]. The proposed Regulation is currently under discussion in the Council. Once adopted, the new Regulation will then become directly applicable across the whole EU territory after a transition period of two years.

The proposed Regulation makes a limited number of technical adjustments to the ePrivacy Directive to take account of the transformation of Directive 95/46/EC into a Regulation. The Commission announced in the accompanying Communication that the substantive legal consequences of the new Regulation for the ePrivacy Directive will be the object, in due course, of a review by the Commission, taking into account the result of the negotiations on the current proposals with the European Parliament and the Council.[23]

2.3. Objectives of this report

The first objective of this report is to provide evidence on the transposition of the ePrivacy Directive and also to conduct an in-depth analysis of the effective implementation and enforcement of key provisions of this Directive in the Member States. The report is focused on five topics: (i) Article 3 regarding the geographical and material scope of application; (ii) Article 5.1 and 5.2 on confidentiality of communications; (iii) Article 5.3 on cookies, spyware and similar techniques; (iv) Articles 6 and 9 on traffic and location data respectively; (v) Article 13 on commercial communications.

---

[20] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP171' (2010), p. 10, discussion on the relation between the Data Protection and the ePrivacy Directives.

[21] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[22] First reading of the European Parliament, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

[23] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF, p. 4, footnote 15

The second objective of the report is to assess whether the ePrivacy Directive appears to be achieving its intended effects, by identifying and discussing possible gaps, overlaps and diverging transpositions in the Member States, in particular taking into account the need to ensure a single market and safeguard the right to free movement by avoiding fragmentation across national boundaries. The report takes into account the evolution of the notion of privacy in a changing digital environment, and in particular whether the ePrivacy Directive is adapted to such environment.

Finally, while the final text of the future Data Protection Framework is not yet known, the report addresses the interaction between the ePrivacy Directive and the proposed Data Protection Regulation in order to assess how the two instruments will operate together. This includes the following tasks:

- Analyse and assess the overall relationship between the ePrivacy Directive and the draft Regulation from a legal perspective, based on the assumption that Article 89 will be adopted;
- Analyse whether the co-existence of the two regimes adequately ensures a level playing field(for example, that the same framework applies to different sectors which engage in the same data processing, taking into account the evolution of the notion of privacy in an evolving digital environment);
- Study the co-existence of two different enforcement mechanisms, given that matters under the ePrivacy Directive will not be covered by the consistency mechanism. Relevant questions on this point will relate, for example, to the situation of controllers established in more than one Member State. Article 51 of the proposed Regulation prescribes that, in such cases, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions related to the cooperation and consistency mechanism.
- Analyse the co-existence of different rules on applicable law. For example due to the fact that the European Commission proposed that the draft Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour.

2.4. Methodology

To assess the five previously mentioned items of the ePrivacy Directive and their transposition into the national law of the Member States, we begin with, for each of the relevant provisions, an in-depth analysis of the text of the provision, its background, context and objective, in order to provide an indication of how the provision should be interpreted.[24]

As a second step for each of the relevant provisions the report contains a summary of the way the Member States have transposed the provision in their national legislation. For more detailed information about the transposition in every Member State we refer to the individual country reports. The country reports have been drafted by national correspondents on the basis of a questionnaire. The national experts were asked to map the transposition of the ePrivacy Directive, as well as to assess the implementation and functioning thereof in their Member State. This information was gathered on the basis of desk research and two face to face interviews, including in particular with privacy and data protection commissioners and electronic communications regulatory authorities. More in-depth desk research has been performed and additional in-depth interviews have been conducted in six selected Member States: Belgium, France, Germany, Poland, Sweden and the UK. As a result this report often refers in more detail to the situation in these countries.

The final step is an evaluation of whether the ePrivacy Directive appears to be achieving its intended effects, by identifying and discussing possible gaps, overlaps and diverging transpositions in the Member States, taking into account the need to ensure a single market and having regard to the evolution of the notion of privacy in an evolving digital environment.

[24] The analysis of the provisions of the ePrivacy Directive in each Chapter has been co-authored by ELENI KOSTA (time.lex) on the basis of her book: See KOSTA, Eleni, Consent in European Data Protection Law, Leiden-Boston, Martinus Nijhoff Publishers, 2012, 441 p.

3. Scope of Application

This chapter deals with the scope of application of the ePrivacy Directive. One of the questions to be examined is whether or not it still makes sense to maintain specialised rules with regard to privacy protection dedicated to the electronic communications sector. The following chapters will then focus on the content of some of these specialised rules.

In order to answer the first question, we first look at the scope of application of the ePrivacy Directive itself.

3.1. Scope of Application of the ePrivacy Directive

The ePrivacy Directive applies, according to the wording of its Article 3, "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices".[25]

Therefore, in order to decide on the applicability of the ePrivacy Directive the following four questions must be answered in the affirmative:

i) whether there is an *electronic communications service*,

ii) whether this service is offered in an *electronic communications network*,

iii) whether the aforementioned service and network are *public,* and

iv) whether the network or service is provided *in the Community*.

3.1.1. Electronic Communications Service

3.1.1.1. Communication

The ePrivacy Directive defines the term "*communication*" in Article 2(d):

[25] Artice 3 ePrivacy Directive. This provision, on the services that are covered by the ePrivacy Directive, was amended during the 2009 review of the electronic communications legal framework[25] via the Citizens' Rights Directive. The new Article 3 of the ePrivacy Directive clarified that "public communications networks supporting data collection and identification devices" are included under the scope of the ePrivacy Directive. Devices for data collection and identification can be contactless devices using radio frequencies**,** such as Radio Frequency Identification ("RFID") devices, which use radio frequencies to capture data from uniquely identified tags, which can then be transferred over existing communications networks. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of the ePrivacy Directive apply, including those on data security, traffic and location data and on confidentiality.

'Communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

The definition of communication clarifies that there needs to be information exchanged or conveyed between a *finite* number of parties. Information, which is part of a broadcasting service for the public and is provided over a public communications network is intended for a potentially unlimited audience, and therefore does not constitute a communication in the sense of the ePrivacy Directive[26].

Consequently linear radio and television services offered via analogue terrestrial networks are not covered by the ePrivacy Directive, as they are broadcasting services, which are intended for a potentially unlimited audience. It is however clarified that when the individual subscriber or user who is receiving information that is part of a broadcasting service, as described above, can be identified, the information conveyed is covered by the ePrivacy Directive[27]. Thus, the concept of broadcasting which is intended for a potentially unlimited audience covers point to multipoint transmissions, such as near- video-on-demand services[28], which are excluded from the scope of application of the ePrivacy Directive. Only when broadcasting is offered under a point-to-point scheme, such as in the case of video-on-demand services, does the Directive apply.[29]

3.1.1.2. Service

In order for the ePrivacy Directive to apply, the processing of personal data has further to take place in connection with an **electronic communications service**. The

[26] Recital 16 2002 ePrivacy Directive.
[27] Recital 16 2002 ePrivacy Directive.
[28] For an analysis of the concept of broadcasting and the difference between video-on-demand and near-video-on-demand see: C-89/04 *Mediakabel BV v Commissariaat voor de Media (Mediakabel)* [2005] ECR I-4891, as well as the Opinion of the Advocate General Tizzano: C-89/04 *Mediakabel* Opinion of the Advocate General Tizzano (10.03.2005). In his Opinion the Advocate General adopted an essentially technical criterion in order to decide on the qualification of a content service as information society service or as television broadcasting service and this was the criterion of point-to-point versus point-to-multipoint transmission. However this reasoning was not followed by the Court of Justice.
[29] Recital 16 ePrivacy Directive. See also: ASSCHER, Lodewijk F. and HOOGCARSPEL, Sjo Anne, *Regulating Spam: A European perspective after the adoption of the E-Privacy Directive* (Information Technology & Law Series, TMC Asser Press, The Hague 2006), p. 34.

term “electronic communications service” is defined in Article 2(c) of the Framework Directive[30] as:

> *[…] a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.*

An electronic communications service is a service within the meaning of Article 56 (ex Article 49 TEC) of the Treaty on the Functioning of the European Union (TFEU)[31], which guarantees the free movement of services. According to Article 57 TFEU (ex Article 50 TEC), in order for a service to be considered as one under the meaning of the Treaties it should be normally provided for remuneration and it should, among others, be of a commercial nature.[32]

An electronic communications service is normally **provided for remuneration**, which should be interpreted with a broad meaning. The Court of Justice of the European Union has dealt with the concept of remuneration in the context of services offered within the European Union in various cases. In *Belgium v Humbel* the Court considered that “the essential characteristic of remuneration […] lies in the fact that it constitutes consideration for the service in question”[33]. It is not the recipient who necessarily gives the remuneration; the critical element is that the remuneration is given to the provider of the service. In *Bond van Adverteerders v Netherlands*, the Court of Justice of the European Union confirmed that the remuneration does not need to come from

[30] European Parliament and the Council of the European Union, Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (“Framework Directive”) [2002] OJ L108/33 (24.04.2002). The Framework Directive contains the basic rules for the establishment of a harmonised framework for the regulation of electronic communications services and electronic communications networks. It also contains many of the definitions that need to be taken into account for the implementation of the ePrivacy Directive, such as the fundamental definitions of “electronic communications service”, “electronic communications network”, “public communications network” or “provision of an electronic communications network”.

[31] Treaty on the functioning of the European Union (consolidated version as amended by the Treaty of Lisbon) (2008/C 115/01) [2008] OJ C115/47 (09.05.2008), as modified by the Treaty of Lisbon: Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 [2007] OJ C306/1 (17.12.2007).

[32] Article 57 TFEU: “[…] ‘Services’ within the meaning of the Treaties shall in particular include (a) activities of an industrial character; (b) activities of a commercial character; (c) activities of craftsmen; (d) activities of the professions”.

[33] C-263/86 *Belgian State v René Humbel and Marie-Thérèse Edel (Belgium v Humbel)* [1988] ECR 5365, para. 17.

the recipient of the service, i.e. the viewer; it suffices that the remuneration comes from another party, such as an advertiser.[34] The Court in various cases has ruled that a service can be considered as provided for remuneration even in cases when the provider is a non-profit organisation, when there is an "element of chance" inherent in the return or when the service is of recreational or sporting nature, within this interpretation.[35] Therefore, an activity that gets profit via advertising can also be considered as provided for remuneration, even if remuneration does not come directly from the user.[36]

Not considered as "electronic communications services" according to Art. 2(c) of the Framework Directive are "services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; **it does not include information society services**, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".

3.1.2. Electronic Communications Network

The ePrivacy Directive presupposes the existence of an **electronic communications network**. The term "electronic communications network"[37] is defined in Article 2(a) of the Framework Directive as a set of systems, equipment, as well as active and passive elements permitting the transmission of signals, regardless of the content that these

[34] C-352/85 *Bond van Adverteerders v Netherlands State* [1988] ECR 2085. CRAIG, Paul and DE BÚRCA, Gráinne, *EU Law - Text, Cases, and Materials* (4th edn Oxford University Press, Oxford, 2008), p. 819.

[35] CRAIG, Paul and DE BÚRCA, Gráinne, *EU Law - Text, Cases, and Materials* (4th edn Oxford University Press, Oxford, 2008), p. 818, who provide extensive references to various cases of the Court of Justice relating to the concept of services and remuneration: See for instance: C-70/95 *Sodemare and others/Regione Lombardia (Sodemare)* [1997] ECR I-3395; C-275/92 *H.M. Customs and Excise/Schindler (Schindler)* [1994] ECR I-1039; C-415/93 *Union royale belge des sociétés de football association and others/Bosman and others (Bosman)* [1995] ECR I-4921.

[36] QUECK, Robert et al., 'The EU Regulatory Framework Applicable to Electronic Communications' in GARZANITI, Laurent and O'REGAN, Matthew (eds), *Telecommunications, Broadcasting and the Internet - EU Competition Law & Regulation* (3rd edn, Sweet & Maxwell, London, 2010), para. 1-047.

[37] It is interesting to note that the definition of "electronic communications network", as well as the ones of "electronic communications service" and "public communications network" contained in the 2002 Framework Directive were identical to the ones contained in the Liberalisation Directive (COMMISSION OF THE EUROPEAN COMMUNITIES, Directive 2002/77/EC of 16 September 2002 on competition in the markets for electronic communications networks and services ("Liberalisation Directive") [2002] OJ L249/21 (17.09.2002)). It is still unclear at this moment whether the fact that the Better Regulation Directive amended the definitions of an "electronic communications network" and the one of "public communications network" will have any impact in the harmonious application of the Liberalisation Directive and the amended regulatory framework on electronic communications.

signals carry[38]. The definition of an electronic communications network, as amended by the Better Regulation Directive (2009/140/EC) reads as follows:

> *'Electronic communications network' means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.*[39]

The Framework Directive defines also the term "provision of an electronic communications network" under Article 2(m). The definition clarifies that the term provision of a network shall be perceived in a broad way.

> *'Provision of an electronic communications network' means the establishment, operation, control or making available of such a network.*[40]

3.1.3. Public

The ePrivacy Directive applies to **publicly available electronic communications services in public communications networks**. In order to apply the ePrivacy Directive, it is not sufficient to have an electronic communications service, nor an electronic communications network involved. Both the relevant service and the network need to be public (or publicly available as is the term usually used in connection with electronic communications services).

The Citizens Rights' Directive introduced a new Recital, which clarified that the ePrivacy Directive did **not apply to closed user groups and corporate networks**.

> *In line with the objectives of the regulatory framework for electronic communications networks and services and with the principles of proportionality and subsidiarity, and for the purposes of legal certainty and efficiency for European businesses and national regulatory authorities alike, Directive 2002/58/EC (Directive on privacy and electronic communications)*

[38] QUECK, Robert et al., 'The EU Regulatory Framework Applicable to Electronic Communications' in GARZANITI, Laurent and O'REGAN, Matthew (eds), *Telecommunications, Broadcasting and the Internet - EU Competition Law & Regulation* (3rd edn, Sweet & Maxwell, London, 2010), para. 1-045.
[39] Article 2(a) Framework Directive.
[40] Article 2(m) Framework Directive.

focuses on public electronic communications networks and services, and does not apply to closed user groups and corporate networks. [41]

The Framework Directive provides a definition of the term 'public communications network'[42] –a definition also amended during the review of the regulatory framework on electronic communications[43].

'Public communications network' means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points".

3.1.4. Territorial Application

Art. 3 of the Directive states that the network or service needs to be provided "in the Community" but in contrast to the Data Protection Directive, the ePrivacy Directive does not contain an explicit provision with regard to the applicable national law. Article 4 of the Data Protection Directive states, for example, that "each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State".

In the absence of such an explicit provision, we estimate that, with regard to the question of the applicable national law, the ePrivacy Directive follows the same logic as the other directives belonging to the European regulatory framework for electronic communications.[44] According to that logic, each National Regulatory Authority (NRA) is in charge of the regulation of the market players active on its national territory. General authorisations granted for those market players according to Directive 2002/20/EC (the Authorisation Directive) may be made subject to personal data and privacy protection specific to the electronic communications sector in conformity with Directive 2002/58/EC.[45] If Member States are competent to control the application of the provisions of the ePrivacy Directive before granting authorisations to network and service providers providing services on their territory, these provisions are evidently applicable to all providers operating on that territory. We therefore conclude that the rules of Art. 4 of Directive 95/46/EC with regard to the geographical scope of the

[41] Recital 55 Citizens' Rights Directive.
[42] Article 2(d) Framework Directive.
[43] The old definition of public communications network (Art. 2(d) 2002 Framework Directive) did not make any reference to Network Termination Points: "Public communications network' means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services".
[44] According to the Authorisation Directive, this is the place where the services are provided.
[45] See the Annex to the Authorisation Directive, A, nrs 7 and 16.

general data protection legal framework, are not applicable to the provisions of the ePrivacy Directive.

Consequently national provisions of a Member State transposing the ePrivacy Directive will be applicable to network and service providers operating on the territory of that Member State. As a result, the ePrivacy Directive is also applicable to network and service providers not established in the European Union, as long as they are providing networks and/or services on the territory of the Union.

3.2. Scope of the Transpositions in the Member States

Directive 2002/58/EC is a directive and consequently its provisions, even if many of them are formulated in a directly binding form, are addressed to the Member States. One of the first observations resulting from our survey of the national transpositions of the Directive is that a large majority of national legislatures have not transposed the directive in a dedicated legislative text. Only a few Member States have introduced a national "ePrivacy law".[46] The provisions of the ePrivacy Directive have, on the contrary, been inserted in distinct national legal instruments, all with their own scope of application. For example, many Member States transposed the provisions of the ePrivacy Directive with regard to unsolicited communications (Art. 13 of the Directive) in their national legal framework relating to consumer protection. National consumer protection laws are generally applicable to all consumers residing on the national territory.

3.2.1. Material Scope

A large majority of Member States have transposed most of the provisions of the ePrivacy Directive in a national legal instrument regulating "electronic communications" containing the bulk of the European "Telecoms Package". For this part, the Member States are facing the same ambiguities with regard to the scope of application as those mentioned previously in our analysis on the European level. In all Member States the scope of the national legal framework with regard to electronic communications is very similar to the one established by the European electronic communications legal framework. In other words: national electronic communications laws are generally applicable to public electronic communications networks and publicly available electronic communications services provided on those networks.

[46] See for example the Finnish "Privacy in Electronic Communications Act". For an English version see http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf; See also the Greek Law 3471/2006, Protection of personal data and privacy in the electronic communications sector and amendment of law 2472/1997, GG A' 113/28.06.2006. Unofficial translation in Greek by the DPA at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF.

At the national level Member States have to decide unambiguously which providers belong to this category because these are the ones subject to the duty to provide information about their activities to the national regulatory authority for the electronic communications sector.[47] Some of these national regulatory authorities have introduced additional criteria to overcome the ambiguities of the European legal concepts. One example is the decision model used by the Swedish PTS (the electronic communications NRA in Sweden). The model builds on three requirements for an electronic communications service to fall under the Act:

- the service is provided to another (external) party, on commercial grounds, and
- the service mainly comprises the transmission of signals, and
- the service provider has the **power to control the transmission**.

It is evident that the solutions adopted by the Member States in this context, are not identical. As a result, a provider operating in Europe will currently be considered as a "provider" in one Member State but not necessarily in another. Services such as VoIP, webmail and location based services are qualified differently across Member States, demonstrating the difficulties in coherently applying the European conceptual framework. In Germany VoIP is considered an electronic communications service, for instance, while in France it will most likely be considered an information society service.[48] In Greece the law defines electronic communications services as services consisting wholly or **partially** in the conveyance of signals on electronic communications networks, while the Directive requires such services to consist wholly or **mainly** in the conveyance of signals. This subtle difference broadens the scope of the Greek provision such that VoIP can be considered to fall within their scope.

Applying the above-mentioned decision model, the Swedish PTS issued decisions against Skype Communications with regard to notification requirements for their services and decided that (only) services such as SkypeIn, SkypeOut, and Skype To Go are included in the application of the Electronic Communications Act, depending on the type of VoIP service.[49] The Austrian RTR GmBH reached a similar decision with regard to the SkypeOut service where this service establishes connections with the public PSTN (Public Switched Telephone Network).[50] Skype S.a.r.l. should have sought to notify RTR GmBH prior to offering SkypeOut. A mere Skype-to-Skype connection

[47] According to Art. 5 of the Framework Directive.
[48] See also Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH), 'Guidelines for VoIP Service Providers - Consultation Document', April 2005, p. 5, https://www.rtr.at/de/komp/KonsultationVoIP2005/3109_VoIP_Guidelines_2005_Cons.pdf
[49] Decision by Swedish Post and Telecom Agency (PTS) of 2 Jul. 2009, no. 06-14224. See also PTS Report PTS-ER-2009:12 on provision of services and networks that require notification.
[50] https://www.rtr.at/en/tk/R_8_08.

cannot, however, be brought within the remit of the Austrian Telecommunications Act.

Member States' solutions for determining the exact scope of application of their national electronic communications legal framework are primarily intended to decide whether or not a network or service provider belongs to the regulated part of the market. Should a company be registered as an operator and become subject to supervision by the NRA? The French NRA commissioned a comprehensive study on these issues.[51]

In Spain the duty to notify or register is an integral part of the definition of an operator, since the General Law on Telecommunications of 2014 defines "operator" as the "*natural or legal person who exploits public electronic communication networks or provides publicly available electronic communication services, and has notified to the Ministry of Industry, Energy and Tourism the start of its operations or is registered with the register of* operators". Similar definitions have also been found in other Member States.

Our survey of the Member States has further shown that, with regard to the transposition of specific provisions of the ePrivacy Directive into the national legal framework on electronic communications, some national legislators have adopted a wider scope, only applicable to these specific privacy-related provisions. For example, the Polish legislator has judged that it would not make sense to limit the scope of the rules with regard to confidentiality to publicly available electronic communications services, thereby excluding all services that are similar from a functional viewpoint but are not mainly consisting in the transmission of signals. Consequently Poland introduced the concept "participants of telecommunications activities within public networks".

Another interesting example comes from Germany: the section of the German TKG (the Federal Telecommunications Act) with regard to the processing of personal data – including e.g. traffic data – is not only applicable to services in the context of public networks but applies also to closed user groups. Member States thus widen sometimes at their national level the scope of particular provisions of the ePrivacy Directive, estimating that these provisions should not only apply to providers of electronic communications services stricto sensu.

3.2.2. Territorial Scope

Our survey in the Member States shows uncertainty regarding the territorial scope of the provisions examined in this Study. This is partly due to the fact that the provisions

[51] Etude sur le périmètre de la notion d'opérateur de communications électroniques, June 2011. See http://www.arcep.fr/uploads/tx_gspublication/etude-Hogan-Analysys-juin2011.pdf

of the ePrivacy Directive have been transposed by most of the Member States in distinct legislative instruments. As a consequence, the territorial scope differs according to the provision concerned. Italy warrants special mention as an exception, since it has transposed the ePrivacy Directive through integration in its general data protection law, which implies that the scope is exactly the same as outlined in Article 4 of the Data Protection Directive.

As far as the national provisions that are transposed in the electronic communications regulatory framework are concerned, the territorial scope generally follows the logic of this framework. This means that these provisions will be applicable to all operators and service providers operating under the jurisdiction of the NRA. Consequently the provisions of a Member State will be applicable to all operators and service providers deploying activities on the territory of that Member State. As a consequence the processing of personal data covered by the ePrivacy Directive, such as traffic and location data, will sometimes fall under the scope of more than one applicable law. Of course, this situation will only materialise if a provider deploys activities in other Member States than those where its establishment(s) is (are) located. The processing of traffic data, for example, will be regulated by the specific provisions - transposing Article 6 of the ePrivacy Directive - of the Member State where the provider is operating.

The above is the consequence of the fact that almost all of the Member States (with a few exceptions such as Italy, France, Finland and Greece) have transposed the provisions of Art. 6 and 9 in the context of their electronic communications legal framework. They apply this framework to all services provided on their territory. For example, the Belgian NRA (BIPT) is currently investigating the processing of traffic data on the Belgian electronic communications market. On the other hand, when processing traffic data, electronic communications service providers are also "controllers" of personal data. Subscribers and users keep the rights granted to them by Directive 95/46/EC, such as access rights or the right to request correction of processed personal data. Providers remain consequently also subject to the general data protection rules of the Member State where they are established.[52] In practice, however, this potential conflict has not been reported to raise any real difficulties thus far.

3.2.3. Supervision

Most of the Member States have multiple supervisory authorities with competences related to the provisions adopted under the ePrivacy Directive. Even in Finland, where

[52] According to Art. 4(1)(a) of Directive 95/46/EC each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State".

the ePrivacy Directive has been transposed as a whole in the Finnish Act on the Protection of Privacy in Electronic Communications, the supervision is divided between three supervisory authorities: the Finnish Data Protection Ombudsman's office, the Finnish Communication Regulatory Authority and - for the enforcement of the provisions relating to unsolicited communications - the Finnish Competition and Consumer Authority. A notable exception to this rule is Italy. The Italian legislator has transposed the entire ePrivacy Directive into the Personal Data Protection Code and supervision of its provisions is exclusively exercised by the Supervisory Authority for Personal Data Protection (*Garante per la Protezione dei Dati Personali*, or *Garante*).

All of the other Member States' correspondents indicate that there is an overlap between the competences of their supervisory authorities, mostly between the data protection authority (DPA) and the telecoms regulator (the "NRA"). The correspondents of Germany, Sweden and the UK emphasize, however, that the DPA and the telecoms regulator have found successful ways of co-existence. In the UK, for instance, all the enforcement competences haven been transferred by a memorandum of understanding to the Information Commissioner's Office (ICO), while the telecoms regulator OFCOM provides technical assistance where needed. In Sweden the PTS (telecoms regulator) and the Datainspektionen (DPA) collaborate successfully.

For particular topics Member States' correspondents indicate that the supervisory competences are not clear or apparently incomplete. Germany for instance has no competent authority for unsolicited communications in general[53] while that same topic in Poland is dealt with by the DPA (GIODO) under the general data protection laws.

3.3. Evaluation

It is almost a cliché to state that, given the rapidly progressing digitalisation and convergence it no longer makes sense to distinguish technologically between information technology services, telecommunication services and media services. [54]

Nevertheless, the legal structure of European regulation dealing with the online environment is still based on the assumption that it is appropriate to operate with three different categories of services (information society services, electronic communications services and audiovisual media services), and three corresponding

[53] There is a specific competence for spam mails in Germany if the spam mailer wants the adresssee to call a phone number: See http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/Rufnummernmissbrauch/Missbrauchsfaelle/missbrauchsfaelle-node.html

[54] For the Commission's recent view on convergence in the audiovisual sector see Green Paper: Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values, COM(2013) 231 final.

regulatory frameworks: the E-Commerce Directive, the Electronic Communications Regulatory Package and the Audiovisual Media Service Directive.

The Electronic Communications Regulatory Package, to which the ePrivacy Directive belongs, applies to providers of electronic communications network and services. The focus is on transport of signals, not on content. In this regard, the Framework Directive states in its Recital (5): "It is necessary to separate the regulation of transmission from the regulation of content. This framework does not therefore cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services, and is therefore without prejudice to measures taken at Community or national level in respect of such services …) The separation between the regulation of transmission and the regulation of content does not prejudice the taking into account of the links existing between them, in particular in order to guarantee media pluralism, cultural diversity and consumer protection".[55]

It is worth mentioning that the European legislator in 2009 decided to maintain this separation. Partly this is due to the fact that the three regulatory frameworks mentioned before have to be considered to a large extent as "regulatory perspectives". In practice, market players will often be regulated by the three frameworks, depending on which aspect of their activities is concerned.

Along the same line it may be rather surprising to find the rules regarding cookies as part of the regulatory framework for electronic communications. An explanation may be that Art. 5.3 of the ePrivacy Directive regulates the use of cookies and similar techniques from the perspective of the protection of the end-user of public electronic communications networks. The provision, like all other provisions of the ePrivacy Directive, has to be read in combination with Art. 3 and thus regulates the "processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks" irrelevant of who processes these data. It is therefore also applicable to information society service providers, to the extent that these providers are making use of cookies or similar techniques in the context of publicly available electronic communications services in public communications networks".

Often cited in this context is also Art. 13 of the ePrivacy Directive. This article prohibits unsolicited communication or more precisely the use of emails, fax and automatic calling machines for direct marketing, unless the user has given his prior consent. This provision too is primarily targeted at providers who perform direct marketing towards potential customers. However, the provision deals with unsolicited communications

[55] Recital 5 of the Framework Directive (2002/21/EC).

carried out via public electronic communications networks and for this reason it is not totally illogical to make it part of the consumer protection rules within the electronic communications regulatory package.

As long as the distinction between “transport of signals” and “provision of content” remains the structural basis of the European regulatory framework with regard to the online environment, discussions about the grey zone between these two categories will be unavoidable. In some cases, the legislator can provide clarifications to solve specific issues. For example, with regard to VoIP the definitions in the Framework Directive from 2002 did not take account of the development from ‘traditional’ telephony (PSTN) to VoIP. With the 2009 amendment of the definition of voice telephony in the Universal Service Directive the question has more or less been solved, at least from a purely legal perspective. According to the definition, a “publicly available telephone service” means a service made available to the public for originating and receiving, directly or indirectly, national, or national and international calls through a number or numbers in a national or international telephone numbering plan. The reference to “numbers in a telephone numbering plan” implies that only VoIP services that allow calls to or from a traditional PSTN phone number are electronic communications services subject to the telecommunications regulation. The ‘pure’ Internet-based VoIP solution which enables people to call up and talk via computer (for example, using ‘Skype’) without the call being routed on to a number in the regular telephony numbering plan is not an electronic communications service.

All in all, however, convergence sometimes results in services that are very similar from a functional perspective but remain subject to different legal regimes depending on whether they are provided in the form of an electronic communications service, an information society service or an audiovisual service. Well-known examples are, as previously described, internet telephony but also webmail. Does this mean that the material scope of application of the ePrivacy Directive should be changed?

A first element for the discussion on this question is whether it makes sense, despite the technological developments and growing convergence, to operate with three different types of services and regulations with regard to the online environment.

Our opinion is that this is an issue that goes far beyond the potential revision of the ePrivacy Directive. For the time being, the European legislation is based on the idea that despite many similarities and overlap there are still fundamental differences between the characteristics of telecoms, media and Internet services, and thus also differences between the legal issues relevant to address with respect to each type of service. It is very possible that this will change in the not too distant future but at that moment the discussion on a fundamental revision of the current regulatory structure will not be limited to the ePrivacy Directive alone but should encapsulate all elements relevant to this discussion.

Today the European legal framework for electronic communications contains a whole range of provisions related to the protection of users and subscribers. Some of these provisions are related to the protection of privacy, others address issues such as protection against unilateral contractual terms, number portability, quality of service, accessibility for disabled users, transparency and publication of information, availability of telephone inquiry services, access to emergency services, etc. Most of these provisions have their historical background in traditional voice telephony and for many of them a distinct legal framework for electronic communications probably remains relevant, at least for the time being. Therefore it does not appear to be very realistic to completely abandon the existing structure of the European legal framework for the online environment in the short term.

Remaining within the existing legal structure – maintenance of a dedicated regulatory framework for electronic communications services, including specialised rules not only with regard to market regulation but also to consumer rights and other issues – is it desirable to continue to dedicate specialised rules on privacy protection only applicable "in connection with the provision of publicly available electronic communications services in public communications networks"?

Art. 3 refers to "the provision of publicly available electronic communications services in public communications networks" and, according to Art. 2(c) of the Framework Directive the notion of "electronic communications service" does not include information society services, as defined in Article 1 of Directive 98/34/EC and which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

On the other hand, nobody seems to contest that certain provisions of the ePrivacy Directive are nevertheless applicable to providers of information society services. The most obvious example is Art. 5(3) dealing with the use of cookies and similar techniques.[56] For other provisions, such as Art. 9 – regulating the processing of location data other than traffic data – the extension of the scope of application to information society service providers is most often excluded.[57] Art. 13 regulating

[56] See e.g. the Article 29 Opinion 2/2010 on online behavioural advertising, p. 9: "The Working Party has already pointed out in WP 29 Opinion 1/2008 that Article 5(3) is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used".

[57] See e.g. the Article 29 Opinion 13/2011 on geolocation services on smart mobile devices, p. 9: ""The e-Privacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network".

unsolicited direct marketing communications is generally interpreted as being exclusively applicable to messages transmitted via electronic communications.[58]

Moreover, for certain provisions, such as Art. 6 – relating to the processing of traffic data – or Art. 9 – on location data other than traffic data – the narrow scope leads to unacceptable situations of unequal treatment. It is difficult to justify why traffic or location data should receive different legal protection if they are processed in the context of very similar services from a functional perspective. The same observation is valid for the provision of Art. 13(1), prohibiting the use of e-mail without prior consent of the recipient only for messages transmitted via electronic communications and not for messages exchanged via information society services such as social media platforms.

In order to remedy this situation, and with a view to ensure consistency and level playing field, we recommend amending Art. 3 of the ePrivacy Directive to make its provisions applicable to the protection of privacy and the processing of personal data in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union.

The amendment would put an end to the discussion about the applicability of the provisions of the ePrivacy Directive to information society services and other value-added services provided via public electronic communications networks. It will remedy the currently perceived distortion in which very similar services are subject to different regimes and the consequent uneven playing field. In addition it extends the scope of the Directive to private networks that are intentionally made accessible to the public. Such extension has also been suggested by the EDPS in his second opinion of 9 January 2009 on the review of Directive 2002/58/EC.[59]

In the longer term, further convergence will probably necessitate a more in-depth revision of the current structure of the European regulatory framework for the online environment. Maintaining a distinct regulatory regime for electronic communications services, information society services or audiovisual services will most probably become less and less relevant in the future. For the time being however, an explicit widening of the scope of application of the ePrivacy Directive can solve, to a large extent, the most urgent issues.

[58] See e.g. the Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines, WP 148 (2008), p. 4: .
[59] O.J. C 128 of 6 June 2009, p. 36.

4. Confidentiality of Communications

The objective of this Chapter is to examine the content of Article 5.1 and 5.2 of the ePrivacy Directive and answer the following questions: How have these provisions been transposed by the Member States? Did they achieve their intended effect? Is it necessary to amend the provisions?

4.1. Articles 5.1 and 5.2 of the Directive

Article 5.1 of the ePrivacy Directive relates to interception or surveillance of communications and related traffic data when they involve a public communications network and publicly available electronic communications services and is formulated as follows:

> *1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15.1. This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.* [60]

The scope of this provision is clearly limited to communications and related traffic data "by means of a public communications network". However, as emphasised in Recital (10) "in 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."

Actions that enable the interception or surveillance of communications are thus allowed when the users concerned have given their consent. Recital 17 of the ePrivacy Directive specifies that, "for the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website".

[60] Article 5.1 ePrivacy Directive.

On the 30th of September 2010 the European Commission referred the United Kingdom to the Court of Justice of the European Union (CJEU) for not fully implementing rules on the confidentiality of electronic communications.[61] Before referring the U.K. to the Court of Justice, the European Commission had sent a letter of formal notice[62], which was followed by a reasoned opinion[63]. More specifically, the European Commission identified three issues in the U.K. legislation relating to the confidentiality of electronic communications, which did not apply the European legislation correctly:

- *There is no independent national authority to supervise interception of communications, although the establishment of such authority is required under the ePrivacy and Data Protection Directives, in particular to hear complaints regarding interception of communications.*
- *The current UK law – the Regulation of Investigatory Powers Act 2000 (RIPA) – authorises interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has 'reasonable grounds for believing' that consent to do so has been given. These UK law provisions do not comply with EU rules defining consent as freely given specific and informed indication of a person's wishes.*
- *The RIPA provisions prohibiting and providing sanctions in case of unlawful interception are limited to 'intentional' interception only, whereas the EU law requires Members States to prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.*[64]

In 2012 the European Commission dropped the privacy infringement case because the UK government announced amendments to the RIPA provisions in order to bring them into line with European law.

It is important to note that, in the context of Art. 5.1, the act is not legitimised with the consent of the subscriber, but only the consent of the *user* to whom the

[61] EUROPEAN COMMISSION, 'Press Release: Digital Agenda: Commission refers UK to Court over privacy and personal data protection, IP/10/1215' Brussels, 30 September 2010. The incident that drew the attention of the European Commission to the U.K. implementation of the provisions relating to the interception of communications was a targeted advertising technology, known as "Phorm". Phorm functions by taking a copy of the information that passes between end-users and websites making use of Policy Based Routing (PBR) and Deep Packet Inspection (DPI).

[62] EUROPEAN COMMISSION, 'Press Release: Telecoms: Commission launches case against UK over privacy and personal data protection, IP/09/570' Brussels, 14 April 2009.

[63] EUROPEAN COMMISSION, 'Press Release: Telecoms: Commission steps up UK legal action over privacy and personal data protection, IP/09/1626' Brussels, 29 October 2009.

[64] EUROPEAN COMMISSION, 'Press Release: Telecoms: Commission steps up UK legal action over privacy and personal data protection, IP/09/1626' Brussels, 29 October 2009.

information relates. However, ensuring the confidentiality of communications does not prevent technical storage of data, if this is necessary for the conveyance of a communication.

According to Art. 5.2 communications may also be recorded, when legally authorised, if this is carried out in the course of a lawful business practice for the purpose of providing evidence of a commercial transaction or any other business communication.[65] This would, for example, cover the recording of a call made to a business call centre, provided that the user is made aware of the recording and its purpose and has a right to refuse the recording.

Recital (23) specifies that "confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged."

Article 5.2 thus provides for an exception to the confidentiality of communications and the related traffic data in the context of lawful business practice. The provision allows for the recording of communications, if and when such recording is necessary and legally authorised (Recital 23), in order to provide evidence of a commercial transaction or of any other business transaction. The issue with this particular provision is directly related with the scope ascribed to it in the national transpositions. In principle, the provisions of the ePrivacy Directive are meant to regulate the processing of personal data in a specific sector, i.e. the electronic communications sector. This follows directly from the scope-setting provision in Article 3 of the ePrivacy Directive, as well as the scope of the whole regulatory framework for electronic communications of which the ePrivacy Directive is an important part.

Exceptions to the prohibition of breaching confidentiality of communications may be included in national legislation for safeguarding national security, defence or public security and for the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system. In these circumstances, data may be retained for a limited period.[66]

Last but not least, there is a general exception for "technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality"[67].

[65] Article 5.2 ePrivacy Directive.

[66] Article 15.1 ePrivacy Directive.

[67] Article 5.1 ePrivacy Directive.

4.2. Transposition in the Member States

4.2.1. Article 5.1

According to Art. 5.1 of the Directive the Member States should ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, "through national legislation". It is therefore not surprising that the legal rules with regard to the protection of confidentiality strongly differ.

First of all, there is a difference in what is understood by the protection of confidentiality of communications and how this protection is being achieved in practice. With regard to content, Belgium and Germany, for example, both consider the content of communications worthy of protection only when in transit. Before a message is sent or once this message has been received, the confidentiality of the information is protected under another legal regime. General data protection rules apply at this stage.

Furthermore, while Belgium, Germany and the UK have different provisions covering the confidentiality of content and traffic data, Poland has one provision dealing with both.

All Member States have an exception to confidentiality of communications for law enforcement purposes. However, the French provisions for the retention of traffic data in the context of copyright infringement case are quite unique, given their far-reaching nature.

Across the Union similar differences can be found. Some Member States treat traffic data and content differently (CY, EL, IE and RO), others have one provision/instrument covering both types of data (AT, BG, CZ, DK, EE, ES, FI, HR, IT, LT, LU, LV, MT, NL, PT, SK and SV). For some Member States only when content is in transit is it considered *a communication* of which the confidentiality should be protected (e.g. BG, CZ, EE, ES, IT, LT, MT, NL, PT, SK and SV), while for others this scope is broadened (AT, HU and LV). In certain countries, the confidentiality of communications is considered a fundamental right, enshrined in the Constitution (AT, BG, CY, EL, ES, FI, PT and RO). In all Member States there are exceptions for law enforcement access to communications.

Our analysis of the laws of the Member States shows that none of these Member States has provisions that deal explicitly with automated data processing, without human involvement, in the context of a breach of confidentiality of electronic communications. Moreover, Sweden requires the involvement of a person in order to speak of an illegitimate breach of confidentiality. Belgium and Germany will consider

the interception of MAC addresses a breach of confidentiality (idem in AU, FI, HU, IT, L, NL, RO and SV), while in France there will need to be additional data captured that link the MAC to an individual. Capturing, without consent, data being transferred in a WiFi network will be considered a (criminally sanctioned) breach in Belgium, Germany, France and the UK, unless there is legal ground for it (also AT, FI, HU, IT, LU, NL, RO and SV).

The conclusion is consequently that the legal rules and the way they are interpreted by authorities and courts with regard to the protection of confidentiality in the context of public electronic networks and publicly available electronic communications services, are not harmonised across the Union. This is due to the fact that Art. 5.1 of the ePrivacy Directive merely contains a very general request to "ensure the confidentiality of communications" without much further detail.

4.2.2. Business Exception

As far as the transposition of Art. 5.2 is concerned, more interesting observations can be made. Member States apparently have taken very different approaches towards transposing the lawful business exception included in this provision.

At first sight, some Member States such as Belgium and the United Kingdom have transposed the lawful business exception in a rather extensive way, encompassing both possible purposes in Article 5.2. These purposes are providing (a) evidence of a commercial transaction and (b) evidence of any other business communication. Both Member States require, however, that the users are informed beforehand of the recording. The level of granularity with which the United Kingdom outlines the modalities of the lawful business exception stands out. On a different note, it is interesting to see that the Belgian legislator made an explicit mention of an exception for call centres.

Germany, France and Sweden, on the other hand, have not transposed the lawful business exception. The German and Swedish reasons for not transposing Article 5.2 ePrivacy Directive are not entirely clear, yet appear to go in the same direction. The German correspondent indicates that it might be because Germany favours a more strict protection of the right to data protection, and the exception in Article 5.2 ePrivacy Directive would be too big an interference. The Swedish correspondent similarly reasons that the transposition of the lawful business exception would indeed water down the protection offered in Article 5.1.

Between the remaining 22 Member States there are equally significant discrepancies. First of all, it is remarkable how much confusion the lawful business exception apparently creates. In several country reports the correspondents indicated that Article 5.2 has indeed been transposed into national law, but when it appears in fact to be quite a literal – albeit partial – transposition of Article 6 of the ePrivacy Directive

(CZ, DK, FI, IT (although this Member States has additional provisions in labour law), LV, NL and SK). In practice, this means that the national implementation covers only traffic data and is aimed solely at operators and providers of electronic communication services.

In three Member States the lawful business exception cannot really be considered transposed, given that the national implementation relies on consent of the users, which would make it an application of Article 5.1 of the ePrivacy Directive (EL, ES and HU). Austria has not transposed the lawful business exception in its pertinent implementing legislation since Article 5.2 of the ePrivacy Directive has been deemed to lie outside the scope of the Directive. Austria has therefore included only exceptions to confidentiality in its general data protection legislation for emergency services and call centres. Some countries have transposed the lawful business exception *verbatim* (CY, HR, IE, MT and RO). Others have not strayed far from the original provision, but have added the requirement to notify the user beforehand of the recording of the communication and related traffic data (BG, LT, LU, PT and SV). In Estonia, the national transposition combines both Articles 5.1 and 5.2 into a single provision, but the scope should be the same – at least with respect to the lawful business exception – as Article 5.2 of the ePrivacy Directive. Portugal, similarly to Belgium, has included the call centre exception but also explicitly includes the duty to notify the national data protection authority. Finally, there are two countries where only the first purpose of the lawful business exception (evidence of a commercial transaction) has been included in the national transposition, thus narrowing the scope somewhat (BG and LT).

4.2.3. Consent

As already mentioned, actions that enable the interception or surveillance of communications are allowed when the users concerned have given their consent. Recital (17) specifies that, "for the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website".

For the definition of "consent" Art. 2(f) of the ePrivacy Directive refers to Directive 95/46/EC. This definition is also the one used in the national laws of the Member States, with the exception of Germany, where the legislator introduced a specific notion of "electronic consent".[68] Since Germany is the only Member State to have introduced a distinct definition of consent for the online environment, it seems

[68] KOSTA, Eleni, *Consent in European Data Protection Law*, Leiden-Boston, Martinus Nijhoff Publishers, 2012, in particular p. 277-284.

appropriate to provide a few more details about this concept in the German legislation.

Section 94 of the German Telecommunications Act provides that the consent can be provided electronically, when the service provider ensures the following:

(a) The subscriber or the user has given his consent consciously and unambiguously
(b) The consent is logged
(c) The subscriber or the user can access at any time the content of the consent and
(d) The subscriber or the user can withdraw at any time the consent with an effect for the future.

The first condition for the provision of a valid electronic consent is that the subscriber or the user has given his consent consciously and unambiguously.[69] This means that the user or the subscriber should have an active wish to act (give his consent) and should be aware that he is consenting, realising the nature and the extent of the processing of this personal data he is consenting to.[70] This condition aims at the exclusion of any coincidental or unintentional agreement to the processing of personal data. The provision of the consent of the user can be inferred by his pressing on the requested buttons of his phone in order to validate his choice.[71] The service provider has to inform the user or the subscriber about all the important circumstances relating to the specific consent that is requested. Thus, general or blanket information on the potential of an electronic consent will not meet this requirement.[72] It should be clear to the user or the subscriber that his consent relates to the processing of personal data. The Higher Regional Court of Brandenburg (*Oberlandesgericht – OLG*) clarified that it suffices when an average rational user (*durchschnittlich verständlicher Nutzer*) can recognise (and he has to be able to recognise) that he is consenting in a legally binding way to the processing of his personal data.[73]

The second condition for the provision of valid electronic consent is the logging of the consent by the data controller, while there is no obligation for a parallel storage of the

[69] Section 94 Nr. 1 German Telecommunications Act.
[70] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 7; BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in Geppert, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 6.
[71] BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in GEPPERT, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 4.
[72] BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in Geppert, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 6.
[73] OLG Bradenburg, *Urteil* vom 11.01.2006 - 7 U 52/05 (LG Potsdam), Multimedia und Recht (MMR) 2006, p. 406. [LG POTSDAM, Urteil vom 10.03.2005 - 12 O 287/04, Datenschutz und Datensicherheit (DuD) (2005) 29, p. 302.]

consent by the data subject.[74] The logging can be realised via the storing of the electronic consent. Although the German Telecommunications Act does not contain any specification on how the logging should be realised, the service should store not only the content of the consent, but also the time when it was given.[75] In any case, the logging should be realised in such a way that it serves the right of the data subject to informational self-determination.[76] This provision aims at enhancing the data subject's ability to relate to when, for which purpose, and in which circumstances he has consented electronically to the processing of his personal data.[77] The stored consent consists in itself of personal data.[78]

For the electronic provision of consent, it has to be ensured that the data subject has access to the full content of the consent at all times,[79] ensuring respect of the transparency principle. This presupposes that the service provider has logged and stored the provided consent in order to be able to provide it to the data subject upon the latter's request. There is no specific requirement on the form in which the consent can be accessed by the data subject. However, it is submitted that access to the content of the consent should be realised using the same device as the one used for the actual provision of the consent.[80] In addition, the service provider has to take the necessary measures to ensure that only the data subject can have access to the consent he has provided.[81]

The final condition foresees that users or subscribers can withdraw their consent at any time with an effect for the future. However, the data subject cannot demand the immediate withdrawal of his consent. Therefore, the use of the personal data based on the consent given by the data subject during the time between the request for the withdrawal of the consent and the actual moment when the withdrawal becomes

---

[74] Section 94 Nr. 2 German Telecommunications Act.

[75] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 8; BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in GEPPERT, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 9.

[76] BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in GEPPERT, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 9

[77] BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in GEPPERT, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 7.

[78] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 8.

[79] Section 94 Nr. 3 German Telecommunications Act.

[80] BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in GEPPERT, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 10.

[81] BÜTTGEN, Peter, 'TKG § 94 Einwilligung im elektronischen Verfahren' in GEPPERT, Martin et al. (eds), *Beck'scher TKG-Kommentar* (Verlag C.H. Beck, München 2006), para. 10; ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 9.

effective is legitimate, if it is justified on objective grounds.[82] Specific factors, such as the complexity in the structure of the company and its IT systems, should be taken into account for the determination of the reasonable time for the withdrawal to become effective.[83] It is interesting to note that Section 94 Nr.4 of the Telecommunications Act does not lay down a respective obligation of the service provider to inform the data subject on his right to withdraw the consent. It has been submitted that the lack of explicit reference to such an obligation of the service provider was intentional during the drafting of the Act, which in practice renders the possibility for withdrawal of consent difficult, as the data subject is not informed about his right to ask for the withdrawal of consent.[84]

4.3. Evaluation

Article 5.1 of the ePrivacy Directive protects the confidentiality of communications and the related traffic data. The provision specifies a few examples of types of conduct by persons other than users which should be prohibited if there exists no legitimising grounds for it in law. The provision states that "in particular, they (Member States) shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users".

It is not clear what this implies when there is not immediately a person involved, but the registration of electronic communications – whether it be content or traffic data – happens automatically by machines without anyone having to intervene. There are various types of technologies which are fully automated and are aimed at registering electronic communications, sometimes on a very large scale. An example could be an Intrusion Detection System (hereinafter: IDS) which includes a Deep Packet Inspection (hereinafter: DPI) module. DPI is commonly understood as a rule-based detection technique which allows a system not only to look at the headers of IP packets, but also at their content. It can be used to detect e.g. malware or phishing mails on (public or private) networks. It is possible that such a system has quite a profound impact on the confidentiality of the electronic communications passing through the IDS, given that even content is (theoretically) accessible. Given that DPI is an automated rule-based

[82] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 10.
[83] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 10.
[84] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §94, para 11.

detection technique no human intervention is needed after the initialisation of the system.

Another example can be found in the growing mobile applications market. Many apps that users install on their smartphones ask for access to, *inter alia,* contact lists, SIM card data, even text messages or calendars, even when the app does not necessarily need access to these data sources to function properly. Moreover, all of this processing happens automatically. The question thus arises whether Member States' implementing laws forbid such automated registration of communications-related data if no legitimising grounds are available, given the impact on the right to privacy and confidentiality. One could argue that such unjustified intrusions, even with the consent of the user – requested according to Art. 5.3 of the Directive – are not compliant with the proportionality principle applicable to the processing of personal data.

It is evident that confidentiality of electronic communications should also be protected against "automatic" intrusions without human intervention. This clarification could be added in a Recital to the Directive.

A next question relates to the current fragmentation. Article 5.1 leaves a wide margin of decision to the Member States for regulating this matter. Should this field be further harmonised?

As a matter of fact the ePrivacy Directive has a dual objective, given the importance ascribed to the aim of protecting privacy and confidentiality of communications. Article 1 stipulates that the intention is also to harmonize the national relevant legislation so as to ensure the free flow of data as well as electronic communication equipment and services in the European Union. The borderless nature of services provided online and since 2000 also the Charter of Fundamental Rights of the European Union may require indeed an aligned legal framework across the Union. If not, it creates significant burdens on service providers to comply with different national obligations in each Member State where services are deployed.

Nevertheless, as far as the confidentiality principle of Art. 5.1 of the ePrivacy Directive is concerned, a higher degree of harmonisation would be difficult to achieve in the short term. In most of the Member States the legislation on this topic is spread over various instruments, including the Constitution, the Penal Code, the rules on Criminal Procedure, etc. and much of this legislation has a long and complex historical background.

Divergences between Member States with regard to the protection of confidentiality of communications are mainly related to definitions, conditions and other modalities and, evidently, also to the exceptions. This is due to the fact that Art. 15.1 of the ePrivacy Directive states that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction

constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC".

As a consequence rules with regard to e.g. wiretapping for law enforcement purposes or monitoring electronic communications in an employment context, are not harmonized at the European level. This situation will not fundamentally change after the transposition by the Member States of the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (so-called "Law Enforcement Directive"). The scope of this proposed Directive is restricted to the processing of personal data by law enforcement authorities and does not deal with topics such as the interception of electronic communications. Further harmonisation of the rules with regard to these topics would also be difficult to achieve in the short term since they are, in most of the Member States, integrated into specific national criminal procedure rules.

In order to bring the text of Art. 5.1 into line with the proposed widening of the scope of the ePrivacy Directive, we suggest amending it and making it applicable to "confidentiality of communications and the related use of traffic data by means of a public or publicly accessible private communications network". It is further evident that confidentiality of electronic communications should also be protected against "automatic" intrusions without human intervention. This clarification could be added in a Recital to the Directive, noting that automated intrusions are of course always initiated and/or controlled by one or more persons. Last but not least the exception from Art. 5(1) for "technical storage which is necessary for the conveyance of a communication" could be broadened to "storage as far as necessary for ensuring the functioning of the network or the provision of the service on that network". Such amendment is nothing more than a logical consequence of the extension of the scope of Art. 5.1 to e.g. information society services.

Article 5.2 of the ePrivacy Directive stipulates that the protection of confidentiality "shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication". This provision – often designated as the "business exception" - has been interpreted and transposed by Member States in very different ways. National legislators in some of the Member States have restricted the scope of Art. 5.2 to the electronic communications sector. In other Member States the provision is applied to all sectors and is aimed at giving employers some margin to register telephone

conversations conducted by employees in the context of, for instance, a call centre. We suggest therefore clarification of the scope of Art. 5.2 in order to obtain a uniform transposition and implementation of this provision throughout the Union. The current restriction to “the provision of evidence of a commercial transaction or of any other business transaction” could be widened to other situations in which recording of communications in an employment context seems to be justified, such as quality control or legitimate supervision of work performance. A clear legal basis for monitoring communications of employees for such legitimate reasons and under the condition to respect general data protection rules is currently missing on the European level.

5. Cookies and Similar Intrusions

This Chapter focuses on Article 5(3) of the ePrivacy Directive. Like the previous Chapter, we will first analyse the provision of the Directive in detail, in order to enable a correct assessment of the transposition into the national law of the Member States. This will result in a short evaluation including suggestions and recommendations.

5.1. Article 5.3 ePrivacy Directive

Article 5.3 of the ePrivacy Directive reads as follows:

> *Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*[85]

5.1.1. Scope of Application

The original phrase contained in the 2002 version of the ePrivacy Directive "the use of electronic communications networks to store information or to gain access to information stored"[86] was replaced in 2009 by "the storing of information or the gaining of access to information already stored" in order to expand the application of Article 5.3. Recitals 24 and 25 of the ePrivacy Directive provided clarification on what was covered by Article 5.3 of the 2002 ePrivacy Directive.

The amended provision covers not only unwanted spying programs or viruses which are inadvertently downloaded via electronic communications networks, but also hidden programs that are delivered and installed in software distributed on other external storage media**,** such as CDs, CD-ROMs, USB keys, flash drives, etc.[87] This amendment was primarily inspired by lessons learned from the Sony-MediaMax case.

In 2003, the Music Company Sony/BMG introduced a tool, called MediaMax, as a Digital Rights Management (DRM) system in order to limit the number of musical

[85] Article 5.3 ePrivacy Directive.

[86] Old Article 5.3 2002 ePrivacy Directive.

[87] Recital 65 Citizens' Rights Directive.

copies of its CDs. However, MediaMax did much more than prevent piracy and limit the number of music copies that could be produced from a CD. When a MediaMax CD was inserted into the computer of a user, a rootkit[88] was installed in the terminal equipment of the user, without informing him or requesting his consent for the installation.[89]

The public reaction against Sony/BMG led to consumer complaints around the world. The European Commission realised that the existing legal framework on the regulation of spyware and similar devices (i.e. Article 5.3 of the 2002 ePrivacy Directive) did not cover cases as the one described above, because it was applicable only when electronic communications networks were used to store information or to gain access to information stored in the terminal equipment of a user or a subscriber. Realising the inability of the legal framework to cope with the technological challenges, the European Commission decided to propose broadening the scope of Article 5.3 of the ePrivacy Directive in order to cover unwanted spying programs or viruses that "are delivered and installed in software distributed on other external storage media, such as CDs, CD-ROMs, USB keys"[90].

Recital 24 of the ePrivacy Directive, which refers to Article 5.3, clarifies that the "[t]erminal equipment of users of electronic communications networks and any information stored on such 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"[91]. The Recital refers to *any information* that is stored on the terminal equipment of a user and not only to information that qualifies as personal data, stressing that any such information is part of the private sphere of the user and deserves protection. This supports the argument that the reference to information in Article 5.3 is intentional and aims at extending the scope of this provision not only to cases when the storing of information or the gaining of access to information entails personal data, but in all cases when any kind of information is involved.[92] The Article 29 Working Party confirmed this approach and took the position that as Article 5.3 of the ePrivacy Directive does not qualify the types of

[88] "Rootkit: A program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit.

[89] PANIZA-FULLANA, Antonia, 'DRM Sony system, consumer protection and user privacy' in MERCADO-KIERKEGAARD, S. (ed) *The first international conference on Legal, Privacy and Security Issues in IT (LSPI 2006)* (Institutt for rettsinformatikk, Hamburg, Germany 2006), p. 67-72

[90] Recital 65 Citizens' Rights Directive.

[91] Recital 24 ePrivacy Directive.

[92] DEBUSSERÉ, Frederic, 'The EU E-Privacy Directive: A monstrous attempt to starve the cookie monster?' (2005) 13 International Journal of Law and Information Technology, pp. 84-85.

information, it "is not a prerequisite for the application of this provision [i.e. Article 5.3] that this information is personal data within the meaning of Directive 95/46/EC".[93]

5.1.2. Historical Background of the Consent Requirement

The Citizens' Rights Directive amended Article 5.3 of the ePrivacy Directive by introducing the consent of the subscriber or the user as a requirement for the storing of information or gaining access to information that is already stored in their terminal equipment, after he has been provided with clear and comprehensive information, in accordance with the Data Protection Directive.

The old provision, as formulated in the 2002 ePrivacy Directive, required the use of electronic communications networks for such actions on the condition that the subscriber or user concerned is provided with clear and comprehensive information and is offered the right to refuse such processing.[94]

The provision on the storing of or gaining access to information already stored on the terminal equipment of a user or a subscriber was not included in the initial proposal of the European Commission for the 2002 ePrivacy Directive.[95] Such a provision was first introduced by the European Parliament during its first reading of the 2002 ePrivacy Directive and read as follows:

> *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.*[96]

---

[93] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP171' (2010), p. 9.

[94] The old Article 5.3 of the 2002 ePrivacy Directive stated that "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 […]."

[95] COMMISSION OF THE EUROPEAN COMMUNITIES, Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector COM(2000) 385 final - 2000/0189(COD) [2000] OJ C365E/223 (19.12.2000).

[96] EUROPEAN PARLIAMENT, First reading (co-decision procedure) Proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 - C5-0439/2000 - 2000/0189(COD)), A5-0374/2001 [2001] OJ C140E/121 (13.06.2002), Amendment 26.

The European Parliament required the *prior, explicit consent* of the subscriber or user concerned for the storing of information or gaining of access to information that is stored on their terminal equipment.

The Council in its common position replaced the prohibition that was introduced by the European Parliament with a provision permitting the storing of or gaining access to information on the condition that the user or the subscriber is offered information and a right to refuse.[97] This choice was adopted in the final version of the 2002 ePrivacy Directive. It seems that the financial and practical burden that could be carried by the industry with regard to the use of cookies or similar devices played a large role in the watering down of the initial proposal of the European Parliament and the removal of the requirement for explicit consent.

The discussions relating to Article 5.3 and the conditions on which the storing of information or the gaining of access to information that is already stored on the terminal equipment of users, which was relevant for the installation and use of cookies, was rekindled during the review of the electronic communications framework, part of which was the ePrivacy Directive. The initial proposal of the European Commission for the Citizens' Rights Directive was presented in 2007 and did not wish to modify the existing regime relating to Article 5.3 of the ePrivacy Directive. The Commission proposal aimed only at the broadening of the scope of this provision, so that the involvement of an electronic communications network would not be required anymore for its application.[98] The European Commission clarified that the

[97] Article 5.3 was amended by the Council as follows: "*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 receives in advance clear and comprehensive information, inter alia, about the purposes of the processing, in accordance with Directive 95/46/EC, 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*": COUNCIL OF THE EUROPEAN UNION, Common Position (EC) No 26/2002 adopted by the Council on 28 January 2002 with a view to adopting Directive 2002/. . ./EC of the European Parliament and of the Council of . . . concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002/C 113 E/03) [2002] OJ C113E/39 (14.05.2002), DEBUSSERÉ, Frederic, 'The EU E-Privacy Directive: A monstrous attempt to starve the cookie monster?' (2005) 13 International Journal of Law and Information Technology, p. 80.

[98] The European Commission proposed that Article 5.3 of the ePrivacy Directive is replaced as follows : "*3. Member States shall ensure that the storing of information, or gaining access to information already 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*

amendment of Article 5.3 of the 2002 ePrivacy Directive constitutes a technical adjustment to the wording of the Directive, which ensures that

> *"use of 'spyware' and other malicious software remains prohibited under EC law, regardless of the method used for its delivery and installation on a user's equipment (distribution through downloads from the Internet or via external data storage media, such as CD-ROMs, USB sticks, flash drives etc.)"*[99].

The European Parliament saw the review of the electronic communications framework as an opportunity to reiterate its wish for a consent requirement for the storing of information, or gaining access to information already stored, in the terminal equipment of a subscriber or user. During the first reading of the Citizens' Rights Directive, the European Parliament introduced the requirement for consent with regard to the use of cookies and similar devices, repeating in this way its desire to introduce the consent of the subscriber or the user as a requirement; a desire that had remained unfulfilled during the adoption of the 2002 ePrivacy Directive. Amendment 128 of the first reading of the European Parliament proposed the modification of Article 5.3 of the ePrivacy Directive as follows:

> *3. Member States shall ensure that the storing of information, or gaining access to information already stored, in the terminal equipment of a subscriber or user,* ***either directly or indirectly by means of any kind of storage medium, is prohibited unless*** *the subscriber or user concerned* ***has given his/her prior consent, taking into account that browser settings constitute prior consent, and*** *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 data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communication network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.*[100]

---

subscriber or user": COMMISSION OF THE EUROPEAN COMMUNITIES, 'Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation' COM(2007) 698, 13(1)1.2007, p. 34.

[99] COMMISSION OF THE EUROPEAN COMMUNITIES, 'Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation' COM(2007) 698, 13(1)1.2007, p. 12.

[100] EUROPEAN PARLIAMENT, 'Legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive

The amendment of the European Parliament on the requirement of consent was not accepted by the European Commission[101], but was reintroduced by the European Parliament during its second reading on the Citizens' Right Directive, albeit with a partly modified wording:

> *3. Member States shall ensure that the storing of information, or* **the gaining of** *access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned* **has given his/her consent, having been** *provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing* ▌ *. This shall not prevent any technical storage or access for the sole purpose of carrying out* ▌ *the transmission of a communication over an electronic communications network, or as strictly necessary in order* **for the provider of** *an information society service explicitly requested by the subscriber or* user **to provide the service**.[102]

The European Parliament, in the amendment it introduced during the second reading, did not include the clarification that "browser settings constitute prior consent", which was part of the initial amendment of Article 5.3 as suggested during its first reading. This choice was moved to Recital 66 which clarified that "the user's consent to processing may be expressed by using the appropriate settings of a browser or other application"[103] and will be examined below.

The European Commission, followed by the Council of the European Union, accepted the amendments of the European Parliament on the introduction of a requirement for the consent of the user or the subscriber for the use of cookies and similar devices[104],

---

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (First Reading) (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD))', 24.09.2008, Amendment 128.

[101] COMMISSION OF THE EUROPEAN COMMUNITIES, 'Amended proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation' COM (2008) 723 final, 06.11.2008.

[102] EUROPEAN PARLIAMENT, 'Legislative resolution of 6 May 2009 on the common position adopted by the Council with a view to the adoption of a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Second Reading) (16497/1/2008 – C6-0068/2009 – 2007/0248(COD))', 06.05.2009, Article 5.3.

[103] Recital 66 Citizens' Rights Directive.

[104] "The Commission amends its Proposal in line with the amendments voted by the European Parliament at its plenary session on 6 May 2009": COMMISSION OF THE EUROPEAN COMMUNITIES,

which it had rejected a few months before. The European Parliament had achieved what it failed to do in 2002: the consent of the person concerned was explicitly mentioned in Article 5.3 as a requirement for the storing of information or the gaining of access to information that is already stored in the terminal equipment and it opened Pandora's Box on the interpretation of this new provision.

After the Council of the European Union approved the amendments made to the Citizens' Rights Directive by the European Parliament during its second reading[105] and before the final signing of the Directive by the European Parliament and the Council[106], thirteen European Member States, realising the potential implications the new requirement in Article 5.3 could have for industry players, made a relevant statement. Austria, Belgium, Estonia, Finland, Germany, Ireland, Latvia, Malta, Poland, Romania, Slovakia, Spain and the United Kingdom commented on the amendment of Article 5.3 of the ePrivacy Directive and stated

> *These Member States recognise that this clarification [i.e. the conditions under which information, including unwanted spy programmes or other types of malware may be placed on an individual's terminal equipment] may require the modification of some national laws. However, as indicated in Recital 66, amended*

'Opinion of the Commission pursuant to Article 251(2), third subparagraph, point (c) of the EC Treaty, on the European Parliament's amendments to the Council's Common Position regarding the Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws' COM(2009) 421 final, 29.07.2009, p. 5.

[105] COUNCIL OF THE EUROPEAN UNION, 'List of "A" items for the 2970th meeting of the Council of the European Union, 14866/09' (2009), Brussels, 23.10.2009 , listed the approval of the amendments of the European Parliament to the Citizens' Rights Directive as item Nr. 25. Although the content of the minutes from the 2970th meeting of the Council of the European Union is not available to the public [COUNCIL OF THE EUROPEAN UNION, 'Draft minutes of the 2970th meeting of the Council of the European Union (General affairs and external relations), held in Luxembourg on 26 October 2009' (2009), Brussels, 01.11.2009, content not available to the public], the Addendum to the minutes, dated 17th of November 2009, explicitly mentions that "The Council approved the European Parliament's amendments to the common position. The above Regulation is therefore deemed to have been adopted in the form of the common position thus amended. (Legal basis: Article 95 of the Treaty establishing the European Community)": COUNCIL OF THE EUROPEAN UNION, 'Addendum to Draft Minutes: 2970th meeting of the Council of the European Union (General affairs and external relations), held in Luxembourg on 26 October 2009, 14985/09, ADD 1, PV/CONS 55', Brussels, 17.11.2009, p. 7.

[106] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 'Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, 2007/0248 (COD)-LEX 1102, PE-CONS 3674/1/09-REV 1', Strasbourg, 25.11.2009.

> *Article 5.3 is not intended to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purposes. These Member States also stress that the methods of providing information and offering the right to refuse should be as user-friendly as possible.*[107]

The thirteen Member States based their argument on the wording of Recital 66 of the Citizens' Rights Directive, which actually kept the phraseology of the former Article 5.3 of the 2002 ePrivacy Directive and stipulated that:

> *It is therefore of paramount importance that **users be provided with clear and comprehensive information** when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and **offering the right to refuse** should be as user-friendly as possible. […] Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the **appropriate settings of a browser or other application**. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.*[108] *(emphasis added)*

Contrary to the wording of the new Article 5.3 of the ePrivacy Directive, Recital 66 of the Citizens' Rights Directive refers to the provision of clear and comprehensive information to the users, offering them a right to refuse. The thirteen Member States, in light of the clarification provided by Recital 66 of the Citizens' Rights Directive, interpreted the consent of the user that is required in the new Article 5.3 of the ePrivacy Directive as "a right to refuse the use of cookies or similar technologies used for legitimate purposes".[109] In this way they took the position that the new Article 5.3

---

[107] COUNCIL OF THE EUROPEAN UNION, 'Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1', Brussels, 18.11.2009, as corrected by Council of the European Union, 'Corrigendum to the Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1 COR 1', Brussels, 19.11.2009.

[108] Recital 66 of the Citizens' Rights Directive.

[109] COUNCIL OF THE EUROPEAN UNION, 'Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and

should not be seen as intending to change the existing situation with regard to the installation of cookies for legitimate purposes. Rather, the currently offered right to refuse should be considered as sufficient to fulfil the requirements of the new provision.

The Article 29 Working Party in its opinion on online behavioural advertising dealt with the interpretation of the new Article 5.3 of the ePrivacy Directive and took the position that the changes introduced in this provision "clarify and reinforce the need for users' informed prior consent", reaching a different conclusion to the position of the aforementioned thirteen Member States. The Article 29 Working Party broke down the new requirement in Article 5.3 to two clear conditions, which, when fulfilled, can legitimate the storing of information or the gaining of access to information that is already stored in the terminal equipment of the subscriber: on the one hand, the subscriber or the user has to be provided with clear and comprehensive information in accordance with the Data Protection Directive about, inter alia, the purposes of the processing; on the other hand, the subscriber or the user has to give his consent to the storage of or the access to information that is stored in his terminal equipment, after having been provided with the aforementioned information. These two conditions apply cumulatively. The Article 29 Working Party paid special attention to the latter condition, relating to the consent of the user or the subscriber, and derived the following two requirements from the wording of Article 5.3:

> *i) consent must be obtained* before *the cookie is placed and/or information stored in the user's terminal equipment is collected, which is usually referred to as prior consent and ii) informed consent can only be obtained if prior information about the sending and purposes of the cookie* has been given to the user.[110]

5.1.3. Exceptions from the Consent Requirement

The storing of information or the gaining of access to information that is already stored in the terminal equipment of the subscriber or the user is allowed in two exceptional cases: (a) for the technical storage of or access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and (b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the access to information is strictly necessary for the provider.[111]

Neither the recitals of the 2002 ePrivacy Directive, nor those of the Citizens' Rights Directive provide any specificity in relation to these exceptions. The former exception

services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1', Brussels, 18.11.2009, p. 3.

[110] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP 171' (2010), p. 13.

[111] Article 5.3 ePrivacy Directive, last sentence.

can be seen as allowing the use of mere session cookies[112]. The latter relates to the provision of information society services that are explicitly requested by the subscriber or the user and when the storage of or the access to information is **strictly necessary** in order for the provider of the service to provide it. In view of the lack of any clarification at European level on when the storage or the access is strictly necessary, the U.K. ICO has provided some guidance on the interpretation of this exception:

> *The term 'strictly necessary' means that such storage of or access to information should be essential, rather than reasonably necessary, for this exemption to apply. However, it will also be restricted to what is essential to provide 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 to comply with any other legislation the service provider might be subject to, for example, the security requirements of the seventh data protection principle […]. Where the use of a cookie type device is deemed 'important' rather than 'strictly necessary', those collecting the information are still obliged to provide information about the device to the potential service recipient so that they can decide whether or not they wish to continue. The information provided about what the collector intends to use that data for should be clear enough to enable the user to make a truly informed decision.*[113]

5.1.4. Information To Be Provided

It may seem strange that Article 5.3 of the ePrivacy Directive contains a specific information requirement, which would at first seem to overlap with the information requirement of the data controller, as specified in Article 10 of the Data Protection Directive. However, the scope of Article 5.3 covers not only personal data, but any kind of information and therefore the inclusion of the information requirement in Article 5.3 renders it obligatory, even when no processing of personal data is taking place.[114] The Article 29 Working Party has specified the information that should be provided to the users with regard to the installation and use of cookies:

> *the user should be informed when a cookie is intended to be received, stored or sent […]. The message should specify, in generally understandable language,*

[112] DEBUSSERÉ, Frederic, 'The EU E-Privacy Directive: A monstrous attempt to starve the cookie monster?' (2005) 13 International Journal of Law and Information Technology, p. 92.
[113] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories, v.3.4' (30.11.2006), p. 7.
[114] DEBUSSERÉ, Frederic, 'The EU E-Privacy Directive: A monstrous attempt to starve the cookie monster?' (2005) 13 International Journal of Law and Information Technology, p. 88.

which information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie.[115]

The information that has to be provided to the user or the subscriber before obtaining their consent should comply with Article 10 of the Data Protection Directive. More specifically, the user or the subscriber should be informed about the identity of the entity that wishes to store information or gain access to information that is already stored in his terminal equipment and about the purposes of the processing. Moreover, he should be provided with any information relating to the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of their right of access, the right to rectify the data concerning him and the right to refuse the storing of or the access to their information.

In the context of cookies and similar devices, the information on whether replies to the questions are obligatory or voluntary and on the possible consequences of failure to reply can be interpreted as 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"[116]. Recital 25 of the 2002 ePrivacy Directive specified that the access to specific website content may be made conditional on the acceptance of a cookie or similar device after the user is provided with clear and comprehensive information, if the cookie is used for a legitimate purpose.[117] This means that a website or service provider can restrict access to the users, if they do not agree to accept cookies. The Article 29 Working Party criticised such an approach, finding that it can be contradictory to the position that the users should have the possibility to refuse the storage of a cookie on their personal computers. It therefore noted that this provision may need to be clarified or revised.[118] However, the Citizens' Rights Directive, which amended the ePrivacy Directive in 2009, did not provide any additional clarification on this point.

Given the modalities of the internet and the lack of personal communication between the entity that wishes to install and use cookies or similar devices and the user, the concept of giving this information "in a clear and comprehensive way" is problematic. Does the provision of the information in the general terms and conditions or in the privacy policy of a service suffice for it to be considered as given "in a clear and

---

[115] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, WP17' (1999), p. 3

[116] DEBUSSERÉ, Frederic, 'The EU E-Privacy Directive: A monstrous attempt to starve the cookie monster?' (2005) 13 International Journal of Law and Information Technology, p. 87.

[117] Recital 25 2002 ePrivacy Directive

[118] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, WP126' (2006), p. 3

comprehensive way"? Recital 66 of the Citizens' Rights Directive, requires that the "methods of providing information […] should be as user-friendly as possible"[119]. Currently, the information is provided in the general terms and conditions or in the privacy policy of the providers' websites. However, the Article 29 Working Party considers information provided in this manner to be "hidden" to the user and proposes that certain key information should be presented on the screen of the user in an interactive way, so that it is clearly spotted by the user; the rest in layers. To this end, the Article 29 Working Party welcomes creativity on new ways of presenting the information to the user that would go beyond the current practices of pop-up windows.[120]

As Article 5.3 does not cover only personal data, but any kind of information, it is applicable to any entity that wishes to store or gain access to information that is already stored in the terminal equipment of the user or the subscriber, irrespective of their function as data controller or data processor.[121] The lack of specification on this point, especially when multiple entities are involved in the installation of and access to a cookie, has been highlighted by the U.K. ICO, who provide guidance on clarifying who bears the responsibility for the provision of the information to the user or the subscriber.

> *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 recognise 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 these cases, the organisation the site primarily refers to will be obliged to alert users to the fact that a third party advertiser operates cookies. It will not be enough for that organisation to provide a statement to the effect that they cannot be held responsible for any use of such devices employed by others they*

[119] Recital 66 Citizens' Rights Directive. This Recital in fact repeats Recital 25 of the 2002 ePrivacy Directive, which stated that "The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible". It is worth noting that Recital 25 of the 2002 ePrivacy Directive refers to the methods for offering a right to refuse or requesting consent, although Article 5.3 of the 2002 ePrivacy Directive referred only to the right to refuse, while Recital 66 of the Citizens' Rights Directive refers only to the methods offering a right to refuse, although the amended Article 5.3 of the ePrivacy Directive refers to the obtaining of the consent of the user or the subscriber".

[120] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP171' (2010), p. 18

[121] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP171' (2010), p. 9.

allow to place content on their websites. The third party would also have a responsibility to provide the user with the relevant information.[122]

5.1.5. Subscriber or User

One issue that has not attracted sufficient attention relates to the specification of the entity that has to be provided with the clear and comprehensive information and has to provide his consent. Article 5.3 requires that the *subscriber or user* concerned gives his consent. Should the choice be at the discretion of the entity that stores or gains access to the information? The Directive does not provide any clarification on this issue.

5.2. Transposition of Article 5.3 in the Member States

When looking at the way Article 5.3 has been transposed by the Member States, a first observation to make is that this provision has not been transposed by the German legislature. It has been considered in Germany that the existing rules of the "Telemediengesetz" relating to the processing of personal data by (information society) service providers are sufficient to protect users and subscribers.

Estonia has not transposed Article 5.3 of the ePrivacy Directive either, but apparently the government intends to do so. As of June 2014 the Estonian Ministry of Economic Affairs and Communications has begun the procedure to amend the Information Society Service Act. This amendment will transpose Article 5.3 of the ePrivacy Directive into the Estonian law.

All other Member States have transposed Article 5.3.[123] However, this does not mean that all Member States also transposed the 2009 amendment to this provision. The Czech legislation, for example, still maintains the 2002 version of Article 5.3, and consequently states:[124]

> "*Anybody wishing to use, or using, the electronic communications network for the storage of data or for gaining access to the data stored in the subscribers' or users' terminal equipment shall inform those subscribers or users beforehand in a provable manner about the extent and purpose of processing such data and shall offer them the option to refuse such processing. This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of message transmission via the*

[122] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories, v.3.4' (30.11.2006), p. 6.

[123] See also the overview provided at http://www.fieldfisher.com/pdf/cookie-consent-tracking-table.pdf

[124] A similar example is the legislation in Bulgaria.

electronic communications network, nor does it apply to the cases where such technical storage or access activities are needed for the provision of an information society service explicitly requested by the subscriber or user."

Many Member States have added some national flavour to Art. 5.3. A typical example is Section 55(5) of the Slovakian Electronic Communications Act:

"*Every person that stores or gains access to information stored in the terminal equipment of a user shall be authorised for that only if the user concerned has given his consent on the basis of clear and comprehensive information about the purpose of the processing; for this purpose the consent shall be also the use of a respective setting of the web browser or other computer programme. The obligation to gain the consent shall not apply to a body acting in criminal proceedings or other state body. This shall not prevent any technical storage of data or access thereof for the sole purpose of the conveyance or facilitation of the conveyance of a communication by means of a network or if it unconditionally necessary for the provider of an information society service to provide information society services if explicitly requested by the user*. "

The Slovak Republic thus inserts an exception for state bodies. Moreover it stipulates explicitly that "a respective setting of the web browser or of another computer programme" is equivalent to the expression of the user's consent. Similar additions can also be found in many other Member States. The Greek law, for instance, provides that consent can be given "*by means of appropriate settings in the web browser or by means of another application*". The Greek data protection authority has made it clear, however, that default settings to accept all cookies are not appropriate to indicate consent. The Irish data protection authority has made a similar remark, i.e. that the term 'appropriate browser settings' does not include default browser settings. Art. 22(2) of the Spanish Law on Information Society Services phrases the possibility of implicit 'browser consent' as "*where it is technically feasible and effective, the recipient's consent to accept the data processing may be granted by the use of the adequate settings of the browser or other applications*". This provision is taken from Recital (66) of the Citizens' Rights Directive.

In many Member States the introduction of the consent rule in 2009 is not reflected in the national provision(s) transposing article 5.3 ePrivacy Directive (see CY, EE, HR, HU, LV, MT, PT and SK). In several other Member States the competent supervisory authority has, however, issued detailed guidelines on how to approach consent in relation to cookies.

Recital (66) of the Citizens' Rights Directive stating that "where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application", has been integrated in the text of the law

by about ten Member States, including e.g. France, Ireland, Luxembourg, Greece, Poland, Slovakia, Slovenia, Spain and the UK. In other Member States such as Austria and Finland, Recital (66) of the Citizen's Rights Directive is referred to in guidance documents issued by national data protection commissioners.

Poland introduced a distinction between "information" (e.g. cookies) and "software (e.g. spyware). The difference mainly concerns the information to be given to the user. Consent is needed for both, although this consent can be deduced from browser settings in the case of "information".

The scope of application of the national provisions transposing Article 5.3 primarily depends on the legal framework in which the national legislature has transposed this provision. France, for example, inserted its cookie provision in the general data protection law (Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés). By so doing, the provision is automatically applicable to every controller or processor of personal data. Italy chose a similar approach, and transposed article 5.3 in art. 122 of the Data Protection Code. The German supposedly "equivalent" of Article 5.3 can be found in the "Telemediengesetz" which is, more or less, the German legal framework for information society services. Bulgaria transposed Art. 5.3 via the Electronic Commerce Act and thus restricted the scope of application of this provision to providers of information society services. In Poland the provisions of the Telecommunications Law with regard to confidentiality – including the Polish transposition of Art. 5.3 – have been transposed in the Telecommunications Act but made explicitly applicable to all "participants in telecommunications activities". Hungary transposed the provision of article 5.3 in two different legal instruments, namely the Electronic Communications Act and the E-Commerce Act, so that both electronic communications service providers as well as information society service providers need to adhere to the obligations of the cookie provision. The Croatian transposing provision has been included in the Electronic Communications Act, but the national regulatory authority HAKOM has specified that the rule applies to all domestic persons/bodies and not just operators. It is notable, however, that the Croatian legislature has not extended the scope of its national provision to include the amendment of Directive 2009/136/EC, meaning that USB keys, CD- and DVD-roms and the like are not covered since an electronic communications network needs to be involved.

Few legislators deemed it necessary to differentiate between different types of monitoring and analysis tools (e.g. different types of cookies or techniques) or different types of devices (e.g. mobile phones, laptops, etc.). One exception is the Dutch legislation, which explicitly provides that cookies meant to collect personal data of users for direct marketing purposes are subject to the rules of the (general) data protection legislation. This statement seems to be purely declarative, because it actually confirms a European legal rule. In other words, the principle, explicitly stated

by the Dutch legislature, is also valid in all other Member States. It means, for example, that the use of cookies for collecting personal data in view of direct marketing is subject to both the consent requirement of Art. 5.3 ePrivacy Directive and the applicable provisions of Directive 95/46/EC.

In the majority of the Member States the competent supervisory authorities have tried to remedy the lack of granularity by providing more detailed guidelines on how to apply the implementing legislation to different types of cookies. *Inter alia* the Greek, Spanish, Irish, Italian and Lithuanian data protection authorities all have a dedicated webpage with information on how to implement the legislation. The Italian DPA provides for example that the information consent rule requires a reasonably sized banner to be displayed on the screen when the user accesses a home page or any other page. It goes on by listing the types of information that should be included in this banner. The Irish Data Protection Commissioner has provided an example of a check box, which the user can tick in order to explicitly consent with the cookie being placed. An example is also given of a way to acquire implicit consent, by providing a box with a link to a cookie policy.

With regard to exceptions to consent, the Member States have transposed the ePrivacy Directive quite similarly, staying very close to the exceptions provided in Article 5.3.

5.3. Evaluation

Recital 17 of the 2002 ePrivacy Directive clarifies that the "consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website"[125]. In the context of Article 5.3 of the ePrivacy Directive one such method could be the provision of user consent via the configuration of browser settings:

> *[…] Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the* ***appropriate settings of a browser or other application****. […]*[126] (emphasis added).

It is true that the Article 29 Working Party was against the use of default browser settings as a means to provide prior consent, fearing that this could lead to "erosion of

[125] Recital 17 2002 ePrivacy Directive.
[126] Recital 66 Citizens' Rights Directive.

the definition of consent and […] subsequent lack of transparency"[127]. However, in a later opinion it examined the conditions under which the settings of a browser will comply with the Data Protection Directive and will constitute a valid consent.[128] Contrary to the statement of the thirteen Member States, which argued that the "amended Article 5.3 is not intended to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purpose"[129], the Article 29 Working Party found that the majority of default browser settings that are available today do not meet the consent requirements of Article 5.3 and that in any case browser settings will meet the requirements of the Data Protection Directive "in very limited circumstances"[130]. Other national authorities (UK ICO, Spanish DPA) have expressed the same views.

Both the Article 29 Working Party and the European Data Protection Supervisor have criticised the practices of obtaining consent of the user via use of a browser or similar application that "by default" enables the storing of or gaining access to information that is already stored in the terminal equipment of the user, such as in the case of cookies. Even when the user is informed about the option to reject cookies in the privacy policy of the website or the service, the Article 29 Working Party questions whether there is actual user awareness on how to configure the settings of their browser in order to reject cookies: "the responsibility for […] processing [of cookies] cannot be reduced to the responsibility of the user for taking or not taking certain precautions in his browser settings"[131]. The installation of and access to cookies that is done by default is based on lack of any action from the user and therefore should not

[127] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 1/2009 on the proposals amending Directive 2002/58 on privacy and electronic communications (e-Privacy Directive), WP159' (2009), p. 10

[128] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP 171' (2010), p. 13 ff.

[129] COUNCIL OF THE EUROPEAN UNION, 'Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1' , Brussels, 18.11.2009, as corrected by Council of the European Union, 'Corrigendum to the Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1 COR 1', Brussels, 19.11.2009.

[130] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2010 on online behavioural advertising, WP171' (2010), p. 13.

[131] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 1/2008 on data protection issues related to search engines, WP148' (2008), p. 20.

be rendered as valid consent, providing a clear and unambiguous indication of the user's wishes.

The Article 29 Working Party has therefore elaborated the conditions for browser settings to be able to deliver valid and effective consent in its Opinion 2/2010 and Working Document 02/2013.[132] Several major web browsers, often having a default setting to allow all kinds of cookies, do not currently fulfil these conditions. As a consequence – and this should preferably be clearly stated in a Recital of the ePrivacy Directive – only browsers or other applications which by default reject 3d party cookies and which require the user to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites are able to deliver valid and effective consent.

It is difficult to deny that the introduction of the consent rule in Art. 5.3 has not entirely reached its objective. This is largely due to the fact that users currently receive a warning message with regard to the use of cookies on almost every web site. Obviously the effect of such warning messages would substantially increase if they only appeared where a web site contained 3rd party cookies, cookies used for direct marketing purposes and, more generally, all cookies that are not related to the purpose for which the user is navigating on the site. This is without prejudice of including appropriate warnings and consent mechanisms whenever someone wants to access any privacy sensitive information (pictures, emails, contact lists) that users may have in their terminal equipment, via any mechanisms other than cookies.

Article 5.3 currently contains two exceptions where prior consent of the user is not needed: a) for the technical storage of the access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the access to information is strictly necessary for the provider. These exceptions should preferably receive a slightly broader formulation, for example, by deleting the condition stating that "the storing of or the access to information (should be) strictly necessary for the provider". In addition we recommend inserting additional exceptions, e.g. for cookies which are exclusively used for web site usage statistics. Finally we propose explicitly requesting specific, active and prior consent in all cases where cookies or similar techniques are used for direct marketing purposes.

Last but not least, while the current discussion mainly deals with the issue of *how* consent should be given and *how* the relevant information should be furnished to the user or the subscriber, it should also be examined *whether* the choice to make the ePrivacy Directive allow the use of cookies (and similar techniques) based only on the

[132] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Working Document 02/2013 providing guidance on obtaining consent for cookies'.

consent of the user or the subscriber is effective and logically plausible. Does the consent of the user justify unlimited tracking of that user's behaviour in the online environment, given the known weaknesses of consent as a mechanism for ensuring legitimacy? This question inevitably leads us to the issue of "profiling", currently under discussion in the framework of the proposed general Data Protection Regulation.

There are additional aspects of this issue which deserve further attention. The first of these issues is the territorial scope of application of Art. 5.3. Currently this scope is unclear. Under which conditions is this provision applicable to providers established outside the Union and how can this provision be enforced in such cases? Which national law is applicable inside the Union? Is, for example, the Belgian transposition of Art. 5.3 – Art. 129 of the Belgian Electronic Communications Act – applicable to all cookies stored on terminal equipment located on the Belgian territory? Or stored on terminal equipment used by persons with a residence in Belgium? Or should the location of the (establishment of the) service provider be taken into account? The most logical solution would probably be to bring the answer to this question in line with the general data protection framework.

A second additional issue relates to the use of new technologies which don't necessarily "store information or gain access to information already stored on the end-user's equipment", making use of Javascripts and browser fingerprinting. [133] A recent opinion of the Article 29 Working Party has, at least to a certain extent, clarified this question.[134]

[133] ECKERSLEY, Peter, How Unique is Your Web Browser?, Privacy Enhancing Technologies, Lecture Notes in Computer Science, Volume 6205, 2010, pp 1-18

[134] See Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, adopted on 25 November 2014.

6. Processing of Traffic and Location data

This Chapter deals with Articles 6 and 9 of the ePrivacy Directive. Like the previous chapters, it is again divided into three parts:

- Analysis of the relevant provisions of the ePrivacy Directive
- Transposition of these provisions in the Member States
- Evaluation, including suggestions and recommendations.

6.1. Analysis of relevant European provisions

6.1.1. Traffic data

Traffic data are "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".[135] They may include any translation of naming, numbering or addressing information by the network over which it is transmitted for the purpose of carrying out the transmission. The 2002 ePrivacy Directive specified that

> *[t]raffic 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.*[136]

Traffic data relating to subscribers and users that are processed and stored by a provider of a public communications network or service must, subject to certain exceptions, be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication.[137] However, certain data collected for the billing of subscribers and for interconnection payments may be processed up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.[138] The processing of stored traffic data must respect the principle of proportionality in relation to the processed data. Therefore, the processing of data must be limited to processing the necessary data and must be adequate, relevant and not excessive in relation to the purposes of billing and making interconnection

[135] Article 2(b) ePrivacy Directive.
[136] Recital 15 2002 ePrivacy Directive.
[137] Article 6(1) ePrivacy Directive.
[138] Article 6.2 ePrivacy Directive.

payments.[139] Although the ePrivacy Directive does not specify any time period in which traffic data may be lawfully stored, the Article 29 Working Party has indicated that a reasonable interpretation is that data may be stored for billing purposes for a maximum of three to six months, except if there is a dispute, in which case the data may be processed for a longer period.[140]

In derogation from Article 6 of the ePrivacy Directive, traffic data can be exceptionally retained for a limited period based on a specific legislative measure taken by the Member States. Such retention is only allowed when it

> *constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications.*[141]

Providers of publicly available electronic communications services may also process traffic data for the purpose of marketing electronic communications services, as well as for the provision of value-added services,[142] to the extent and for the duration that this is necessary for such services. This is allowed, provided that the subscriber or the user to whom the data relate has given his prior consent, which may be withdrawn at any time.[143] Compared to the Data Protection Directive, the specific provision of Article 6.3 of the ePrivacy Directive, by referring only to the prior consent of the subscriber or the user, imposes stricter rules for the processing of traffic data for the purpose of marketing electronic communications services, or for the provision of value-added services in the electronic communications sector. In practice it means that traffic data, unlike other categories of personal data, cannot be processed for direct marketing purposes on the basis of Art. 7(f) of Directive 95/46/EC.

Whenever processing of traffic data takes place for the purposes of subscriber billing and interconnection payments, the service provider must inform the subscriber or the user of both the types of traffic data that are being processed and the duration of the processing. When the processing of traffic data takes place for the marketing of electronic communications services of the provider or for the provision of value added services, then the service provider has to provide the aforementioned information prior to obtaining the consent. The processing of traffic data must be restricted to persons acting under the authority of the public electronic communications network

---

[139] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 1/2003 on the storage of traffic data for billing purposes, WP69' (2003), p. 6

[140] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 1/2003 on the storage of traffic data for billing purposes, WP69' (2003), p. 7.

[141] Article 15.1 ePrivacy Directive.

[142] Article 2(g) ePrivacy Directive defines "value added service" as "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof".

[143] Article 6.3 ePrivacy Directive.

and service providers and be limited to what is necessary for the purposes of billing or traffic management, customer inquiries, fraud detection, marketing electronic communications services or providing value-added services.[144]

6.1.2. Location data

6.1.2.1. Definition

The definition of location data was amended by the Citizens' Rights Directive. According to the new definition

> *"location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service"*[145]

The Council amended the definition in its common position in order to cover not only data that are processed in an electronic communications network, but also data processed by an electronic communications service.[146] Location data may, thus, refer to the geographic coordinates of the terminal equipment of a user, i.e. its latitude, longitude and altitude, to the identification of the network cell in which the terminal equipment is located at a given time, to the level of accuracy of the information that related to the location of the user, as well as to the time this information was recorded.[147]

The concept of location data is closely related to the one of traffic data, which is defined as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof"[148]. Traffic data refer, among others, to the location of the terminal equipment at the beginning and at the end of a communication[149] and therefore some traffic data are also location data. Similarly, location data that are processed for the purpose of the conveyance of an electronic communications network are also traffic data and should be processed in accordance with Article 6 of the ePrivacy Directive.

---

[144] Article 6.5 ePrivacy Directive.
[145] Article 2(c) ePrivacy Directive.
[146] COUNCIL OF THE EUROPEAN UNION, Common Position (EC) No 16/2009 adopted by the Council on 16 February 2009 with a view to the adoption of a Directive 2009/…/EC of the European Parliament and of the Council of … amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation protection laws [2009] OJ (05.05.2009), C103 E/40.
[147] Recital 14 2002 ePrivacy Directive.
[148] Article 2(b) ePrivacy Directive.
[149] Recital 15

6.1.2.2. Location data other than traffic data

Besides the location data that qualify also as traffic data and have to be processed in accordance with Article 6 of the ePrivacy Directive, there are location data that are "not processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof"[150]. These data are referred to in the ePrivacy Directive as "location data other than traffic data" and are processed for the provision of value added services[151] that are based on the location of the user. Such value added services are commonly known as location based services and cover for instance services that provide the users with traffic information or offer guidance to drivers[152], direct marketing services based on the location data of users, and tracking services for children or for elderly people.

Within the protective ambit of Article 9 of the ePrivacy Directive, location data other than traffic data relating to users or subscribers of public communications networks or publicly available electronic communications services that are used for the provision of a location based service, may be processed only when they are made *anonymous*, or when the users or subscribers have given their *consent* to the provision of such a location based service.[153] In any case, the location data may only be used to the extent and for the duration necessary for the provision of the value added service.[154] The users and the subscribers should be given the opportunity to withdraw their consent for the processing of the location data at any time[155]. The withdrawal will be valid for the future.

The ePrivacy Directive explicitly requires that the service provider must, before obtaining the consent, provide the individual with specific information regarding the type of location data that will be processed, of the purposes and the duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the location based service[156]. To the extent that location data are also personal data, the general information obligations that are foreseen in the Data Protection Directive are also applicable.

The Article 29 Working Party compiled a comprehensive list of the information that should be provided to the individuals before obtaining their consent for the

[150] Article 2(b) ePrivacy Directive.
[151] Value added services are defined in Article 2(g) of the ePrivacy Directive as "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof".
[152] Recital 35 2002 ePrivacy Directive.
[153] Article 9(1) ePrivacy Directive. A high-level description of the European framework on location based services can be found at HLADJK, Jorg, 'Location Based Services: European data protection rules for mobile commerce' (2009) 8 Privacy and Security Law Report, p. 24 ff.
[154] Article 9(1) ePrivacy Directive.
[155] Article 9(1) ePrivacy Directive.
[156] Article 9(1) ePrivacy Directive.

processing of their location data for the provision of a location based service, specifying the information that has to be provided to the individual concerned:

- *the identity of the controller and of his representative, if any;*
- *the purposes of processing;*
- *the type of location data processed;*
- *the duration of processing;*
- *whether the data will be transmitted to a third party for the purpose of providing the value-added service; the right of access to and the right to rectify the data;*
- *the right of users to withdraw their consent at any time or temporarily refuse the processing of such data, and the conditions on which this right may be exercised;*
- *the right to cancel the data.*[157]

The information should be given in a "clear, complete and comprehensive" way focusing on the features of the value added service.

A location based service, falling under the scope of Article 9 of the ePrivacy Directive, can either be provided directly by the electronic communications operator, or there may be third parties, besides the electronic communications operator, involved, who provide the service based on location information that they obtain from the operator. However, only one of the parties involved in the provision of the location based service should be responsible for offering the information relating to the processing of location data to the user or the subscriber: the one that determines the means and the purposes for the processing of the data and qualifies as data controller. In practice, this will be the party that is collecting the location data for processing, which in principle will be the provider of the location based service. When this party does not have a direct contact with the user or the subscriber, the information should be provided by the electronic communications operator.

The information can be provided in various ways. It can for instance be provided every time the service is used, or in the general terms and conditions for the location based service. In the latter case the service provider should make the information available so that the individuals concerned can consult it at any time and easily, such as via visiting a dedicated website or while using the service, by dialling, for instance, a toll-free number. It is debatable whether the information can be given in the general contract terms of the contract that is concluded between the subscriber and the

[157] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 4-5.

operator, if it is clearly highlighted as relating to the provision of the location based service.

The ePrivacy Directive requires the consent of the users or the subscribers for the processing of these data. Recital 35 of the Directive states that "[t]he processing of [location data other than traffic] data for value added services should only be allowed where subscribers have given their consent".[158] In many cases the subscriber to the service is also the user of the terminal equipment, for instance of the mobile device. In these cases no real practical difficulty arises, as the two roles, those of the user and the subscriber, coincide in one natural person. When both a user and a subscriber are involved in the processing of location data and these two attributes are allocated to different persons, questions arise as to whose consent needs to be obtained. The decision

> *[w]hether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.*[159]

In an attempt to shed light on the issue of whether it should be the user or the subscriber to offer his consent, the Article 29 Working Party has taken the position that when a location based service is offered to "private individuals, consent must be obtained from the person to whom the data refer, i.e. the user of the terminal equipment"[160]. Although this suggestion can be used as a general rule, when applying Article 9 of the ePrivacy Directive,[161] there are cases when the simple application of the aforementioned rule may be inefficient. The examples of localisation of minors and of employees for the provision of a value added service are representative of situations when the user and the subscriber can be different natural persons and will therefore be discussed below.

The consent can be given in the general terms and conditions for the location based service, in order to avoid the nuisance of consenting to each transmission of data for the purpose of providing the same value added service.[162] However, the Article 29

---

[158] Recital 35 2002 ePrivacy Directive.
[159] Recital 31 2002 ePrivacy Directive.
[160] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 7.
[161] The same is valid for Article 6 of the ePrivacy Directive.
[162] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §98, para. 12; OHLENBURG, Anna, 'Der neue Telekommunikationsdatenschutz - Eine Darstellung von Teil 7 Abschnitt 2 TKG' [2004] Multimedia und Recht (MMR), p. 436.

Working Party has taken the position that the consent for the processing of the location data other than traffic data for the provision of the location based service cannot be given as part of accepting the general terms and conditions for the electronic communications service that is offered.[163]

When the automatic localisation of the individual is required for the provision of a location based service, the initiation of the process by the individual would amount to consenting to being located, provided that he is fully provided with the aforementioned information relating to the processing of his location data.[164] For instance when an individual can dial a specific number or send an SMS to a dedicated number in order to get information on the weather conditions at his location, then the dialling of the number or the sending of the SMS should be considered as consent to the processing of his location data.[165]

The users and the subscribers should also be offered the choice to temporarily refuse the processing of their location data for each connection to the network or for each transmission of a communication, using simple means and free of charge.[166] This can for instance be done via a switch on/off option of the terminal equipment. The processing of location data may be undertaken only by persons acting under the authority of the network operator, the service provider or the third party providing the value added service and only for the purposes of providing the value added service.[167] When the location based service requires the localisation of the user on an ongoing basis, it suffices when the consent is provided once before the localisation takes place and after the individual concerned is duly informed about the details relating to it. In addition, the provider should send regularly reminders to the terminal equipment of the individual about the localisation.[168] However, the danger lurks that the use of the location based service may become cumbersome in case the users are sent notifications too frequently.[169] The German legislature has concretised the frequency of these reminders in relation to value added services that require the processing of other subscribers or third parties, besides the provider of the value added service. In these cases, the service provider has to inform the subscriber via an SMS about the number of the localisations he has realised after (at a maximum) the

[163] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 5.
[164] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 6.
[165] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 6.
[166] Article 9.2 ePrivacy Directive.
[167] Article 9.3 ePrivacy Directive.
[168] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 7.
[169] GADZHEVA, Maya, 'Privacy concerns pertaining to location-based services' [2007] International Journal of Intercultural Information Management (IJIIM), p. 53.

fifth localisation via the location data of the mobile device, unless the subscriber has objected.

An exception to the general rule of obtaining the consent of the subscriber or the user for the processing of location data (other than traffic data) exists in relation to emergency calls. National organisations handling emergency calls that are recognised as such are entitled to override the temporary denial or absence of consent of a subscriber or a user on a per-line basis for the purpose of responding to such calls.[170] This provision reflects the Universal Service Directive[171], which requires public telephone network operators to make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls made to the single European emergency call number "112".[172]

It has been pointed out by the Article 29 Working Party that, while the obligations relating to the processing of location data for the provision of value added services covers only mobile operators (or electronic communications operators in general), the third parties that are involved in the provision of a value added service on the basis of location data that they receive from the mobile operators are bound by the obligations arising from the Data Protection Directive.[173]

Although location data other than traffic data can be processed only for the duration necessary for the provision of the value added service, they can exceptionally be retained for a limited period based on a specific legislative measure taken by the Member States. Such retention is only allowed when it "*constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use the electronic communications".*[174]

The provisions in articles 6.1 and 9.1 of the ePrivacy Directive stipulate what the provider must do to be allowed to process traffic data or location data, especially in the event that the purpose of the legitimate processing no longer requires it. For

---

[170] Article 10(b) ePrivacy Directive. Specifying further the provision of Article 10 of the ePrivacy Directive, the Commission adopted a recommendation on the handling of location information of the caller for the purpose of location-enhanced emergency call services: COMMISSION OF THE EUROPEAN COMMUNITIES, Commission Recommendation of 25 July 2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services (2003/558/EC) [2003] OJ L108/49 (29.07.2003).

[171] EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 2002/22/EC of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services ("Universal Service Directive") [2002] OJ L108/51 (24.04.2002),

[172] Article 26 Universal Service Directive.

[173] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 4

[174] Article 15.1 ePrivacy Directive.

traffic data the provider must erase the data or must make it anonymous when it is no longer needed for the purpose of transmission, unless he can invoke exceptions (e.g. billing, interconnection payments, or retention obligations) which in turn will have specific erasure/anonymisation requirements. Location data should only be processed anonymously, unless the user or subscriber consents to the processing. Processing should only be allowed for the legitimate purpose of service provision, after which the data need to be deleted. Again there are exceptions, such as the one in article 15.1 ePrivacy Directive regarding their retention in national law.

6.2. Transposition in the Member States

The provisions relating to the processing of traffic and location data have been transposed in all Member States, and in all Member States the transposing measures are more or less consistent with the text of the Directive.

Some of the national legislators have added details to the provisions of the ePrivacy Directive. This is, for example, the case of the UK where the legislation has a more detailed definition of "location data". The Privacy and Electronic Communications (EC Directive) Regulations define location data as

> "*any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—*
>
> *(f) the latitude, longitude or altitude of the terminal equipment;*
>
> *(g) the direction of travel of the user; or*
>
> *(h) the time the location information was recorded."*

The Greek legislature has introduced a very detailed definition of traffic data, which defines it as "*data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data may, inter alia, consist of the number, the address or the identity of the connection or the terminal equipment of the subscriber and/or user, the passwords, location data, the date and time of beginning and end and duration of a communication, the volume of transferred data, information about the protocol, the formatting, the routing of the communication, as well as the network from which the communication originates or terminates in*". What is quite striking here, is that the Greek definition considers passwords to be traffic data. In Spain, on the other hand, traffic data is simply not defined, while the Estonian legislature has defined neither traffic nor location data.

Croatia deserves special mention here, not so much because of its definitions of traffic or location data, but because it has taken the concept of value added services out of its national framework and replaced it with special tariff services. Special tariff services are defined as "*services provided via public communications networks and services by means of special numbers or special codes from the 'Numbering Plan' or the 'Addressing Plan', for the purpose of realisation of predetermined additional contents and/or services within these contents outside the scope of public communications*".

Some Member States have more detailed rules on the processing of traffic or location data. By way of example, one can refer to the Finnish provision relating to the processing of traffic data for invoicing purposes:

> *Billing-related data must be stored for a minimum of three months from the due date of the bill or the saving of the identification data, whichever is later. Such data must not, however, be stored beyond the time the debt becomes statute-barred under the Act on statute-barred debt (728/2003). However, in the case of a dispute over a bill, the data pertaining to that bill must be stored until the matter has been settled or resolved.*

The Austrian legislature introduced a similarly detailed provision relating to the processing of traffic data for billing purposes. But where the Finnish legislature requires data to be stored for a *minimum* of three months, the Austrian legislature allows the data to be stored for a *maximum* of three months, a period which can be extended when the bill is challenged, the bill was not paid or dispute proceedings are on-going. Bulgaria also has some very specific exceptions in which traffic and location data can be processed, e.g. for detecting, locating and eliminating defects and software errors or detecting and tracing nuisance calls. The traffic data should – when no other legal ground for processing them is available - be deleted or anonymised as soon as the call or connection ends, unless they are needed for the immediate establishment of a new call or connection. The Greek requirements for processing traffic and location data even include the express obligation on operators and providers of electronic communications systems to uphold the data minimisation principle when designing and selecting technical means and information systems. The Czech transposition of article 15.1 ePrivacy Directive also stands out, because it interprets abuse of electronic communications services as encompassing consistent late payment of bills. It implies that providers are allowed to share customer information with one another on 'bad' clients.

In contrast to Article 9 of the ePrivacy Directive there are no specific provisions on location data other than traffic data in the French law. The processing of location data will fall under the provisions of the Postal and Electronic Communications Code when they qualify as traffic data and are processed by electronic communications operators

(and other entities subject to art. L34.1) and under the Data Protection Act whenever they qualify as personal data.

Where data is processed in accordance with Section 6 of the Swedish Electronic Communications act, the provider must inform the user of the type of traffic data and for how long the data will be processed. This information must be provided before consent is obtained. On this point the Swedish law goes further than the Directive because prior consent must be obtained not only for marketing and other services (Article 6.3 of the Directive) but also for billing and payment purposes (Article 6.2 of the Directive). The Czech correspondent noted in this regard that users who ask providers to be informed of the traffic data relating to them being kept, may be asked to pay for this information. The pricing policies in this regard, however, are extensive. It is also interesting to note that the Hungarian transposition of article 9 of the ePrivacy Directive does not include the possibility for withdrawing consent temporarily, as provided for in article 9.2.

According to Paragraph 98 of the German Telecommunications Act, the processing of location data for the provision of a value added service should rely on the consent of the subscriber, unless the data are made anonymous.[175] In case the location data are used for the provision of a value added service, which relies on the conveyance of location data of a mobile device to other subscribers or to third parties, who are not providers of the value added service, the subscriber has to give his explicit, separate and written consent.[176] This choice of the German legislature to base the processing of location data other than traffic data for the provision of value added services on the consent of the subscriber is in line with Recital 35 of the 2002 ePrivacy Directive, which actually requires the consent of the subscriber for the processing of the data. When the device is used by more people (*Mitbenutzer*), the subscriber has to inform them[177] about the provided consent and avoid in this way the unwanted disclosure of their location data. In simple words, the subscriber will have to inform the user, when this is a different person, about the consent that is provided for the processing of the location data. However, this requirement does not have an impact on the service provider, for whom the consent of the subscriber suffices for the processing of the location data.[178]

Regulation 14 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) in the UK refers to the consent of the user or the subscriber to whom the data relate. However there is no further clarification either in the Regulations or by

[175] Section 98(1) German Telecommunications Act.
[176] Section 98(1) second sentence German Telecommunications Act.
[177] The term "Mitbenutzer" is not defined in the German Telecommunications Act.
[178] ECKHARDT, Jens, 'Zehnter Teil. Telekommunikationsgesetz (TKG)' in SPINDLER, Gerald and SCHUSTER, Fabian (eds), *Recht der elektronischen Medien* (Verlag C.H. Beck, München 2008), §98 para. 13.

the U.K. ICO on who should be the one to provide his consent, the user or the subscriber, when it is not clear to the provider that these are two distinct entities.[179]

The Danish correspondent highlights that the exceptions to the erasure or anonymisation of traffic and location data have been included in the Administration of Justice Act, which goes even further than the Data Retention Directive the legitimacy of which has recently been successfully challenged before the European Court of Justice.

Last but not least in many Member States the retention of traffic and location data for law enforcement purposes has become uncertain as a consequence of the European Court of Justice's jurisprudence on the Data Retention Directive (CZ, DK, ES, PT, RO and SV). Other reasons for less effective deletion/anonymisation rules include the fact that the obligations are aimed solely at operators and electronic communications service providers which means that (new) information society services remain outside the scope, that there are multiple supervisory authorities competent and the introduction of specific legislation with additional exceptions (see e.g. FI with the so-called "Lex Nokia"). Finally, it is notable that in Latvia the provision on deletion of traffic data has been taken out of the law, although location data still needs to be anonymized.

6.3. Evaluation

Although Article 6 of the ePrivacy Directive seems to be more or less correctly transposed by a majority of the Member States, there are serious problems with regard to the compliance of some of its provisions which leaves doubts as to whether it achieves the purposes sought by the law.

Most problematic is Art. 6.3 which stipulates:

> "*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 or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.*"

[179] The U.K. ICO refers to "the consent of the user or subscriber" in its Guidance on PECR and does not provide any further clarification on the discussed issue: UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories, v.3.4' (30.11.2006).

In practice some mobile operators merely mention the possibility of processing user and traffic data in the general terms and conditions, without further information. Some of these terms and conditions grant the operator a right to process the data for a duration of two years after the end of the contract.[180]

The provisions with regard to location data are frequently criticised. The ePrivacy Directive regulates only a fraction of location based services and namely those that rely on the processing of location data other than traffic data offered via a public communications network or in a publicly available electronic communications service.[181]

In its Opinion 13/2011 dealing with geolocation services on smart mobile devices the Article 29 Working Party, referring to the definition of "electronic communications service" in Art. 2, c) of the Framework Directive, clearly stated that "the ePrivacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network" (p. 9).

Consequently, following this interpretation, all location data processed by information society services are outside the scope of the Directive. This seems difficult to justify because in practice users are nowadays primarily confronted with the processing of location data in the context of such services, in particular provided via mobile apps.

In addition, location based services that are offered to members of a private network are neither governed by the provisions of Article 9 of the ePrivacy Directive. For example Article 9 does not cover location data that are transmitted via enterprise networks aimed for a private user group, or data collected and transmitted via infrared signals or GPS signals in combination with a private secured wireless LAN.[182]

In line with our proposed amendment to Article 3 of the ePrivacy Directive it is sufficient to slightly modify the wording of these Articles in order to make them applicable to all services provided via public or publicly available private communications networks that collect and further process traffic and location data. As a result, the processing of location data by information society services will be subject to the application of Art. 6 and Art. 9.

Users and/or subscribers might further experience difficulties in specifying the data controller, i.e. the party that is responsible for the provision of information to the data

[180] This has for example been reported by the Belgian consumers organisation "Test-Achats" in a report of October 2014, summarised in their magazine "Budget & Droit", January-February 2014, p. 10-11.
[181] Article 9(1) ePrivacy Directive.
[182] STEIDLE, Roland, 'Datenschutz bei Nutzung von Location Based Services im Unternehmen' [2009] Multimedia und Recht (MMR), p. 168.

subject and to whom the data subjects can turn in order to exercise their rights. These difficulties however do not relate only to the processing of location data for value added services. The problem of defining the controller of the data in new telecommunications networks has already been identified by the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data of the Council of Europe:

> *Nowadays […] this model in which a sole person or body is responsible for determining the parameters of the automatic processing is increasingly challenged by examples to the contrary. Several actors, among which the controller or co-controllers, the processor(s) and the service provider(s) interact in the processing. As a result, data subjects might not always know whom to turn to in order to exercise their rights.*[183]

The Consultative Committee, realising the difficulties in the attribution of responsibility, when various entities are involved in the processing of the personal data, suggested that it is up to the entities involved "to clarify among themselves who is responsible for what, taking account of legal criteria. Otherwise they might be held jointly responsible for any damage".

In the context of the provision of information to the individual before obtaining his consent, a possible suggestion could be that, when there are various parties involved in the provision of the location based service, besides the electronic communications operator, the information should in principle be offered by the party that is collecting the location information for the processing, i.e. by the provider of the location based service. Similarly, the same party should be the one to obtain the consent of the individual concerned.

In the majority of the current commercial systems of location based services, the electronic communications operator systematically sends location data of the individual concerned to the providers of value added service upon their request for the provision of the service, except when this information is automatically created by the terminal equipment of the user. The Article 29 Working Party expressed doubts about these current practices which allow for the identification of the user by the location based service provider, while this is not necessary for the successful provision of the service. Therefore it suggested that the electronic communications operators should transfer the localisation requests to the third party, the provider of the location based service, in a way that will not allow the identification of the individual

[183] COUNCIL OF EUROPE - CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD), 'Opinion of the T-PD on the interpretation of the concepts of automatic processing and controller of the file in the context of worldwide telecommunications networks (T-PD-BUR (2006) 08 E fin)' (15.03.2007), p. 4.

by the third party.[184] In such a case, the consent of the individual should be collected by the electronic communications operator, as the individual will remain anonymous to the provider of the location based service.

The nature of location based services implies a lack of direct communication between the individual who requests the service on the one hand, and the providers of the publicly available electronic communications service and the provider of the location based service on the other. Therefore it is important that the provider of the location based service (or the electronic communications service provider, when this entity is defined as data controller), takes measures in order to ensure that the location data that are going to be processed belong to the same person who is consenting to the processing. To this end, the provider should confirm the subscription to the location based service after the receipt of the consent. This can for instance be realised via sending an SMS to the terminal equipment of the user. If necessary, the provider should request a further confirmation of the subscription.[185] The Citizens' Rights Directive recognised that the consent of the user, when this is technically feasible and effective, can be expressed via the configuration of the appropriate settings of an application.[186] Although this clarification was made in the context of Article 5.3, which has been presented above, it could be applied in the context of location based services as well.

A special kind of location based services, the so-called passive location based services, raise questions with regard to the provision of consent of the localised individual. Passive location based services are defined "as those services where a mobile phone user, once he has enabled the service, consents to be located by another, when that other person initiates a location request either from another mobile phone or from a PC"[187]. Very popular passive location based services are the services that allow the parents to track their children (*child location services*). Two fundamental problems arise with regard to such services: whether both the parent and the child should consent to the processing of the location data and at what age a child is capable of giving his consent to his localisation for such a purpose There is currently no harmonisation among the European Member States with regard to the age when a minor becomes competent to consent to the processing of his personal data.

[184] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 6.
[185] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 7.
[186] Recital 66 Citizens' Rights Directive.
[187] 'Industry Code of Practice for the use of mobile phone technology to provide passive location services in the UK (v1.1)' (2006), p. 3.

In an attempt to deal with the former issue, several mobile network operators and location service providers developed a Code of Practice for the use of passive location services in the UK.[188] According to the Code of Practice,

> *"if the locatee is under 16, the parent or guardian must give consent to the child signing up to the location service. In addition, the child should also consent. If the child does not consent, his or her wishes must not be overridden and the service must not be activated. In the event that the child does not have the capacity to give consent, the consent of the parent will suffice"*[189].

It goes without saying that the service providers have to introduce appropriate procedures in order to ensure the identity of the people that register are parents or guardians of a child and prevent anyone else from having access to the service.[190] It has already been stipulated above that the consent should be obtained by the person to whom the personal data relate. Within an employment context, it may, however, be argued that in some cases the employer (*subscriber*) has a legitimate interest in making use of location based services that may involve the localisation of employees (*users*) during their working hours. This can for instance be the case for the owner of a delivery company who has a legitimate interest in knowing where a company vehicle is and whether the planned schedule is carefully followed. However, the location information of the company vehicle will reveal location data of its driver. Notwithstanding the eventual legitimate interest of the employer, the right of the employee to his private life should not be underestimated and therefore there should be some safeguards in place in cases of localisation of an employee.[191]

The validity of the consent that is provided by the employee within an employment context has already been questioned and should not be relied upon for the processing of location data of the employee. The Article 29 Working Party suggested as a potential solution the collection of the consent statements of the employees via collective agreements.[192] In any case, the employer should make sure that the processing of the location data corresponds to a well specified purpose that cannot be reached by other means less intrusive to the privacy of the employee, in full respect of the proportionality principle. In such cases, the consent of both the employer and the

---

[188] 'Industry Code of Practice for the use of mobile phone technology to provide passive location services in the UK (v1.1)' (2006).

[189] 'Industry Code of Practice for the use of mobile phone technology to provide passive location services in the UK (v1.1)'(2006), p. 7-8.

[190] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 9.

[191] The location data can refer directly to the location of the employee or can be construed indirectly, for instance via the location of a vehicle that he is authorised to use, or an asset that is in his charge: ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 9.

[192] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 10.

employee should be obtained and the localisation should only cover the working hours of the employee. The obtaining of the consent of employees is also suggested by the U.K. Industry Code of Practice on passive location based services.[193] When the equipment that allows the localisation of the employees is available to them also for private use, then it should be equipped with a system that will allow them to easily deactivate the localisation functionality outside their working hours.[194]

Our conclusions with regard to the provisions of Articles 6 and 9 of the ePrivacy Directive are as follows:

- The current definition of "traffic data" seems to be broad enough and probably does not need to be changed. Art. 6.1, however, currently refers only to "traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available communications service (…)". In line with our proposed amendment of Article 3 of the ePrivacy Directive we recommend modifying Art. 6(1) and Art. 9(1) in order to make the rules on the processing of traffic and location data applicable to all services provided via public or publicly available private communications networks that collect and further process traffic and location data. As a result, the processing of location data by information society services will be subject to the application of Art. 6 and Art. 9. Moreover the wider scope of the provisions of Articles 6 and 9 will also necessitate a revision of the definitions of the terms "user" (in Art. 2(a) of the ePrivacy Directive) and "subscriber" (in Art. 2(k) of the Framework Directive), if these terms are used in the context of the ePrivacy Directive.

- Although the provisions examined in this Chapter have been more or less correctly transposed by a majority of the Member States,

- the actual processing of traffic and location data in Member States should be closely monitored in order to ensure that European legal rules in this domain are correctly complied with.[195]

- The solution for determining the applicable law as well as the competent supervisory authority should be brought into line with the solution adopted in the general data protection framework. This step should ideally be coordinated with the discussion on the proposed Data Protection Regulation.

---

[193] 'Industry Code of Practice for the use of mobile phone technology to provide passive location services in the UK (v1.1)' (2006), p. 15.

[194] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion on the use of location data with a view to providing value added services, WP115' (2005), p. 10.

[195] Some Member States, e.g. Sweden and Belgium, have already started or announced projects in order to obtain a better insight in the way traffic data are processed by network and service providers in practice.

7. Unsolicited Direct Marketing Communications

This Chapter is dedicated to the rules relating to unsolicited commercial communications. It starts with an analysis of the relevant provisions of the ePrivacy Directive. The following parts of the Chapter will provide a summary of our survey in the Member States with regard to the transposition of the European provisions and a short evaluation of the current European legal framework on this issue.

7.1. Article 13 of the Directive

The sending of unsolicited commercial communications by e-mail became commonly known as "spam".[196] The impact of such unsolicited communications on privacy and consumer protection, on the protection of minors and human dignity, as well as on the economic burden caused to business and lost productivity brought the issue of combating spam to the top of the European agenda.[197]

[196] COMMISSION OF THE EUROPEAN COMMUNITIES, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam'' COM(2004) 28 final, 22.01.2004, p. 3..

[197] See among others: COMMISSION OF THE EUROPEAN COMMUNITIES, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam'' COM(2004) 28 final, 22.01.2004; COMMISSION OF THE EUROPEAN COMMUNITIES, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Fighting spam, spyware and malicious software' COM(2006) 688 final, 15.11.2006. The European Commission procured in 2009 a study on the actions taken at national level from the Member States on the combating of spam, as well as spyware and malicious software: time.lex Law Offices, 'Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software (Study procured by the European Commission, SMART 2008/ 0013)' (2009). Besides the provisions about unsolicited communications for direct marketing purposes in relation to the privacy of the citizens, the European Commission has introduced a number of other provisions that can be applicable to such communications, such as: EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 2006/114/EC of 12 December 2006 concerning misleading and comparative advertising (codified version) [2006] OJ L376/21 (27.12.2006), which repealed the older 84/450/EEC Council Directive on misleading advertising (COUNCIL OF THE EUROPEAN COMMUNITIES, Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising [1984] OJ L250/17 (19.09.1984), EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") [2000] OJ L178/01 (17.07.2000), EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts (Distance Selling Directive) [1997] OJ L144/19 (04.06.1997), as modified.

7.1.1. The Baseline of Article 13(1)

Article 13(1) of the ePrivacy Directive regulates the use of specific electronic means for direct marketing purposes, as follows:

> *The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.*[198]

Similar to many other provisions of the ePrivacy Directive confusion exists as to whether or not this provision is applicable to messages sent by means of information society services, in particular via so-called "webmail" or via social media platforms such as Facebook, Twitter, etc. One of the reasons for this confusion is the fact that neither the Art. 29 Working Party nor the EDPS have ever issued a clear opinion on this topic. Because the scope of application of the ePrivacy Directive specifies that its provisions apply to electronic communications services, the Article 29 Working Party concluded in an Opinion of 2004 that Article 13(1) applies exclusively to "messages by electronic communications".[199] Following this interpretation the provision is not applicable to messages exchanged via information society services. This viewpoint is in line with the viewpoint of the Article 29 Working Party with regard to the scope of Art. 9 of the Directive. In its Opinion 13/2011 dealing with geolocation services on smart mobile devices the Article 29 Working Party, referring to the definition of "electronic communications service" in Art. 2, c) of the Framework Directive, clearly stated that "the ePrivacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network" (p. 9). Also in more recent opinions the Article 29 Working Party seems to confirm that Art. 13(1), like all other provisions of the Directive, covers only these techniques which can be considered as electronic communications, with the exclusion of information society services.[200]

On the other hand there seems to be a consensus about the fact that Article 13(1) is applicable to *any entity* that sends unsolicited communications via electronic communications. Art. 13(1) doesn't prohibit only unsolicited direct marketing messages sent by providers of electronic communications services but is applicable to anyone who sends unsolicited direct marketing messages via electronic communications.[201] Not only the Article 29 Working Party but also the EDPS have

[198] Article 13(1) ePrivacy Directive.

[199] ARTICLE 29 WORKING PARTY, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, p. 4

[200] ARTICLE 29 WORKING PARTY, 'Opinion 1/2008 on data protection issues related to search engines, WP148' (2008), p. 12.

[201] ARTICLE 29 WORKING PARTY, Opinion 1/2008, oc., p. 12: "Search engines therefore fall outside of the scope of the definition of electronic communication services. A search engine provider

confirmed this viewpoint.[202] The fact that not only electronic communications service providers are submitted to the prohibition to use e-mail for direct marketing purposes without prior consent, but virtually anyone using electronic communications, doesn't however mean that Article 13(1) is applicable to messages exchanged via information society services.[203]

The above interpretation with regard to the scope of Art. 13(1) should normally lead to the conclusion that prior consent of the user is not required for direct marketing messages sent via a webmail platform or via social media. In practice, however, as we will further describe, the provision of Art. 13(1) has received sometimes a broader interpretation including also "webmail" exchanged via the web sites of information society service providers. One can therefore only conclude that the interpretation on this aspect of the scope of Art. 13(1) is currently very ambiguous.

Fortunately there is less uncertainty with regard other aspects related to the scope of this provision. Based on Recital 30 of the Data Protection Directive, the Article 29 Working Party came to the conclusion that the concept of direct marketing should cover "any form of sales promotion, including direct marketing by charities and political organisations (e.g. fund raising, etc.)"[204].

The ePrivacy Directive further refers to the "use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail".[205] The common characteristic of these methods is that they are relatively easy and cheap to send, while they may impose a burden or even a cost to the recipient.[206] Besides the nuisance caused to the recipients, in cases when such unsolicited commercial communication is sent in bulk, it can also cause problems for both the electronic communications networks and the terminal equipment of the recipients.[207] Especially with regard to terminal equipment with limited storage capacity, such as mobile phones, the volume of unsolicited communications sent to the device can cause significant disruption to its functionality.

---

can however offer an additional service that falls under the scope of an electronic communications service such as a publicly accessible email service which would be subject to ePrivacy Directive 2002/58/EC and Data Retention Directive 2006/24/EC".

[202] EUROPEAN DATA PROTECTION SUPERVISOR, Second opinion on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), adopted on 9 January 2009 [2009] OJ C128/28 (06.06.2009), para. 27.

[203] This confusion has apparenty led to a note of the Ombudsmen of Sweden, Denmark and Norway sent to the Commission in 2012 about individual Facebook messages. See http://www.pcworld.com/article/2016581/scandinavia-cracks-down-on-facebooks-unsolicited-ads.html

[204] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 7.

[205] Article 13(1) ePrivacy Directive.

[206] Recital 40 2002 ePrivacy Directive.

[207] Recital 40 2002 ePrivacy Directive.

The reference to automatic calling and communications systems clearly leaves direct marketing methods that involve in person communication out of the scope of this provision, such as in the case of telemarketing. Such methods will be discussed separately below. The addition of "communication" systems, as suggested by the Article 29 Working Party in order to "maintain a technology neutral approach whilst taking into account on-going technological changes"[208], aimed at covering Bluetooth marketing applications.[209]

"Electronic mail" is defined in the ePrivacy Directive as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient"[210]. The definition of electronic mail refers to a public communications network and therefore excludes any text, voice, sound or image that is sent over a private communications network or in any case over a network that is not public. Under the concept of electronic mail one should include also SMS, MMS and other similar applications.[211] Moreover it requires that the "message" can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient. For instance, the definition covers messages left on answering machines, voice mail service systems and newsletters sent by e-mail.[212]

The definition of electronic mail excludes any message that requires the simultaneous participation of the sender and the recipient.[213] The transmission of a Bluetooth message requires a simultaneous communication between two Bluetooth enabled devices. Moreover, messages sent via Bluetooth cannot be stored on any network or in the recipient's terminal equipment until they are collected by the recipient (contrary to conventional electronic mail).[214] Therefore, such messages cannot be

---

[208] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), WP150' (2008), p. 5.

[209] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 1/2009 on the proposals amending Directive 2002/58 on privacy and electronic communications (e-Privacy Directive), WP159' (2009), p. 9.

[210] Article 2(h) ePrivacy Directive.

[211] Recital 40 ePrivacy Directive and Recital 67 Citizens' Rights Directive. Increasing technological progress and the decreasing cost of transmitting messages enabled the spread of unsolicited communications in new ways, such as via fax, SMS or MMS. These developments were taken into account by European legislator during the drafting of the ePrivacy directive (referring to fax and SMS) and were further expanded to cover MMS and "any other kinds of similar applications" via the Citizens' Rights Directive.

[212] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 4.

[213] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 4.

[214] In the case of Bluetooth, a network is created using a wireless Bluetooth connection, commonly known as *piconet*. In this kind of network, one device provides the synchronisation reference and is known as the *master*. All other devices are known as *slaves* (SEYS, Stefaan,

considered as electronic mail, in accordance with the definition of the ePrivacy Directive.

Realising the limitations arising from the wording of Article 2(h) of the 2002 ePrivacy Directive, the addition of "communication systems" in Article 13(1) aimed at subsuming Bluetooth messages with advertising content under the requirement for prior consent. The Article 29 Working Party found that:

> *This [i.e. the use of the word "communication" and the new Recital referring to "similar technologies"] ensures that prior consent is required in Bluetooth marketing applications, thus taking into account the observations made by the Working Party in its Opinion 2/2008 on the "need to protect users of short range wireless media against unsolicited communication as defined in Article 13". An explicit reference to Bluetooth and similar technologies could also be included in Recital 40.*[215]

Bluetooth messages would not need to qualify as electronic mail anymore, but can be considered as sent via an automated communications system.

If a message cannot be stored in the network or in the terminal equipment of the recipient, until it is collected by him, then this message does not fall under the scope of application of Article 13(1) of the ePrivacy Directive. Conventional e-mail is exchanged between e-mailservers. The messages are sent via the outgoing mailserver of the sender, transmitted over the network and stored on the incoming mailserver used by the recipient.[216]

It may be questioned whether the scope of Art. 13(1) is restricted to e-mail messages accessed by means of a dedicated e-mail client software programme or includes also e-mail accessed via a webmail service.[217] One could argue that in both cases the messages are transmitted via an electronic communications network (the internet) and an electronic communications service (provided by the ISP). On top of this the information society service provider puts a web application to facilitate the e-mail management for the end-user. [218]

SINGELÉE, Dave and PRENEEL, Bart, 'Security in Wireless PAN Mesh Networks' in Hu, H., Zhang, Y. and Zheng, J. (eds), *Security in Wireless Mesh Networks* (Auerbach Publications, 2008), pp. 349-381). In simple words, Bluetooth technology enables the creation of an ad hoc network between the transmitting device and the Bluetooth enabled receiving device of the user (MARCHINI, Renzo and TEBBUTT, Kate, "Bluespam: Is it legal?" [2007] BNA International - World Data Protection Report).

[215] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 1/2009 on the proposals amending Directive 2002/58 on privacy and electronic communications (e-Privacy Directive), WP159' (2009), p. 9.

[216] http://computer.howstuffworks.com/e-mail-messaging/email.htm

[217] http://www.quora.com/How-webmail-works.

[218] The Article 29 Working Party stated: "A search engine provider can however offer an additional service that falls under the scope of an electronic communications service such as a

Therefore one could disagree with the opinion that Art. 13 does not apply as soon as the recipient makes use of an information society service to access her or his mailbox. Messages are nowadays exchanged via all kinds of online platforms, such as LinkedIn, Facebook or Twitter. Because they are sent over a public communications network and stored on the server of the platform provider – which is "in the network" – one could argue that such messages have to be considered as e-mail following the definition of Art. 2(h) of the Directive.

Article 13(1) is only applicable if e-mail is "used for the purpose of direct marketing". It is irrelevant whether the direct marketing message is part of the message body or attached in a separate document. However direct marketing should be the primary purpose. This is the reason why, for example, a newsletter or a magazine, sent as an attachment to a conventional e-mail will not fall under the scope of Art. 13(1), as long as the newsletter or magazine is primarily sent for a different purpose, other than merely direct marketing.

7.1.2. Recipients of Unsolicited Communications

The Citizens' Rights Directive broadened the protective ambit of Article 13(1) of the ePrivacy Directive in order to cover not only subscribers, but also users. It should be reminded that the ePrivacy Directive defines users as "any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service."[219]

In contrast, the term subscriber is not defined in the ePrivacy Directive. Instead, the definition of subscriber contained in the Framework Directive is applicable, according to which a subscriber is "any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services."[220] According to this definition, the basic prerequisite for somebody to be classified as a subscriber is that the person has a contract with a provider of a publicly available electronic communications service, who will then actually offer the service. It is specified that the subscribers under this provision are natural persons, while Member States can broaden its scope in order to cover legal persons as well, if this is required for the latter's legitimate interests to be sufficiently protected.[221]

7.1.3. Consent

publicly accessible email service which would be subject to ePrivacy Directive 2002/58/EC and Data Retention Directive 2006/24/EC". See Opinion 1/2008 on data protection issues related to search engines, p. 12.

[219] Article 2(a) ePrivacy Directive.

[220] Article 2(k) Framework Directive.

[221] Article 13.5 ePrivacy Directive.

The use of the systems and techniques mentioned in Article 13(1) for direct marketing purposes is allowed only after the prior consent of the users and subscribers involved. The requirement for prior consent lays down a general "opt-in" rule for the sending out of direct marketing messages via automatic calling systems, fax, e-mail, SMS, MMS or any similar methods. Consent can be given by any appropriate method, as long as it corresponds to the definition of consent contained in the Data Protection Directive.[222] The Article 29 Working Party clearly excludes consent to be derived from sheer inaction of the recipient, by the installation of pre-ticked boxes on a website, for instance that by default allow the sending of unsolicited communications. This explains why the agreement of a social media platform user with the terms and conditions published by the platform provider, will not be considered as a valid consent as requested by Art. 13(1). In other words, the agreement of a user with the terms and conditions of Twitter or Facebook doesn't mean that this user does consent to receive direct marketing messages from advertisers via these platforms.

A valid consent cannot be obtained via a general e-mail sent to prospective recipients of unsolicited communications for direct marketing, requesting their consent to receive such communications.[223] It goes without saying that arbitrary collection of e-mail addresses or other information that falls under the scope of Article 13(1) with automatic means that do not involve the consent of the person concerned, such as the automatic harvesting of personal data from public internet places via software programs, and their use for unsolicited communications for direct marketing is not permitted.[224]

7.1.4. Exception for Existing Customer Relationship

7.1.4.1. Article 13(2) of the Directive

The ePrivacy Directive provides for derogation from the consent requirement covering situations when there is an existing customer relation for the sending of unsolicited communications for direct marketing purposes:

---

[222] Article 2(f) ePrivacy Directive specifies that the consent of the user or the subscriber in the frame of the ePrivacy Directive corresponds to the consent of the data subject, as defined in the Data protection Directive.

[223] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 5.

[224] ASSCHER, Lodewijk F. and HOOGCARSPEL, Sjo Anne, *Regulating Spam: A European perspective after the adoption of the E-Privacy Directive* (Information Technology & Law Series, TMC Asser Press, The Hague 2006, p. 69 ff. CHENG, Tania, 'Recent international attempts to can spam' (2004) 20 Computer Law and Security Report, p. 477, implies that address harvesting should not be allowed under the U.K. legislation. In any case, such harvesting of personal data is not allowed under the Data Protection Directive, as it does not respect the finality principle and it does not provide the individuals concerned with the information that is required under that Directive: ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90'(2004), p. 6.

where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.[225]

I.e. , if a person or a company receives electronic mail contact details from its own customers (whether they be natural or legal persons) in the context of the sale of a product or a service, then direct marketing for its own similar products or services is allowed unless the customer explicitly opts out. This exception is also known as "soft opt-in".[226] The use of the term "soft opt-in" is used due to the fact that the customer has already given his electronic mail contact details to the sender in the context of a customer relation. However the term can be criticised, as the customers are given the opportunity to object to receiving direct marketing communications and they do not express in any way their agreement to receive such communications.

7.1.4.2. Conditions for the application of the exception

The exception is applicable when the sender, who can be either a natural or a legal person, obtains from its customers their electronic contact details for electronic mail in the context of the sale of a product or a service. However, even when the aforementioned conditions are fulfilled, the sender who has obtained electronic contact details for electronic mail from its customers cannot use it as he wishes, but only within the clearly defined frame provided for in Article 13(2) of the ePrivacy Directive. The sender can use electronic contact details for electronic mail only for direct marketing of its own similar products and services and on the condition that the customer has already been provided with the option to object to such use at the time of the collection of his details, free of charge and in an easy way.

The exception for existing customers covers only direct marketing that is based on the use of electronic contact details for electronic mail. According to the definition of

[225] Article 13(2) ePrivacy Directive.

[226] See among others: DONOVAN, Colleen, 'Implementation of the e-Privacy Directive in the UK - Understanding the new rules' (2004) 20 Computer Law and Security Report, p. 128; UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 16.

electronic mail, which was discussed above, these contact details can refer for instance to the e-mail address of the customer or his SMS details.[227]

It is interesting to mention that in the UK, although charity organisations and political parties are covered by the obligation to obtain prior consent before sending unsolicited communications, they cannot make use of the existing customer exception, on the argumentation that the ePrivacy Directive has restrained it to purely commercial relationships.[228] Moreover, in case the customer has not initially refused such use at the time of collection of his electronic contact details, although he is given the right to object, he should be given this opportunity each time he receives a message. This provision establishes a right to object to the use of the electronic contact details of a customer, instead of the stricter requirement for prior consent, which is applicable when there is no existing customer relationship between the sender and the recipient of the message. Given that Article 13(2) requires a right to object and lays down an exception from the requirement for prior consent stipulated in the first paragraph, it should be carefully examined, as it lowers the standards for user protection.

7.1.4.3. In the context of a sale of a product

The collection of the e-mail address or the mobile phone number of the customer has to be obtained in the context of a sale of a product or a service. How broad is the scope of this exception for existing customers? Does it only cover customers who have purchased a product or a service? Could somebody who expressed interest in a product be contacted based on this exception, without having given his prior consent, although he did not complete the transaction? The term "sale" replaced the term "purchase" that was included in an early draft version of Article 13(2) in the 2002 ePrivacy Directive.[229] The European Parliament considered that the use of the term "sale" instead of "purchase" would provide additional safeguards to the protection of citizens. The new wording would prevent senders from claiming that "although no sale took place, a consumer could be included under the 'opt-out' regime as they had

[227] FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING (FEDMA), 'European Code of Practice for the use of personal data in direct marketing - Electronic Communications Annex' (2010), p. 4.

[228] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 31.

[229] The term "purchase" was replaced by the term "sale" during the Second Reading of the European Parliament: European Parliament, European Parliament legislative resolution on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (15396/2/2001 - C5-0035/2002 2000/0189(COD)) [P5_TA(2002)0261] - Second reading [2003] OJ C187E/103 (07.08.2003), Article 13(2).

expressed an interest in purchasing a product."[230] Therefore, the exception should only cover customers who have completed a sale, while potential customers should be contacted after they have provided their prior consent, in accordance with Article 13(1).[231]

7.1.4.4. Similar products or services

The limitation to send direct marketing messages only for their own similar products or services is challenging to interpret. On the one hand the Directive refers to the sender's "own" similar products or services, while on the other it restricts the existing customer exception to "similar" products or services. With regard to the reference to the sender's "own" similar products or services, subsidiaries or mother companies should not be understood as the same company.[232] The term "similar products or services" is difficult to specify and the relevant products or services should be examined on a case-by-case basis. In general, the issue whether the products or services are similar with the ones that established the customer relationship between the sender and the recipient, should be approached in an objective way, examining the reasonable expectations of the recipients and not focus on the perspective of the sender.[233] FEDMA, the Federation of European Direct and Interactive Marketing, in its code of conduct for online marketing[234], set the additional requirement that the customer has to be informed at the time of collection of his personal data what is meant under "similar goods and services" for the sender.[235]

---

[230] MAGEE, John, 'The law regulating unsolicited commercial e-mail: an international perspective' (2003) 19 Santa Clara Computer & High Technology Law Journal, p. 372.

[231] ASSCHER, Lodewijk F. and HOOGCARSPEL, Sjo Anne, *Regulating Spam: A European perspective after the adoption of the E-Privacy Directive* (Information Technology & Law Series, TMC Asser Press, The Hague 2006, p. 48.

[232] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 9; Federation of European Direct and Interactive Marketing (FEDMA), 'European Code of Practice for the use of personal data in direct marketing - Electronic Communications Annex' (2010), p. 4.

[233] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 9; UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 17-18.

[234] The Article 29 Working Party closely examined the FEDMA Code of Conduct for the use of personal data in direct marketing using electronic communications means and approved it as being compliant to both the Data Protection Directive and the ePrivacy Directive: ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP174)' (2010).

[235] FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING (FEDMA), 'European Code of Practice for the use of personal data in direct marketing - Electronic Communications Annex' (2010), p. 4.

7.1.4.5. Chance to object

The customer should be given the opportunity to object at the time of collection of his e-mail address. In case he does not refuse the use of his contact details, he should be given this opportunity on the occasion of every message he is receiving. He should be offered the means to express his objection free of charge and in an easy manner, at least by using the same communication method. In the context of e-mails or internet websites, the opportunity to object can be provided via an "unsubscribe" option.[236] With regard to direct marketing sent via SMS, it has been rendered that it is sufficient for the recipient to send an SMS to a dedicated number in order to indicate his objection to receiving an SMS with direct marketing content.[237] Although the UK ICO initially required a postal or e-mail address to be provided for the exercise of the right to object, they accepted the use of short codes under the conditions that the sender is clearly identified in the message, that the use of the short code does not incur a premium rate charge and that the provided short code is valid.[238]

7.1.5. Unsolicited Communications Via Other Means

Unsolicited communications for direct marketing can of course be sent using other means than those mentioned in paragraph 1 of Article 13; telemarketing, for instance[239], which involves in- person communication and is therefore left outside the scope of Article 13(1). Such telemarketing calls can be made either to a fixed line or to a mobile phone number. The ePrivacy Directive does not leave these cases completely unregulated. It rather requires that such unsolicited communications for direct marketing are not allowed either (a) without the consent of the subscribers or users concerned or (b) in respect of subscribers or users who do not wish to receive these communications.[240] This rule applies to natural persons, but the Member States can expand its protection to also cover legal persons, so that their legitimate interests are sufficiently protected.[241]

---

[236] JAY, Rosemary, *Data Protection Law and Practice* (3rd edn Sweet & Maxwell London 2007, para. 22-47.

[237] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 6; UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 18-19; JAY, Rosemary, *Data Protection Law and Practice* (3rd edn Sweet & Maxwell London 2007, para. 22-47.

[238] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', pp. 18-19.

[239] Recital 42 of the 2002 ePrivacy Directive refers to "person-to-person voice telephony calls".

[240] Article 13.3 ePrivacy Directive.

[241] Article 13.5 ePrivacy Directive.

The advancements of technology create new ways for delivering advertising messages, such as pop-up windows with advertising content. Soon after the adoption of the 2002 ePrivacy Directive, the Commission was confronted with the question whether direct marketing via pop-up windows has to rely on prior consent of the recipient. The Commission found that "Messages that depend on the addressee being on-line and that disappear when this is not the case, are not covered by the definition of electronic mail"[242]. Therefore they should be treated under Article 13(3) that leaves the choice for their regulation to the Member States.

The ePrivacy Directive leaves it up to the Member States to choose between either requiring the prior consent of the subscribers or the users on the one hand, or giving the opportunity to subscribers or users to express their wish not to receive such communications. In the example of telemarketing, besides the explicit objection of a user to a telemarketing call, the latter choice offered by the Directive can be realised via the establishment of preference lists and have to be consulted by the senders of unsolicited communications for direct marketing before they send it.

7.1.6. Disguising or Concealing the Identity of the Sender

The practice of sending electronic mail for the purposes of direct marketing, which disguise or conceal the identity of the sender on whose behalf the communication is made, which do not fulfil the information requirements that are laid down in the eCommerce Directive for information society services, which do not have a valid address to which the recipient may send a request that such communications cease, or finally which encourage recipients to visit malicious websites, is prohibited.[243]

The amendments introduced to the ePrivacy Directive during the 2009 review expanded the protection offered to consumers in the 2002 ePrivacy Directive, by ensuring protection not only against unsolicited commercial communications, but also against scam e-mails and links to phishing websites sent via email. Crucial for the legitimacy of the electronic mail that is sent for direct marketing is that it complies with the informational requirements that are established in Article 6 of the eCommerce Directive and that it does not encourage the recipients to visit websites that contravene these requirements. Article 6 specifies the information as follows:

> *(a) the commercial communication shall be clearly identifiable as such;*
> *(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;*
> *(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly*

[242] EUROPEAN PARLIAMENT, Written questions with answers: E-3392/02 by Astrid THORS to the Commission / Subject: Unsolicited advertising in Windows, protection of personal data in telecommunications networks [2003] OJ C155E/148 (03.07.2003)
[243] Article 13.4 ePrivacy Directive.

identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously".

7.1.6.1. Article 13.6 of the Directive

Besides the expansion of Article 13 to scam e-mails and links to phishing websites, the 2009 review of the ePrivacy Directive introduced a right for any individual or legal person, affected by spam, as well as email service providers and other service providers, to initiate legal action against spammers.[244] The economic impact of unsolicited communications, especially the vast amount of messages sent via email, is potentially immense. Therefore, the ePrivacy Directive, via Art. 4, implicitly creates an obligation for electronic communications service providers to make investments in order to protect users against spam. Member States may also take specific measures against or impose penalties on providers of electronic communications services, who by their negligence contribute to infringements of national legislation regulating unsolicited marketing communications.[245]

7.2. Transposition in the Member States

One of the first observations resulting from our survey in the Member States is that Article 13 of the ePrivacy Directive has been transposed by a variety of legal frameworks. The UK transposed Article 13 via electronic communications legislation. France used a mix of electronic communications legislation and consumer law. Poland relied on a mixture of electronic communications law and e-commerce legislation. Belgium transposed via e-commerce legislation. Germany used unfair competition law, while Sweden used its general market practices legislation.

This variation was also reflected in the remainder of the Member States. While many Member States (AT, BG, CY, EE, EL, ES, FI, HR, HU, IE, LT, LU, MT, NL, PT, RO, SI, SK) transposed the provisions of Article 13 using electronic privacy legislation, several of these (EE, ES, HR, HU, LT, MT, RO, SK) also used other legislation for part of the transposition, or relied on other legislation to determine key concepts (particularly EE and LT, where reference is made to concepts such as consent set out in national data protection law). Several Member States relied on a combination of electronic privacy and electronic commerce/information society legislation (ES, HR, HU, MT, RO, SK).

[244] Recital 68, Citizens' Rights Directive.
[245] Article 13(6) ePrivacy Directive.

Two Member States relied solely on electronic commerce/information society legislation to transpose Article 13 (CZ, LV), while Italy relied solely on data protection legislation. Denmark relied on market practices legislation to transpose the provisions.

While most Member States have transposed the "own customer" exception for e-mail under Article 13(2) of the Directive, an issue arises in Poland whereby the exception may be inferred from data protection legislation.

The Directive leaves discretion to Member States as to the treatment of "other forms of direct marketing" such as person-to-person telephony. Germany, for example, has opted for opt-in consent (this is only for consumers; opt-out consent applies to "other market players"). In relation to the remainder of the Member States, opt-out is the norm, with only AT, BG, DE, HU, TV and SI (and in some circumstance IE) having chosen an opt-in regime. In Ireland, there is an opt-out for person-to-person telephony, except in respect of calls to mobile phones, which are opt-in. In Ireland, there is also an exception for emails sent to email addresses of natural persons reasonably believed to be business or professional addresses.

In relation to protection afforded to legal persons, none of the six Member States subjected to in-depth analysis have extended the opt-in consent to them. However, several Member States do extend the opt-in consent that is afforded to natural persons (e.g. BG, CY, CZ, DK, EL, ES, FI, HU, IT, MT, NL). While France provides that communications can be made to legal persons unless they opt-out, the legislation specifies that these communications must relate to the professional activity carried out by the recipient. In IE, there is an opt-out, except in respect of communications made to mobile phones, which are subject to an opt-in regime. In other Member States, there does not seem to be any specific provisions protecting legal persons (AT, LU, SI, SK). In Latvia and Poland, protection is afforded to natural persons via general data protection law, but legal persons do not qualify for protection under these provisions. In Romania, opt-in consent is provided in respect of communications to legal persons. However, the relevant competent authority refuses competence in relation thereto, leading to a de facto lack of protection. In Sweden, legal persons are protected via industry standards; legal persons (as well as consumers) can report those companies which do not follow these standards.

Article 13 of the ePrivacy Directive is entitled "unsolicited communications". Notwithstanding the importance of the term for the transposition and the further implementation of the relevant provisions of Article 13[246], the term is not defined in the Directive. In an attempt to clarify the range of activities that are to be understood

[246] ASSCHER and HOOGCARSPEL highlight that "unsolicited seems to be the keyword of any method to describer, to prevent and to fight spam": ASSCHER, Lodewijk F. and HOOGCARSPEL, Sjo Anne, *Regulating Spam: A European perspective after the adoption of the E-Privacy Directive* (Information Technology & Law Series, TMC Asser Press, The Hague 2006, p. 10.)

by this term the UK ICO described an "unsolicited marketing message that a subscriber has opted into receiving" as one that they have not invited but they have indicated that they do not, for the time being, object to receiving it.[247]

Noteworthy in this context is the rule adopted by the Austrian legislator. Section 107 paragraph 2 prohibits the sending – irrespective of the technology used - of messages without consent not only if they are sent for direct marketing purposes but also if they are sent to more than fifty recipients.

The UK legislator defined direct marketing as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals."[248] However, the UK ICO adopted a broad understanding of the concept of direct marketing, covering "the promotion of an organisation's aims and ideas [such as] a charity or a political party making an appeal for funds or support."[249] The UK Tribunal dealt with the question whether the automatic call made by a political party should be covered by the provisions on direct marketing.[250] Interestingly, both parties made reference to the European Directives to strengthen their argumentation. The political party –among others– focused its argumentation on the fact that the Recitals of the ePrivacy Directive make specific reference to "unsolicited commercial communications" and to the customer relation between the sender and the recipient and claimed that the scope of the 2002 Privacy Directive does not extend to direct marketing by political parties.[251] On the contrary, the Information Commissioner made reference to Recital 30 of the Data Protection Directive, which explicitly referred to charity organisations and political parties in relation to marketing purposes.[252] The UK Information Tribunal confirmed this broad interpretation of "direct marketing" and concluded that "not for profit organisations such as political parties"[253] are not

[247] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 5.
[248] Section 11(3) of the U.K. Data Protection Act.
[249] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, v3.1' (08.10.2007), p. 3.
[250] *Scottish National Party v the Information Commissioner* (Appeal Number: EA/2005/0021), U.K. Information Tribunal
[251] *Scottish National Party v the Information Commissioner* (Appeal Number: EA/2005/0021), U.K. Information Tribunal, para. 58, referring to Recitals 40, 41 2002 ePrivacy Directive.
[252] Recital 30 Data Protection Directive: "[…] Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons".
[253] *Scottish National Party v the Information Commissioner* (Appeal Number: EA/2005/0021), U.K. Information Tribunal, para. 98.

excluded for the provisions relating unsolicited communications for direct marketing, as direct marketing is not an intrinsically commercial concept.[254]

Although the ePrivacy Directive does not explicitly refer to the period of time throughout which the consent can be considered as valid, it can be supported that the concept of consent implies that the reasonable expectations of the recipient should be crucial in determining the time validity of the given consent.[255] This aspect has been specified in UK legislation, which stipulates that the subscriber or the recipient consents *for the time being* to such communications.[256] It has been supported that the phrase "for the time being" implies that the given consent should not be indefinitely valid.[257] However, this position is not endorsed by the UK ICO, who clearly stated that they "do not interpret the phrase 'for the time being' as meaning that consent must inevitably lapse after a certain period."[258] It has further been supported in the literature that this phrase "makes explicit that contributors are always able to change their minds and therefore neither consent nor an objection is an eternal choice."[259] It is interesting to mention that although the German legislation does not make any explicit reference to the time validity of consent, the German Courts have ruled that given consent is not indefinitely valid. The District Court (*Landgericht – LG*) of Berlin ruled for instance that the sending of a commercial e-mail two years after the consent

[254] *Scottish National Party v the Information Commissioner* (Appeal Number: EA/2005/0021), U.K. Information Tribunal, para. 71, part of the contentions of the Information Commissioner.

[255] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 6.

[256] The limitation "for the time being" is present in relation to direct marketing via automated calling systems (Regulation 19), via fax (Regulation 20), via unsolicited calls (Regulation 21), via electronic mail (Regulation 22) and in relation to the preference lists for direct marketing via fax (Regulation 25) and unsolicited calls (Regulation 26).

[257] MUNIR, Abu Bakar, 'Unsolicited commercial email: implementing the EU Directive' (2004) 10 Computer and Telecommunications Law Review, p. 107.

[258] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 6.

[259] JAY, Rosemary, *Data Protection Law and Practice* (3rd edn Sweet & Maxwell London 2007, para. 22-36. The U.K. ICO mentions as examples that would indicate that the consent is still valid or not the following: "it will remain valid until there is good reason to consider it is no longer valid, for example, where it has been specifically withdrawn or it is otherwise clear that the recipient no longer wants to receive such messages. The initial consent will remain valid where there are good grounds for believing that the recipient remains happy to receive the marketing communications in question, for example, where the recipient has responded **positively** (that is, other than to object) to previous, reasonably recent marketing emails.": UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 6.

was given could not be based on that consent, as there was no communication between the sender and the recipient during that time.[260]

The German legislator did not regulate the issue of unsolicited communications in the Telecommunications Act, but rather included it in Section 7 of the German Unfair Competition Act.[261] The Act offers equal protection to both natural and legal persons and requires the "prior explicit consent" (*vorherige ausdrückliche Einwilligung*) of the recipient before the sending of "unacceptable nuisances" (*unzumutbare Belästigungen*)[262], specified as advertising (*Werbung*) via automatic calling systems, fax machines or electronic mail (including SMS and MMS). The Act differentiates between consumers and market participants.[263] It is questionable what can qualify as advertising in the context of this provision. Should a newsletter or a greeting card be considered as advertising? The answer will probably depend on the context of the message: if it relates to offers relating to a product or a service, it falls under the concept of advertising and the consent of the recipient has to be obtained. [264]

Contrary to the Directive and the implementing legislation in e.g. the UK, the Cypriot legislator has included a detailed definition of direct mail into its transposing legislation. 'Direct mail' has been defined as "*the dispatch of material consisting solely of advertising or marketing material and comprising an identical message, except for the addressee's name, address and identifying number as well as other modifications which do not alter the nature of the message, which is sent to a significant number of addressees, to be conveyed and delivered at the address indicated by the sender on the item itself or on its wrapping.*"

The Danish transposition of unsolicited communications has not been included in the Act on Electronic Communications and Services but in the Marketing Practices Act. The consequence is that the obligations regarding unsolicited communications are aimed at the broad category of 'traders'. Hungary has used three different legal instruments to transpose the provisions regarding unsolicited marketing, leading to unnecessary complications. Poland offers protection to natural persons against unsolicited communications via its general data protection legislation, but this means that legal persons are not entitled to it since they are not covered by the latter legislation. It is also interesting to note that the Polish correspondent has indicated

[260] LG Berlin, *Beschluss* vom 2.7.2004 - 15 O 653/03 (rechtskräftig), Multimedia und Recht (MMR) 2004, p. 688.
[261] Gesetz gegen den unlauteren Wettbewerb (UWG) vom 3. juli 2004 (BGBl. I 2004, S. 1414) [German Unfair Competition Act]
[262] The German Unfair Competition Act does not refer to "unsolicited communications", but to "unacceptable nuances".
[263] Market participant is defined "as any person, besides competitors and consumers, who acts as provider or buyer of goods or services: Section 2((1)(3) German Unfair Competition Act.
[264] ARNING, Marian and HAAG, Nils, 'Datenschutz' in HEIDRICH, J., FORGÓ, N. and FELDMANN, T. (eds), *Heise Online-Recht – Ein Leitfaden für Praktiker & Juristen* (2nd Ergänzungslieferung edn, Heise, Hannover 2010), Volume 2, Chapter C II, para. 107.

that, while in principle the 'own customer'-exception could have been inferred from data protection legislation, consistent interpretation of the law would not allow it. Indeed, data protection legislation is considered *lex generalis* vis-à-vis the law governing services by electronic means (*lex specialis*). Since the latter does not contain the exception, the more general law cannot add it, meaning that for own customers opt-in is required.

Ireland is noteworthy with regard to the national approach towards different technologies covered by Art. 13. The legislator has chosen an opt-out system for person-to-person telephony, but not where it concerns mobile phones, because in the latter case opt-in is required. Also peculiar is the exception for emails which were sent to email addresses of natural persons reasonably believed to be business or professional addresses.

The UK has broadened the scope of the Art. 13.2 exception regulating that the existing customer exception applies when the sender has "obtained the contact details of the recipient of that electronic mail in the course of the sale *or negotiations for the sale* of a product or service to that recipient"[265] (emphasis added). The UK ICO reaffirmed this approach recognising that the sale does not need to be completed.[266] However, the reference to negotiation for sale remains rather broad and unclear.[267] At which point does an individual enter into "negotiation for the sale"? In any case, it is questionable whether this derogation is compatible with the spirit of the ePrivacy Directive.

In the *Payback* decision the German Federal Court of Justice[268] examined the issue of consent and the way it should be given for direct marketing via post on the one hand and via e-mail or SMS on the other. The Court specified the conditions under which a consent clause for marketing and market research purposes can be validly given with regard to the sending of advertisements via electronic mail or SMS. The sending of advertisements via e-mail and SMS is regulated by Section 7(2)(3) of the German Unfair Competition Act and not by data protection legislation.

The German Unfair Competition Act specified that direct marketing activities making use of automatic calling machines, facsimile machines or electronic mail are considered to be unacceptable nuisances, unless the recipients have given their prior explicit consent.[269] This rule applies not only to consumers, but also to market participants. The Court in the *Payback* decision focused on the fact that the German

[265] Regulation 22(3)(2) PERC.
[266] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 17.
[267] ROGERS, Kevin, 'Viagra, viruses and virgins: A pan-Atlantic comparative analysis on the vanquishing of spam' (2006) 22 Computer Law and Security Report, p. 232.
[268] BUNDESGERICHTSHOF (BGH - GERMAN FEDERAL COURT OF JUSTICE), Decision of 16 July 2008, Az: VIII ZR 348/06 ("Payback"), MMR 2008, p. 731.
[269] Section 7(2)(3) of the German Unfair Competition Act.

Unfair Competition Act does not simply make reference to the consent of the recipients but requires their "prior explicit consent". Therefore, the Court considered that consent clauses that are formed in such a way that the customers have to act and tick a box, when they do not want to give their consent for the sending of advertising via electronic mail ("opt-out" statement), are not in line Section 7(2)(3) of the German Unfair Competition Act.[270]

Moreover, the Court concluded on this point that contrary to the provision of Section 4a(1) fourth sentence of the German Data Protection Act, the provision of consent for the sending of advertising via electronic mail or SMS cannot be given together with other declarations.[271]

The rules on unsolicited communications for direct marketing were transposed in the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Regulation 19 deals with the use of automated calling systems, Regulation 20 with the use of facsimile machines and Regulation 22 with the use of electronic mail for direct marketing purposes. The sending of unsolicited communications for direct marketing purposes via the use of automated calling systems[272] or electronic mail (including SMS and MMS) is not allowed, unless the subscriber[273], in the cases where automated calling systems are used, or the recipient, in the case of electronic mail, has consented for the time being to the sending of such communications.[274] These provisions cover both natural and legal persons. In relation to the use of facsimile machines, PECR differentiates between individuals[275](natural persons) and corporate subscribers[276] (legal persons). In relation to individual subscribers, the sending of unsolicited

[270] BUNDESGERICHTSHOF (BGH - German Federal Court of Justice), Decision of 16 July 2008, Az: VIII ZR 348/06 ("Payback"), MMR 2008, p. 734.
[271] BUNDESGERICHTSHOF (BGH - German Federal Court of Justice), Decision of 16 July 2008, Az: VIII ZR 348/06 ("Payback"), MMR 2008, p. 734.
[272] An automated calling system is "a system which is capable of (a) automatically initiating a sequence of calls to more than one destination in accordance with instructions stored in that system; and (b) transmitting sounds which are not live speech for reception by persons at some or all of the destinations so called": Regulation 19(4) PECR.
[273] A "subscriber" is defined as "a person who is a party to a contract with a provider of public electronic communications services for the supply of such services": Regulation 2(1) PECR. The term subscriber covers both "the legal being who enters into the contract to pay for the services" and the "person whose name is on the bill and who signed the original agreement": JAY, Rosemary, *Data Protection Law and Practice* (3rd edn Sweet & Maxwell London 2007), para. 22-22.
[274] Regulations 19(1), 19(2) and 22(1), 22(2) PECR.
[275] An "individual" is "a living individual and includes an unincorporated body of such individuals": Regulation 2(1) PECR.
[276] A "corporate subscriber" is defined as "a subscriber who is (a) a company within the meaning of section 735.1 of the Companies Act 1985.2; (b) a company incorporated in pursuance of a royal charter or letters patent; (c) a partnership in Scotland; (d) a corporation sole; or (e) any other body corporate or entity which is a legal person distinct from its members": Regulation 2(1) PECR.

communications for direct marketing purposes via faxes is not allowed unless they have consented to the sending of such communications[277]; while for corporate subscribers it is allowed, unless they have previously notified the caller that such communications should not be sent on that line.[278] However, the sending of unsolicited communications for direct marketing purposes via faxes is not permitted when the subscribers and the called line are included in the relevant registries[279] that have to be consulted by the senders prior to sending of any unsolicited communication for direct marketing purposes by means of facsimile machines.[280]

It is clear that the concept of consent is understood in a "flexible" way in the United Kingdom. The Courts seem more eager to accept implied consent as a valid form of expressing consent. Does this approach extend also to consent for direct marketing? In the context of direct marketing via electronic means it is broadly accepted in the UK that the recipient has to do "something from which the marketer is able to infer consent to the marketing."[281] With regard to consent that is given online some kind of clear action has to be taken. For instance, it can be the ticking of a box, the clicking of an icon or the sending of an e-mail. But would the failure to register an objection, i.e. not ticking a box that indicated the objection of the user to receive direct marketing (commonly known as "opt-out"), be sufficient to provide legitimate ground for the sending of unsolicited communications via electronic means?

The UK ICO has in principle rejected the option that the failure to register an objection would constitute valid consent. However, they purport that "in context, failing to indicate objection may be **part of** the mechanism whereby a person indicates consent"[282], claiming that when the sender has clearly given the opportunity to the potential recipient to object to receiving unsolicited communications and the latter does not make use of this option, then the consent can be implied. In the following example, the ICO found that the consent can be implied and used for the sending of direct marketing via electronic mail:

---

[277] Regulation 20(1)(a) PECR.
[278] Regulation 20(1)(b) PECR.
[279] Regulation 20(1)(c) PECR.
[280] Regulation 25 PECR foresees the maintenance of a preference list for unsolicited communications for direct marketing via fax. This list, commonly known as FPS (Fax Preference Service) is maintained by OFCOM, the Independent regulator and competition authority for the UK communications industries.
[281] JAY, Rosemary, *Data Protection Law and Practice* (3rd edn Sweet & Maxwell London 2007), para. 22-35.
[282] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 5.

*"For example, 'By submitting this registration form, you will be indicating your consent to receiving email marketing messages from us **unless** you have indicated an objection to receiving such messages by ticking the above box.'"*[283]

It is surprising that while the UK ICO found that "[b]y itself, failing to register an objection will be unlikely to constitute valid consent"[284], the placement of a clear statement in a registration form, as the one presented above, would put the failing to register an objection in such context that would indicate consent and render it as sufficient ground for the sending of direct marketing communications.

It is important to keep in mind at this point that although Article 13 does not foresee any additional information to be provided to the prospective recipient, the information obligations of the data controller that are stipulated in the Data Protection Directive cover the sender of unsolicited communications in order to obtain a valid consent. Mobile marketing entails an intrinsic character limitation (usually limited to 160 characters). In such cases, the recipient can be provided with a short notice containing the essential information, along with a reference to a website or to another source, where he can access all the information in detail.[285] Technical solutions have also been promoted as adequate to address the space limitation that arises with regard to mobile devices.[286] Notwithstanding the importance of such initiatives, it remains outside the scope of this report to examine technical solutions.

According to the information obligations of the data controllers, they have to provide the data subject with information relating to the recipients or the categories of recipients of the data.[287] The Article 29 Working Party specified this requirement in the context of Article 13, requiring from a sender of direct marketing who intends to disclose to third parties the contact information of the recipients of his direct marketing communications, to acquire the recipient's consent for that purpose.[288] It

---

[283] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 5.

[284] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 5.

[285] FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING (FEDMA), 'European Code of Practice for the use of personal data in direct marketing - Electronic Communications Annex' (2010), p. 5.

[286] P3P (Platform of Privacy Preferences) has been presented as such a potential solution in order to provide the required information to the mobile users via the privacy policy of the website (http://www.w3.org/P3P/, last accessed on 17/11/2014)), see: CLIFF, Evelyne Beatrix, 'Implementing the legal criteria of meaningful consent in the concept of mobile advertising' (2007) 23 Computer Law and Security Report, p. 266 ff. P

[287] Article 10(c) Data Protection Directive.

[288] ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP90' (2004), p. 5.

can be seen as surprising that the UK has adopted a rather lenient position on how such consent for transmission to third parties can be obtained. A sender can, for instance, pose a general question to his recipients of direct marketing communications asking "We would like to pass your details on to specially selected third parties so that they can send you more information about holidays in America. Do you agree to this?"[289]. A positive answer from the recipients "is likely to be sufficient to allow third parties to use those contact details for promoting holidays in America by electronic mail"[290]. It is questionable if such an approach could, however, be justified in the light of the Data Protection Directive and whether this would fulfil the specificity requirement for the provision of valid consent.

7.3. Evaluation

In general, Member States have adequately transposed the provisions of Article 13(1) of the Directive. Thus, they have introduced national provisions ensuring that the use of automated calling and communication systems without human intervention, fax and email for direct marketing is prohibited, unless prior consent has been obtained (opt-in). They have also provided for the exception (Art 13.2 of the Directive) in the context of "own customers", whereby opt-out consent is sufficient.

The Directive leaves some discretion to Member States in relation to "other forms of direct marketing", such as person-to-person voice telephony. As they are relatively more costly for direct marketers, Member States are free to choose an opt-in or opt-out consent regime. Some Member States have chosen opt-in, and others opt-out.

In relation to communications made to subscribers who are legal persons, the Directive stops short of specifying what rules should be put in place at Member State level, but provides the broad requirement that the legitimate interests of such subscribers be "sufficiently protected". In general, one of three approaches was adopted in each Member State: opt-in, opt-out, or no protection for legal persons.

An important issue is the type of legislation used. Many Member States have transposed the provisions of Article 13 using ePrivacy or electronic communications legislation, while others have done so with information society/e-commerce rules. Some have relied on general data protection law. Some have implemented provisions using specific direct marketing or advertising law, grafting the ePrivacy provisions onto

[289] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 23.
[290] UK INFORMATION COMMISSIONER'S OFFICE (ICO), 'Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by electronic means (v3.1/08.10.2007)', p. 23.

existing legislation. This presents difficulties both in terms of scope (e.g. whether the application of national rules on direct marketing are limited to communications arising in connection with the "provision of publicly available electronic communications services in public communications networks" or whether they extend to communications which are normally considered to be information society services such as social media), but also enforcement (often competences are split across two or more competent authorities.

The term "electronic mail" – being defined in Art. 2(h) of the ePrivacy Directive as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient" – is generally interpreted as being restricted to e-mail via electronic communications and not applicable to messages exchanged via information society services such as Facebook, LinkedIn, Skype or Twitter, even when the transmission of such messages ultimately occurs over the internet and thus makes use of publicly available electronic communications services provided on public electronic communications networks. This restrictive interpretation seems also be the one adopted by the Article 29 Working Party.

Our main recommendation with regard to Art. 13 is therefore to bring the scope in line with our proposed amendment to Art. 3 so that Art. 13(1) also becomes applicable to messages transmitted via information society services such as Facebook, LinkedIn, Skype or Twitter. This extension of the scope of Art. 13(1) should however not lead to the prohibition without the prior consent of the user of all kinds of online advertising. the definition of "e-mail" in Art. 2(h) of the Directive should be amended as follows: "any electronic message addressed to one or more identified recipients, sent over a public communications network, and which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient."

Article 13(1) would of course only be applicable if e-mail is "used for the purpose of direct marketing". It is irrelevant whether the direct marketing message is part of the message body or attached in a separate document. However direct marketing should be the primary purpose. This is the reason why, for example, a newsletter or a magazine, sent as an attachment to an e-mail will not fall under the scope of Art. 13(1), as long as the newsletter or magazine is primarily sent for a different purpose, other than direct marketing.

In practice, Art. 13(3) is applicable to communications which cannot be stored in the network or in the recipient's terminal equipment until it is collected by the recipient. This addresses primarily direct marketing voice calls to fixed or mobile phones would remain under the scope of Art. 13(3), at least as long as the call is not recorded and stored (as in the case of voice mail). Although such calls, in particular to mobile phones, are often perceived as very intrusive, we do not recommend bringing them

under the opt-in regime of Art. 13(1). Various Member States have established or are currently establishing coordinated opt-out lists in the domain of telephone direct marketing. These initiatives should be continued and evaluated after a certain period of time. On the other hand, it would be difficult for Member States where a choice has been made to submit direct marketing telephone calls to an opt-in consent regime, to move backwards. Last but not least one could also argue that a harmonised consent regime for telephone direct marketing is not strictly necessary because this kind of marketing is most often organised at a national level.

In relation to communications made to subscribers who are legal persons, the Directive stops short of specifying what rules should be put in place at Member State level, but provides the broad requirement that the legitimate interests of such subscribers be "sufficiently protected". In general, one of three approaches was adopted in each Member State for this situation: opt-in, opt-out, or no protection for legal persons.

A last recommendation is to determine more clearly the applicable law in this domain. In Member States having transposed Article 13 in the framework of the data protection legislation, the question of the applicable law will be dealt with according to Article 4 of Directive 95/46/EC. This means that the establishment of the unsolicited e-mail sender will determine the applicable law. In other Member States the provisions of Article 13 have been transposed in the context of consumer protection legislation. In these cases the residence of the e-mail recipient will be taken into account. This should not be a problem if the content of the national provisions transposing Article 13 would be perfectly harmonised. Our survey has, however, shown that there are important divergences. In addition, conflicts can arise with regard to supervision. Similar to what has been stated in the previous chapter with regard to the processing of traffic and location data, companies using e-mail for direct marketing purposes could be subject to the supervision of authorities from different Member States for the same activity. Without any "consistency mechanism" such as the one proposed in the context of the revision of the general data protection framework, this could lead to unwanted complications and legal uncertainty.

8. Relationship with the Draft Data Protection Regulation

On 25 January 2012, the European Commission released its proposal for a comprehensive reform of the 1995 data protection rules on personal data processing.[291] The proposed Regulation is currently under discussion in the Council. Once adopted, this Regulation will become directly applicable across the whole EU territory after a transition period of two years.

8.1. Adjustments to the ePrivacy Directive

The draft Regulation makes a limited number of technical adjustments to the ePrivacy Directive in order to take account of the transformation of Directive 95/46/EC into a Regulation. The Commission announced in its Communication that the substantive legal consequences of the new Regulation for the ePrivacy Directive will be the object, of a review by the Commission, after the end of the legislative process on the general Data Protection Regulation.[292]

Recital (135) of the draft Regulation states that the Regulation "should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly."

Article 89.1 is worded as follows: "This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC". According to article 89.2, the second paragraph of Article 1 of the ePrivacy Directive ("The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.") will be deleted.

[291] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[292] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF, p. 4, footnote 15

8.2. Potential effect on the ePrivacy Directive

The objectives of the proposed Article 89(1), further developed in Recital (135) are to delimit the scope of application of both legislative instruments and to ensure that the modified ePrivacy Directive and the Regulation can work together in the future, after the adoption of the General Data Protection Directive. The proposed Regulation will not be applicable in all cases where the ePrivacy Directive contains specific obligations with the same objective. For the provisions examined in our Study this solution is perfectly possible to implement.

However, if, according to the recommendations formulated in this Study, the scope of application of the ePrivacy Directive were to be modified, the text of Article 89(1) should be amended as well. Currently this text refers to "obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union". This should be changed into "obligations on natural and legal persons in relation to the processing of personal data in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union".

The proposed Art. 89(2) is necessary because a directive cannot "particularise" a regulation. According to Art. 288(2) TFEU a regulation has not only general application but is also binding in its entirety and directly applicable in the whole of the Union. Member States can therefore not be requested in a directive to derogate from rules contained in a regulation.

In our view, the Commission should consider transforming the Directive into a regulation for three reasons. . First of all, the relationship between the provisions of the two legislative instruments would be considerably less complex if they are at the same level. This would make the announced revision of the ePrivacy Directive a lot easier.[293] In the second place it may considerably facilitate the application of the entire supervisory and enforcement mechanism introduced by the proposed Data Protection Regulation to the topics currently covered by the ePrivacy Directive. Arguably the adoption of this mechanism will be justified once the scope of the Directive (or of a future regulation) would be widened beyond the borders of the

[293] The revision would be easier because, not only for many current provisions such as Art. 1(3) – the exclusion of the former second and third pillar from the scope of the ePrivacy Directive -, Art. 4(3) – security breach notification - , Art. 15 (1) – allowing Member States to restrict certain provisions of the Directive –, etc. but also for not explictly regulated issues such as the territorial scope, it will suffice to refer to the corresponding provisions of the general Data Protection Regulation. Notice that many current provisions of the ePrivacy Directive are already formulated in a directly binding form (see e.g. Articles 4, 6, 7, 8, 9, 13(1)).

electronic communications sector. Last but not least, it would allow the amendment of Art. 89 of the general Data Protection Regulation (once adopted) if this provision was no longer in line with the final text of a future "ePrivacy Regulation".[294]

If the ePrivacy Directive is not transformed into a regulation and remains a directive, it would be necessary to transform it into a self-standing instrument after the adoption of the General Data Protection Directive, following the example of the proposed Law Enforcement Directive. As a result there would be two instruments containing provisions on personal data protection with mirroring provisions but on different levels. Moreover, if the scope of application of the ePrivacy Directive will be widened and include services which do not belong to the electronic communications sector in the strict sense, the ePrivacy Directive will no longer address a separate sector but the entire online environment, which is also one of the main targets of the proposed Data Protection Regulation. This overlap will inevitably create a very complex situation.

[294] In this hypothesis it is, for example, no longer necessary to delete Art. 1(2) of the ePrivacy Directive because a future ePrivacy Regulation can perfectly particularise and complement the General Data Protection Regulation. Consequently Art. 89(2) would have to be abrogated again.

9. Conclusions

Directive 2002/58/EC – hereafter "the ePrivacy Directive" – aims to protect the privacy and regulate the processing of personal data in the electronic communications sector. This report did not deal with the entire ePrivacy Directive but focused on five topics: (i) Articles 1 to 3 regarding the geographical and material scope of application; (ii) Article 5(1) on confidentiality of communications; (iii) Article 5(3) on cookies, spyware and the like; (iv) Articles 6 and 9 on traffic and location data respectively; (v) Article 13 on unsolicited commercial communications. Topics such as security (Art. 4), itemized billing (Art. 7), calling and connecting line identification (Art. 8 and 10), automatic call forwarding (Art. 11) and subscriber directories (Art. 12) are thus outside the scope of this report.

Scope of application

The Regulatory Framework for Electronic Communications to which the ePrivacy Directive belongs, applies to providers of electronic communications networks and services. More precisely, according to Art. 3, the Directive is applicable "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community." Consequently only services consisting wholly or mainly in the conveyance of signals – as opposed to e.g. the provision of content or other value added services – are within the scope of the Directive. However convergence sometimes results in services that are very similar from a functional perspective being subject to different legal regimes depending on whether they are provided in the form of an electronic communications service, an information society service, or an audiovisual service. Well-known examples are internet telephony and webmail.

Our survey of the transposition of the ePrivacy Directive in the national legislation of the Member States has demonstrated that the provisions of the Directive are not always transposed in the context of the national legal framework applicable to the electronic communications sector. Several provisions of the Directive have been transposed by Member States in the context of another legal framework, such as the legislative instrument applicable to information society services or the legal framework for consumer protection. As a result, the scope of the national provisions on topics such as cookies, traffic and location data, or unsolicited direct marketing communications, adopted pursuant the ePrivacy Directive, frequently have a different scope of application than the one defined by Art. 3 of the ePrivacy Directive.

The definition of the scope of application of the ePrivacy Directive is moreover ambiguous. The provision refers to "the provision of publicly available electronic

communications services in public communications networks" and, according to Art. 2.c) of the Framework Directive the notion of "electronic communications service" does not include information society services, as defined in Article 1 of Directive 98/34/EC and which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

On the other hand, nobody seems to contest that certain provisions of the ePrivacy Directive are nevertheless applicable to providers of information society services. The most obvious example is Art. 5(3) dealing with the use of cookies and similar techniques.[295] For other provisions, such as Art. 9 – regulating the processing of location data other than traffic data – the extension of the scope of application to information society service providers is most often excluded.[296] Art. 13 regulating unsolicited direct marketing communications is generally interpreted as being exclusively applicable to messages transmitted via electronic communications.[297]

Moreover, for certain provisions, such as Art. 6 – relating to the processing of traffic data – or Art. 9 – on location data other than traffic data – the narrow scope leads to unacceptable situations of unequal treatment. It is difficult to justify why traffic or location data should receive a different legal protection if they are processed in the context of very similar services from a functional perspective. The same observation is valid for the provision of Art. 13(1), prohibiting the use of e-mail without prior consent of the recipient only for messages transmitted via electronic communications and not for messages exchanged via information society services such as social media platforms.

In order to remedy this situation we recommend amending Art. 3 of the ePrivacy Directive to make its provisions applicable to the protection of privacy and 'the processing of personal data in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union. The amendment would put an end to the discussion about the applicability of the provisions of the ePrivacy Directive to information society services and other value-added services provided via public electronic communications networks. In addition it extends the scope of the Directive to private networks that are

[295] See e.g. the Article 29 Opinion 2/2010 on online behavioural advertising, p. 9: "The Working Party has already pointed out in WP 29 Opinion 1/2008 that Article 5(3) is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used".

[296] See e.g. the Article 29 Opinion 13/2011 on geolocation services on smart mobile devices, p. 9: ""The e-Privacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network".

[297] See e.g. the Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines, WP 148 (2008), p. 4: .

intentionally made accessible to the public. The impact of such an intervention should be carefully assessed, as it may overlap with the general data protection reform.

In the longer term, further convergence will probably trigger a broader debate about the opportunity of a more in-depth revision of the current structure of the European regulatory framework for the online environment. Maintaining a distinct regulatory regime for electronic communications services, information society services or audiovisual services will most probably become less and less relevant in the future. For the time being however, an explicit widening of the scope of application of the ePrivacy Directive can solve, to a large extent, the most urgent issues.

Confidentiality

It is evident that, at the moment of the adoption of this provision in 2002, all Member States already had since long introduced legislation protecting the confidentiality of private communications. The transposition of Art. 5.1 did not have a harmonizing effect on these existing national legal provisions. The legal protection of confidentiality of communications in the Member States remains therefore diverse. The diversity is mainly related to definitions, conditions and other modalities but, evidently, also to the exceptions. This is due to the fact that Art. 15.1 of the ePrivacy Directive states that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC".

As a consequence, rules with regard to e.g. wiretapping for law enforcement purposes or monitoring electronic communications in an employment context, are not harmonized at the European level. This situation will not fundamentally change after the transposition by the Member States of the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (so-called "Law Enforcement Directive"). The scope of this proposed Directive is restricted to the processing of personal data by law enforcement authorities and doesn't deal with topics such as the interception of electronic communications. Further harmonisation of the rules with regard to these topics would also be difficult to achieve in the short term since they are, in most of the Member States, integrated into specific national criminal procedure rules.

In order to bring the text of Art. 5.1 in line with the proposed widening of the scope of the ePrivacy Directive, we suggest amending it and making it applicable to "confidentiality of communications and the related use of traffic data by means of a public or publicly accessible private communications network". It is further evident that confidentiality of electronic communications should also be protected against "automatic" intrusions without human intervention. This clarification could be added in a Recital to the Directive, noting that automated intrusions are of course always initiated and/or controlled by one or more persons. Last but not least the exception of Art. 5(1) for "technical storage which is necessary for the conveyance of a communication" should probably be broadened to "storage as far as necessary for ensuring the functioning of the network or the provision of the service on that network". Such amendment would be a logical consequence of the extension of the scope of Art. 5.1 to e.g. information society services.

Article 5.2 of the ePrivacy Directive stipulates that the protection of confidentiality "shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication". This provision – often designated as the "business exception" - has been interpreted and transposed by Member States in very different ways. National legislators in some of the Member States have restricted the scope of Art. 5.2 to the electronic communications sector. In other Member States the provision is applied to all sectors and is aimed at giving employers some margin to register telephone conversations conducted by employees in the context of, for instance, a call center. We suggest therefore clarification of the scope of Art. 5.2 in order to obtain a uniform transposition and implementation of this provision throughout the Union. The currrent restriction to "the provision of evidence of a commercial transaction or of any other business transaction" could be widened to other situations in which recording of communications in an employment context seems to be justified, such as quality control or legitimate supervision of work performance. A clear legal basis for monitoring communications of employees for such legitimate reasons, and under the condition to respect general data protection rules, is currently missing at the European level. A careful assessment of the impact of such change on stakeholders would be needed to assess its feasibility, taking into account the diversity of rules currently applicable to the processing of personal data in the employment context.

Cookies and Similar Techniques

Article 5.3 requests the Member States to "ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent (…)". Recital (24) explains that "so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal

without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned".

The requirement to collect the users' prior consent in the context of Art. 5.3 is the result of an amendment adopted in 2009 in the context of the Citizen's Rights Directive. Besides the fact that the 2009 amended version of Art. 5.3 has not yet been transposed by all Member States, the main conclusion of our survey on the transposition of the ePrivacy Directive in the Member States is that there is a need for EU-wide guidance on how to implement this amendment in practice. In particular, the possibility to express consent via the configuration of browser settings has initially led to uncertainty. The Article 29 Working Party has therefore elaborated the conditions for browser settings to be able to deliver valid and effective consent in its Opinion 2/2010. Several major web browsers, often having as a default setting to allow all kinds of cookies, don't currently fulfil these conditions. As a consequence – and this should preferably be clearly stated in a Recital of the ePrivacy Directive – only browsers or other applications which by default reject 3d party cookies and which require the user to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites are able to deliver valid and effective consent.

It is further difficult to deny that the introduction of the consent rule in Art. 5.3 did not entirely reach its objective. This is largely due to the fact that users currently receive a warning message with regard to the use of cookies on almost every web site. Obviously the effect of such warning messages would substantially increase if they only appeared where the web site contained 3d party cookies, cookies used for direct marketing purposes and, more generally, all cookies that are not related to the purpose for which the user is navigating on the site.

Article 5.3 currently contains two exceptions where prior consent of the user is not needed: a) for the technical storage of the access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the access to information is strictly necessary for the provider. These exceptions should preferably receive a slightly broader formulation, for example, by deleting the condition stating that "the storing of or the access to information (should be) strictly necessary for the provider". In addition we recommend inserting additional exceptions, e.g. for cookies which are exclusively used for website usage statistics. Finally we propose explicitly requesting specific, active and prior consent in all cases where cookies or similar techniques are used for direct marketing purposes.

Traffic and Location Data

Although Article 6 of the ePrivacy Directive seems to be more or less correctly transposed by the Member States, there are serious problems with regard to the enforcement of some of its provisions. Most problematic is Art. 6(3) which stipulates: "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 or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time."

In practice some mobile operators mention the possibility of processing user and traffic data in their general terms and conditions. Some of these terms and conditions grant the operator a right to process the data for a duration of two years after the end of the contract.

Also frequently criticised are the provisions with regard to location data. The ePrivacy Directive regulates only a fraction of location based services and namely those that rely on the processing of location data other than traffic data offered via a public communications network or in a publicly available electronic communications service. Location based services that are offered to the members of a private network are not governed by the provisions of Article 9 of the ePrivacy Directive, even though privacy risks may be the same or even greater. For example, Article 9 does not cover location data that are transmitted via enterprise networks aimed at a private user group, or data collected and transmitted via infrared signals or GPS signals in combination with a private secured wireless LAN. Moreover, in its Opinion 13/2011 dealing with geolocation services on smart mobile devices the Article 29 Working Party, referring to the strict definition of electronic communications service in Art. 2, c) of the Framework Directive, stated that "the ePrivacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network" (p. 9).

In line with our proposed amendment to Article 3 of the ePrivacy Directive it is sufficient to slightly modify the wording of these Articles in order to make them applicable to all services provided via public or publicly available private communications networks that collect and further process traffic and location data. As a result the processing of location data by information society services will be subject to the application of Art. 6 and Art. 9. Additionally, efforts are needed at the Union and the national level to ensure a correct transposition of the European rules and to enforce their implementation in practice.

Unsolicited Direct Marketing Communications

In general, Member States have adequately transposed the provision of Article 13(1) of the Directive. Thus, they have introduced national provisions ensuring that the use of automated calling and communication systems without human intervention, fax and e-mail for direct marketing is prohibited unless prior consent has been obtained. The term "electronic mail" – being defined in Art. 2(h) of the ePrivacy Directive as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient" – is generally interpreted as being restricted to e-mail via electronic communications and not applicable to messages exchanged via information society services such as Facebook, LinkedIn, Skype or Twitter, even when the transmission of such messages ultimately occurs over the internet and thus makes use of publicly available electronic communications services provided on public electronic communications networks. This restrictive interpretation seems also be the one adopted by the Article 29 Working Party. The Directive leaves some discretion to Member States in relation to "other forms of direct marketing", such as person-to-person voice telephony. As they are relatively more costly for direct marketers, Member States are free to choose an opt-in or opt-out consent regime. Some Member States have chosen opt-in, and others opt-out. This distinction is a natural consequence of the margin of policy making left to the national legislators by EU legislation.

In relation to communications made to subscribers who are legal persons, the Directive stops short of specifying what rules should be put in place at Member State level, but provides the broad requirement that the legitimate interests of such subscribers be "sufficiently protected". In general, one of three approaches was adopted in each Member State for this situation: opt-in, opt-out, or no protection for legal persons.

Our main recommendation with regard to Art. 13 is to bring the scope in line with our proposed amendment to Art. 3. This means in the first place that the opt-in rule of Art. 13(1) should also apply to e-mail messages transmitted via information society services. This extension of the scope of Art. 13(1) should however not lead to the prohibition of all kinds of personalised online advertising without first collecting the consent of the user. Therefore the definition of "e-mail" in Art. 2(h) of the Directive should be amended.

Relationship with the proposed general data protection regulation

In our view, the Commission should consider transforming the Directive into a regulation for three reasons. . First of all, the relationship between the provisions of the two legislative instruments would be considerably less complex if they are at the

same level. This would make the announced revision of the ePrivacy Directive a lot easier.[298] In the second place it may considerably facilitate the application of the entire supervisory and enforcement mechanism introduced by the proposed Data Protection Regulation to the topics currently covered by the ePrivacy Directive. Arguably the adoption of this mechanism will be justified once the scope of the Directive (or of a future regulation) would be widened beyond the borders of the electronic communications sector. Last but not least, it would allow the amendment of Art. 89 of the general Data Protection Regulation (once adopted) if this provision was no longer in line with the final text of a future "ePrivacy Regulation".[299]

If the ePrivacy Directive is not transformed into a regulation and remains a directive, it would be necessary to transform it into a self-standing instrument, after the adoption of the General Data Protection Directive, following the example of the proposed Law Enforcement Directive. As a result there would be two instruments containing provisions on personal data protection with mirroring provisions but on different levels. Moreover, if the scope of application of the ePrivacy Directive will be widened and include services which do not belong to the electronic communications sector in the strict sense, the ePrivacy Directive will no longer address a separate sector but the entire online environment, which is also one of the main targets of the proposed Data Protection Regulation. This overlap will inevitably create a very complex situation.

[298] The revision would be easier because, not only for many current provisions such as Art. 1(3) – the exclusion of the former second and third pillar from the scope of the ePrivacy Directive -, Art. 4(3) – security breach notification - , Art. 15 (1) – allowing Member States to restrict certain provisions of the Directive –, etc. but also for not explicitly regulated issues such as the territorial scope, it will suffice to refer to the corresponding provisions of the General Data Protection Regulation. Notice that many current provisions of the ePrivacy Directive are already formulated in a directly binding form (see e.g. Articles 4, 6, 7, 8, 9, 13(1)).

[299] In this hypothesis it is, for example, no longer necessary to delete Art. 1(2) of the ePrivacy Directive because a future ePrivacy Regulation can perfectly particularise and complement the General Data Protection Regulation. Consequently Art. 89(2) would have to be abrogated again.

European Commission

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Luxembourg, Publications Office of the European Union

2015 – 122 pages

ISBN 978-92-79-47439-2

doi:10.2759/411362

KK-04-15-268-EN-N

doi:10.2759/411362

ISBN 978-92-79-47439-2