ETNO

Study on the revision of the ePrivacy Directive

August 2016

TABLE OF CONTENTS

A EXECUTIVE SUMMARY

1 INTRODUCTION TO THIS STUDY

This study has been prepared by the international law firm DLA Piper UK LLP (Brussels office), at the request of ETNO. ETNO is the European Telecommunications Network Operator's Association calling for the European legislator to repeal Directive 2002/58/EC (**"ePrivacy Directive"**), which has been slated for review by the European Commission.

Regulation 2016/679 (**"General Data Protection Regulation"** or **"GDPR"**), formally approved in April 2016, is meant to apply to all players offering services to European citizens, notwithstanding the sector they are active in, and aims to achieve a full and horizontal harmonisation in the area of privacy, based on the principle of technology neutrality and adapted to the needs of a digital society.

While ETNO fully supports this idea, it is convinced that such harmonised privacy area will not be realized as long as the ePrivacy Directive continues to exist next to the GDPR. Since the start of the GDPR discussions, and even prior to that, ETNO has expressed its request to repeal the e-Privacy Directive. ETNO believes that if the ePrivacy Directive were not to be repealed and continues to exist next to the GDPR, there is a significant risk that legal uncertainty for consumers as well as telecom providers will continue to last, which is to be avoided at all cost.

Against this background, and further building on the results and findings of the previous study on the ePrivacy Directive in which DLA Piper came to the conclusion that there are solid arguments in support of repealing the ePrivacy Directive, DLA Piper has been requested by ETNO to further investigate arguments supporting said long-term objective of repealing the ePrivacy Directive. The analysis of this request forms the scope and subject matter of the present document.

The upcoming review of the ePrivacy Directive is a unique opportunity:

- To build consumer trust by reducing the regulatory complexity of having a dual data protection regime whereby consumer face inconsistent and different privacy experiences for functionally-equivalent services;
- To achieve a true level playing field between telecom providers and other market players (such as for example providers of over-the-top services) in order to ensure that the same technologically neutral principles apply to all stakeholders; and
- To ensure a consistent application and enforcement of a single set of data protection principles valid in the same way throughout the entire European Union.

Therefore ETNO urges the policy makers to take into account the arguments developed and suggestions formulated in this study. It cannot be denied that in today's converged world, the distortions between sectors and technologies are not justifiable and this particular example of asymmetry needs to be addressed without delay.

2 STUDY RESULTS

The reasons underpinning ETNO's objective of repealing the ePrivacy Directive can be summarized as follows:

- First of all, the co-existence of the ePrivacy Directive and GDPR will likely lead to legal uncertainty and confusion for all stakeholders (telecom providers, consumers and regulatory bodies), notably with regard to the scope of the ePrivacy Directive and with regard to the competent regulatory bodies;
- Secondly, while at the time of adoption of the ePrivacy Directive it was justified to have a specific set of privacy rules for the telecom sector, the existence of such a dual data protection framework can no longer be justified in today's new reality of converged media and communication services and increasingly innovative offers from a myriad of new players. Indeed, telecom providers are subject to the GDPR and the sector-specific rules of the ePrivacy Directive as regards the processing of personal data (notably location and traffic data), whereas the – mainly US-based – over-the-top players that are offering functionally equivalent services (such as Whatsapp and Skype) are only subject to the GDPR, and not to the ePrivacy Directive. This situation needs to be reconsidered: similar services should be subject to the same rules;
- Thirdly, as long as the ePrivacy Directive coexists with the GDPR, there will be an **unlevel playing field** between all market players, consumers will not experience comparable digital privacy online and the competitive position of European providers will be compromised, possibly until 2020 if the European legislator does not take immediate action.

As a result of these considerations, and to remedy its consequences, DLA Piper has further analysed and developed arguments that support the objective of repealing the ePrivacy Directive. As a result of that analysis, the following legislative changes are being proposed:

- The privacy-related provisions of the ePrivacy Directive that overlap with the GDPR, notably the clauses on security of processing (Art. 4 EPD), traffic data (Art. 6 EPD), location data (Art. 9 EPD), cookies (Art. 5(3) EPD) and unsolicited communications (Art. 13 EPD) as well as Regulation 611/2013 on the notification of personal data breaches under the ePrivacy Directive[1] can and should be repealed in their entirety. Removing those provisions will not impact the level of protection offered to consumers;
- Only one privacy-related provision of the ePrivacy Directive, i.e. the article on confidentiality of communications (Art. 5 EPD), may still be relevant today. Following further assessment of this issue, and if still deemed required, we propose to move this to a more horizontal legislation covering all services that allow interpersonal communications; and
- The non-privacy-related provisions of the ePrivacy Directive that govern general telecom and/or consumer protection topics, i.e. the articles on non-itemised bills (Art. 7 EPD), control over call line identification (Art. 8 EPD), automatic call forwarding (Art. 11 EPD) and directories of subscribers (Art. 12 EPD) have either become outdated or no longer need to be regulated. Consequently they can be

[1] Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, *OJ. L.* 173, 26 June 2013, 2–8.

repealed, or to the extent still deemed relevant by the European legislator moved to the updated regulatory framework covering a broader range of communication services.

As a result of the arguments and proposed legislative changes set out above, it is clear that there no longer is a need to keep the ePrivacy Directive. However, For the sake of completeness, and only to the extent that the European legislator would not fully follow the proposed changes, but consider that a separate ePrivacy instrument would remain required for specific topics (e.g. the confidentiality of communications principle), ETNO is of the opinion that that such revised ePrivacy instrument should take the form of a regulation complementing the GDPR, of which the material, geographical and personal scope is aligned with the GDPR and for which data protection authorities should become competent for enforcing said revised ePrivacy instrument.

B STUDY REPORT

1 INTRODUCTION AND CONTEXT OF THE STUDY

Today, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data[2] (hereafter referred to as **"Data Protection Directive"**) is the central legislative instrument in the protection of personal data. On 27 April 2016, Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[3] (hereafter referred to as **"General Data Protection Regulation"** or **"GDPR"**) has been adopted. The GDPR shall apply from 25 May 2018 and will repeal and replace the Data Protection Directive as from that date. The GDPR introduces a number of new concepts and new rights and obligations for both data controllers and data subjects.

At the time, the Data Protection Directive was complemented by a specific set of rules on the processing of personal data in the electronic communications sector, including rules on traffic and location data, as well as on the notification of personal data breaches. Currently, these rules are contained in the Directive 2002/58/EC on privacy and electronic communications[4], as amended by Directive 2006/24/EC and Directive 2009/136/EC[5] (hereafter referred to as **"ePrivacy Directive"** or **"EPD"**), which in itself replaced an earlier directive of 1997. As the growth and development of the electronic communications sector gave rise to specific requirements concerning the protection of personal data and the privacy of the user, the European legislator considered the adoption of different rules for amongst others the treatment of traffic data to be necessary and appropriate.

While the approval of the ePrivacy Directive might have been necessary and appropriate at the date of its adoption, it should be emphasised that nowadays the entire area of electronic communications has undergone significant changes, is converging and is no longer exclusively reserved for telecom providers. As the Internet has evolved rapidly, a range of new telecom-alike services (including over-the-top services such as Whatsapp and Skype) started developing, some of which are functionally equivalent to traditional telecom services and also give rise to the collection of location data and traffic data and which are not necessarily

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ.L*. 281, 23 November 1995, 31 – 50.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ.L*. 119, 4 May 2016, 1-88.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ.L*. 201, 31 July 2002, 37-47.

[5] Consolidated version of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) amended by (i) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC and by (ii) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

subject to the ePrivacy Directive. Beyond convergence, various services, such as for communications, are bundled with other services and integrated in single offerings. The existence of different and unequal rules for equivalent services does not only greatly impact telecom providers' ability to compete on equal footing but also creates legal uncertainty and overall confusion for consumers. Moreover, a dual regime is unlikely to lead to a single market in privacy or data protection and distorts the value in data and innovation in data-driven services.

Since the start of the GDPR discussions, and even prior to that, ETNO has expressed its request to repeal the ePrivacy Directive. Therefore, in 2015, ETNO requested the international law firm DLA Piper UK LLP (Brussels office) to investigate the technical and legal feasibility of addressing the regulatory asymmetries created by the ePrivacy Directive and to propose a way how this could be dealt with in the light of the then on-going discussions in relation to the draft GDPR.[6] DLA Piper came to the conclusion that there are solid arguments in support of repealing the ePrivacy Directive and that there undoubtedly was room for the integration of the ePrivacy Directive and draft GDPR into one single legal instrument, notably the draft GDPR, and proposed in that respect a text amendment to the draft GDPR.

Although the European Commission recognised and emphasised in its Digital Single Market Strategy[7] that there indeed is a pressing need to assess and review the ePrivacy Directive in order to ensure a high level of protection for data subjects and a level playing field for all market players, ETNO regrets that – due to time and political constraints – the proposed amendments have not been incorporated in the final text of the GDPR.

In execution of its Digital Market Strategy, the Commission published in June 2015 a study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation"[8] and launched in April 2016 a public consultation on the evaluation and review of the ePrivacy Directive.

Against this background, and further building on the results and findings of the previous study on the ePrivacy Directive, DLA Piper has been requested by ETNO to further investigate arguments supporting the long-term objective of repealing the ePrivacy Directive, with the aim to (i) build consumer trust (by reducing the regulatory complexity), (ii) restore the level playing field between all market players and (iii) ensure consistency between the regulatory framework applicable to providers of electronic communication services and the GDPR. In this respect it must be stressed that the upcoming revision of the ePrivacy Directive is undeniably a unique opportunity to take big steps forward in achieving that long-term objective of repealing the ePrivacy Directive.

The main outcome of this Study is that:

[6] The full report can be downloaded from the ETNO website (https://www.etno.eu/datas/publications/studies/DPTS_study_DLA_31052015_Final.pdf). For a summary, see R. SCHOEFS and P. VAN EECKE, "Do we still need the ePrivacy Directive?", www.think-digital.eu/?n=2015/306.

[7] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions, A Digital Single Market Strategy for Europe, COM(2015), 192, final, 6 May 2015, 10 and 13.

[8] The final report of the study "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071), as prepared for the European Commission, can be downloaded from https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

- The privacy-related provisions of the ePrivacy Directive that overlap with the GDPR, notably the clauses on security of processing (Art. 4 EPD), traffic data (Art. 6 EPD), location data (Art. 9 EPD), cookies (Art. 5(3) EPD) and unsolicited communications (Art. 13 EPD) as well as Regulation 611/2013 on the notification of personal data breaches under the ePrivacy Directive[9] can and should be repealed in their entirety;

- Only one privacy-related provision of the ePrivacy Directive, i.e. the article on confidentiality of communications (Art. 5 EPD), may still be relevant today. Following further assessment of this issue, and if still deemed required, we propose in any event to move this to a more horizontal legislation covering all services that allow interpersonal communications. and

- The non-privacy-related provisions of the ePrivacy Directive that govern general telecom and/or consumer protection topics, i.e. the articles on non-itemised bills (Art. 7 EPD), control over call line identification (Art. 8 EPD), automatic call forwarding (Art. 11 EPD) and directories of subscribers (Art. 12 EPD) can be repealed, or to the extent still deemed relevant by the European legislator moved to the updated regulatory framework covering a broader range of communication services.

This Study briefly discusses the relevant legislative evolutions and market evolutions (*Section 2*) as well as the long-term objectives and benefits intended to be achieved through repealing the ePrivacy Directive (*Section 3*). Hereafter, the Study will further explain how the upcoming revision of the ePrivacy Directive fits into that long-term objective (*Section 4*), whereby an analysis will be made of the key provisions of the current ePrivacy Directive, notably of the privacy-related provisions that overlap with the GDPR (*Section 4.2*), the privacy-related provision that requires a clarification (*Section 4.2*) and the non-privacy-related provisions, of which the need and relevance can be questioned (*Section 4.3*). To conclude, an overview will be presented of the proposed changes to the regulatory framework on ePrivacy and communications services and the appropriate means to accommodate those changes (*Section 5*).

[9] Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, *OJ. L.* 173, 26 June 2013, 2–8.

2 LEGISLATIVE & MARKET EVOLUTIONS

2.1 Legislative evolutions

2.1.1 From Data Protection Directive to GDPR

The Data Protection Directive – which constitutes the centrepiece of the currently applicable European legislation on personal data protection – was adopted in 1995, with a two-fold objective: (i) to protect the fundamental rights to data protection and (ii) to guarantee the free flow of personal data between Member States. It has been complemented by Framework Decision 2008/977/JHA as a general instrument at EU level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters.[10]

Over the past 20 years, rapid technological developments have brought new challenges for the protection of personal data. With the rise of amongst others, social networking sites, cloud computing, location-based services, big data technologies and over-the-top services, the scale of data sharing and collecting increased dramatically, and technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Moreover, individuals increasingly make personal information available publicly and globally, and technology has transformed both the economy and social life.

In regard of those challenges and in order to build trust in the online environment, the current framework needed modernising, as it has been introduced at a time when many of today's online services and the challenges they bring for data protection did not yet exist. With this objective and after four years of intense debates and discussions a final agreement has been reached in the Spring of 2016, resulting in the GDPR. The GDPR is complemented with Directive 2016/680 on the processing of personal data for law enforcement purposes and repealing Framework Decision 2008/977/JHA.[11]

2.1.2 From ePrivacy Directive to …

In the mid-1990s specific European telecommunication data protection rules were enacted complementing the Data Protection Directive. Because of the introduction of new advanced digital technologies in public telecommunications networks, the adoption of Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[12] (**"Telecommunications Data Protection Directive"**) was considered necessary to protect the fundamental rights and freedoms of natural persons and legitimate interests of legal persons, "*in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users*" .

[10] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ.L.* 350, 30.12.2008, 60-71.

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ.L*. 119, 4 May 2016, 89–131.

[12] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ.L. 24, 30 January 1998, 1–8.

The telecom sector has been evolving rapidly and still evolves at a high speed. Consequently, over the past years the sector-specific rules had to be changed several times in order to keep up with new developments in the telecom sector.

In 2002, the European legislator decided to rename the Telecommunications Data Protection Directive into the ePrivacy Directive. The 'first' ePrivacy Directive modernised and broadened many of the concepts already included in the Telecommunications Data Protection Directive, and more importantly included a different treatment for the processing of location data that was only applicable to telecom providers.

In 2006, the ePrivacy Directive has been amended again by Directive 2006/24/EC[13], also known as the Data Retention Directive. On 8 April 2014 the Court of Justice of the European Union however declared the Data Retention Directive to be invalid, hence those modifications are no longer to be taken into account.[14]

In 2009, the ePrivacy Directive has been amended another and also a last time by Directive 2009/136/EC[15], on which moment the new so-called 'cookie provision', changing the former opt-out regime into an opt-in regime, was introduced. As the cookie provision is not specifically applicable to actors in the telecom sector, but instead to all website operators, it has never been clear for which reason such provision has been included in the ePrivacy Directive.

On 6 May 2015, the European Commission published its Digital Market Strategy for Europe, in which it acknowledges the inadequacy of the current legal framework, and explicitly recognises the need to reassess the ePrivacy Directive so as to implement a level playing field for all market players, since "*most of the articles of the current e-Privacy Directive apply only to providers of electronic communications services, i.e. traditional telecoms providers. Information society service providers using the Internet to provide communication services are thus generally excluded from its scope.*".[16]

Indeed, the applicability of the majority of the rules set out in the ePrivacy Directive depends on whether or not a particular service qualifies as an 'electronic communications service' (Article 2.c of the Framework Directive, meaning "*a service normally provided for remuneration which consist wholly or mainly in the conveyance of signals on electronic communications networks (…)*"). According to the general interpretation, most OTT services are considered as not conveying signals on electronic communications networks and thus fall outside the scope of this definition and regulatory framework. Consequently, they do not need to comply with most obligations under the ePrivacy Directive. Instead, they are generally considered to fall within the definition of 'information society services'[17] and consequently under the scope of the E-commerce Directive.[18] The problems and difficulties caused by the definition of 'electronic communications services' are

[13] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ.L.* 105, 13 April 2006, 54-63.

[14] CJEU 8 April 2014, C-293/12 and C-594/12, www.curia.eu.

[15] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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, *OJ.L.* 337, 18 December 2009, 11-36.

[16] European Commission, "A Digital Single Market Strategy for Europe", COM(2015) 192 final, 10, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

[17] As defined in Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

[18] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ.L.* 178, 17 July 2000, 1-16.

only expected to increase, as this technical definition neither reflects consumers' perception nor is future-proof. While this technical definition does not match with services that are IP-based, it is expected that in a few years' time, telecom services will be completely switched from public switched telephone networks (PSTN) to IP-networks.

On 10 June 2015, only one month after the publication of its Digital Market Strategy for Europe, the Commission published a commissioned study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (hereafter referred to as **"Commission Study"**).[19] That study examined whether the ePrivacy Directive has achieved its intended effects and puts forward recommendations for future revision. Instead of including all provisions, the focus of the study has been on the geographical and material scope of the ePrivacy Directive (Art. 1 to 3 EPD), the confidentiality of communications (Art. 5(1) EPD), the cookie provision (Art. 5(3) EPD), traffic and location data (Art. 6 and 9 EPD) and unsolicited communications (Art. 13 EPD). The findings of this study will be incorporated in the relevant sections of this report.

Almost one year later, on 11 April 2016, notably a few days before the formal adoption of the GDPR, the Commission launched its long-awaited public consultation on the ePrivacy Directive. Through the consultation the Commission seeks to gather views on the effectiveness, efficiency, relevance, and coherence of the current EU rules, and also on possible approaches for the revision of the Directive.

Finally, on 25 May 2016, the Commission published its communication on online platforms and the Digital Single Market, in which it paves the way for a degree of deregulation of EU telecom rules by suggesting to only retain a limited set of communications-specific rules that would apply to all relevant and comparable services (including when provided by OTT players). Notably with regard to the ePrivacy Directive, the Commission suggests to consider a simplification of the rules.[20]

2.2 Market evolutions

The aim of this Study is not to present all economic evolutions the telecom sector went through as from the existence of state-owned monopolies, over the liberalisation of the market to the current rise of OTT players. We nevertheless consider it highly relevant to briefly discuss the current state of the market, and the important and increasing position of OTT players on the market.

The entire area of electronic communications has undergone significant changes and is no longer exclusively reserved for telecom providers. More in particular, over the last years the telecom sector has witnessed the rise of OTT players offering several competing and functionally-equivalent services.[21]

The majority of the respondents to the public consultation on the evaluation and review of the regulatory framework for electronic communications consider that communication services offered by OTT players are

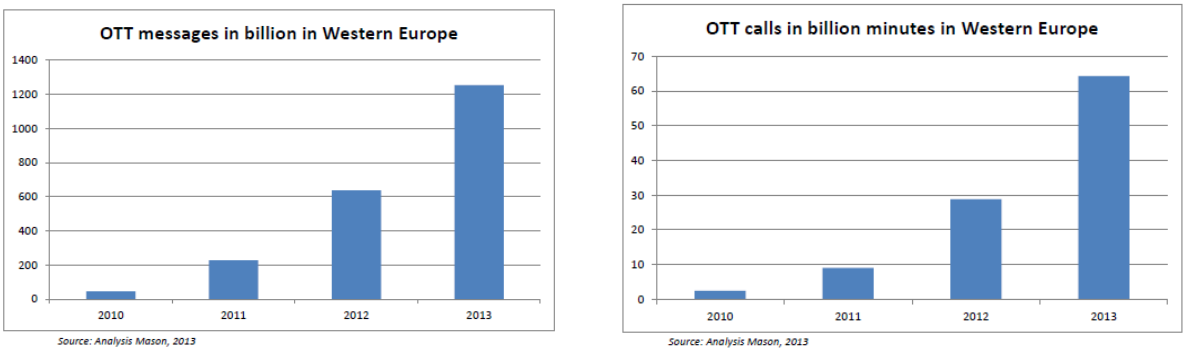
[19] The final report of the study "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071), as prepared for the European Commission, can be downloaded from https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

[20] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM (2016) 288/2, https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-market.

[21] CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 15, http://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf

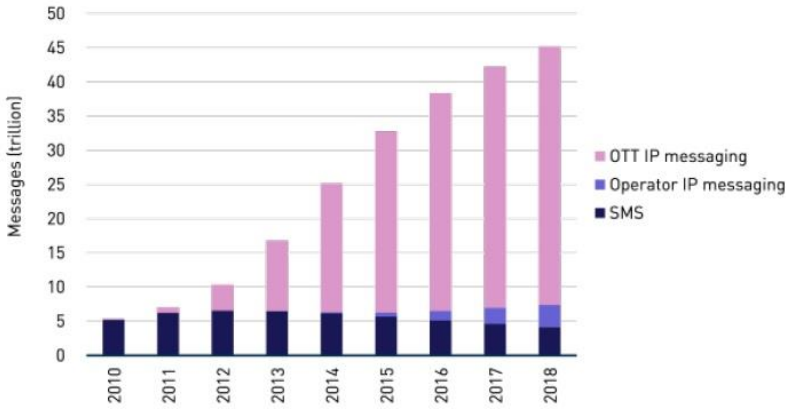
close substitutes to the corresponding services offered by telecom providers.[22] Well-known substitutes for both traditional SMS and MMS services are Whatsapp, Apple's iMessage, Facebook Messenger, Twitter and Instagram, while Skype, Viber, Apple's FaceTime and Google's Voice/Hangout are well-known substitutes for traditional voice services.

As has been observed by CERRE (Centre on Regulation Europe), the increase of OTT messaging and call volumes has been enormous over the last years, as is illustrated by the following figures:



Source: CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 16.

Whilst in 2010 OTT messages in Western Europe only accounted for **8,31%** of overall messaging traffic, this number has increased to not less than **66,96%** in 2013.[23] Due to the still increasing popularity of smartphones, the ease of installing mobile voice, messaging and video services as applications on such devices and the increasing availability of stable mobile broadband services, the European Parliament expects that the popularity of OTT communication services will only increase significantly, as becomes clear from the following diagram:



Source: DG for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 31.

[22] Synopsis report on the public consultation on the evaluation and review of the regulatory framework for electronic communications, https://ec.europa.eu/digital-single-market/en/news/full-synopsis-report-public-consultation-evaluation-and-review-regulatory-framework-electronic.

[23] Data cited in CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 15, http://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf.

On the basis of the identified trends, OTT messaging is even forecasted to reach a market share of **90%** of the total messaging market in **2020**.[24]

In addition, also international voice services show a strong uptake of OTT services, although the effect is not as overwhelming as in messaging. In 2013, the international traffic volume carried by Skype grew 36 percent to 214 billion minutes, while the international telephone traffic (both fixed and mobile) carried by telecom operators in that year only grew 7 percent to 547 billion minutes.[25] One reason for this still limited substitution may refer to specific characteristics that are ensured by communication services offered by telecom providers. Some consumers highly value the offering of phone numbers that allow any-to-any connectivity with other providers, end-to-end quality or reliable emergency services.

In regard of the market evolutions and trends presented above, the presence on the market of OTT players and OTT services providing consumers a functional substitute for traditional telecommunications services can no longer be ignored.

2.3 Time to act

Taking into account (i) that there is a consensus on the need to evaluate and revise the ePrivacy Directive in its current form and (ii) that the changing market illustrates the increasing presence of OTT players on the telecom market, a momentum for action undeniably exists and has existed already for some time.

As stated earlier, ETNO believes it would have made more sense from an efficiency perspective to revise and repeal the ePrivacy Directive through the GDPR, rather than dealing with one review after the other, and thus postponing any and all discussions on the ePrivacy Directive until after the adoption of the GDPR.

That being said, we believe that there is still time to correctly adapt the e-Privacy regime so as to enhance consumer trust, legal certainty and to achieve the objective of efficient regulation. ETNO urges this to happen by 25 May 2018, which is the date as from which the GDPR will apply. In the absence thereof, if there were too much time between the entry into force of the GDPR and the closing of the revision of the ePrivacy Directive, operators would continue to face dual compliance regimes as a result of which their competitive position will be compromised, possibly until 2020. This will merely exacerbate existing market distortions and weaknesses in consumer privacy protection.

For telecom providers it is already five to twelve. Therefore the Commission is urged to speed up the process of revising the ePrivacy Directive and come up with legislative proposals in the coming months that address all issues and problems surrounding the current ePrivacy Directive. Although there is a need for a revision on the short term, it cannot be stressed enough that there also is a big need for a thorough assessment, evaluation and revision of the ePrivacy Directive. Therefore, the Commission should not limit its legislative efforts to a cosmetic clean-up exercise or to a mere extension of the scope of the ePrivacy Directive. Instead, the Commission should tackle all challenges, inconsistencies and unjustified differences that exist and should more importantly dare to question the need and relevance of the existence of the ePrivacy Directive as such.

[24] Directorate-General for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 31, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.
[25] Directorate-General for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 32, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

If no or no thorough legislative action is undertaken, it will have considerable negative consequences, and notably impact the level of legal (un)certainty for consumers, the continued existence of an unlevel playing field and a dual compliance regime, which is likely to lead to a fragmented market. As will be further detailed in the next section, at least those considerations are to be tackled during the revision of the ePrivacy Directive.

3 LONG-TERM OBJECTIVES

The EU needs to create an environment that encourages data driven innovation in Europe and put in place a regulatory framework supporting said idea, notably with the aim to (i) build consumer trust by reducing regulatory complexity, (ii) restore the level playing field and (iii) create a consistent legal framework.

As the GDPR has been agreed upon in April 2016, it is now time for an urgent evaluation of the ePrivacy Directive. In regard of the identified market and legislative evolutions, the upcoming revision of the ePrivacy Directive has to be seen as an instrumental step to repealing the ePrivacy Directive with the aim to achieve the goals and objectives further detailed in this section.

3.1 Building consumer trust by reducing regulatory complexity

From a user experience and market perspective, communication services provided by telecom providers and by OTT players are close substitutes. And from a data protection perspective, not only services provided by telecom providers but also by OTT services falling outside the scope of the ePrivacy Directive store vast amounts of personal information, identifiers, traffic and location data, however without being regulated in the same way as telecom providers.

As illustrated by a recent survey conducted by ComRes, consumers and data subjects are not fully aware of the differences and inconsistencies in data protection standards between traditional voice and SMS services on the one hand and OTT voice and messaging services (such as Skype and WhatsApp) on the other hand.[26] When SMS functionality and OTT messaging functionality are integrated into one mobile application, whereby the choice as to whether a message is sent as a traditional SMS or as an OTT message is not with the user but with the smartphone software, it becomes even more difficult to justify and explain to the user that different legal regimes apply, depending on the choice made by the smartphone.

As the GDPR provides a future-proof framework for the protection of personal data, the existence of diverging privacy-related provisions in the ePrivacy Directive can no longer be justified and would mean that the GDPR does not reach its objectives. Such dual data protection regime inevitably leads to increased legal uncertainty and an asymmetry of data protection and privacy laws, and leaves consumers to assess which rules and rights apply to functionally-equivalent services.

In addition, the coexistence of two different sets of rules creates confusion for consumers, which does not play in favour of a coherent consumer policy online. Hence, to build trust and increase legal certainty for consumers, it is key to reduce the regulatory complexity and simplify the applicable legal framework, which can be done by applying the same data protection rules to all market players, independent of the sector in which they are active and of which technology is being used.

[26] ComRes, “Digital consumer Survey”, September 2015, www.etno.eu.

Key message

Consumers face inconsistent privacy experiences for functionally-equivalent services, often without being fully aware. To resolve the legal uncertainty, similar data protection rules should be applied to similar services. Only a consistent set of rules for consumers and industry will provide the required legal certainty, avoiding overlapping provisions (confusing for consumers and service providers and without added value for the protection of privacy) and stimulating innovative services in a responsible way in the EU.

3.2 Restoring the level playing field

Although telecom providers and OTT players increasingly compete for the same public, they are currently not subject to the same rules. While specific data protection rules for telecom operators may have been justified in the past, today, it makes little sense to single out one particular sector when there are such a broad range of online service providers collecting and processing large volumes of personal data. As has been demonstrated by a recent study published by CERRE[27], today, there is little economic rationale for treating OTT players offering communication services (such as Skype and Whatsapp) differently and imposing different privacy and data security requirements to telecom providers and OTT players.

Moreover, while it would make sense to impose additional obligations for the processing of sensitive data (such as medical data, which is also recognised as such under Art. 9 of the GDPR), it can even be considered discriminatory to apply additional rules to one specific sector irrespective of the data processed, without there being a justification for such different treatment. In this regard, a second and more recent study published by CERRE on consumer privacy in network industries states that a future proof regulation requires a common approach to all industries and that sector-specific privacy regulations are inadequate in a dynamic environment and should be withdrawn.[28] When it comes to network industries, CERRE considers the existence of sector-specific data protection legislation to be problematic for a number of reasons, notably because (i) it is likely to lead to inconsistencies and create legal uncertainty due to conflicting provisions in sector-specific and general privacy regulation, (ii) the definition of the scope of sector-specific legislation almost invariably leads to boundary problems in the application thereof, and (iii) it is likely to distort competition. Applied to the ePrivacy Directive, it must be observed that all the identified issues are present in the context of the ePrivacy Directive.

By maintaining one set of data protection rules that apply in the same way to telecom providers, OTT players as well as all other data controllers, the level playing field between different services providers can be restored.

It cannot be denied that the ongoing review of the ePrivacy Directive is the opportunity that must be seized to achieve a true level playing field in order to ensure that technology-neutral principles apply to all

[27] CERRE, "Study on Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", http://www.cerre.eu/sites/default/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final_0.pdf.

[28] CERRE, "Consumer privacy in network industries, a CERRE policy report", http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf.

stakeholders. This is also a key element in the debate towards promoting the internal market and achieving increased competitiveness. In the current converged world, the distortions between sectors are not justifiable and it is necessary to avoid competition distortions among the players of the digital ecosystem.

As the use of OTT services augmented significantly over the last years and as this growth is expected to increase exponentially in the coming years, there is an urgent need to level the playing field rather soon than late, in the absence of which the legislative intervention might be 'too little, too late', and domestic telecom providers are very likely to lose ground to – mainly US-based – OTT players. Hence, if the European Union wants telecom providers to compete with OTT players on an equal level, notably in the field of big data which the European Commission sees as central to the digital economy and growth path, then legislative action may no longer be postponed.

Key message

By having/maintaining one set of data protection rules that applies to all data controllers and data processors, notwithstanding the sector in which they are operating, the level playing field between telecom providers and OTT players can be restored.

3.3 Ensuring consistency

Today, the legal framework applicable to telecom operators and other data controllers is characterised by a number of inconsistencies and unjustified differences that should be addressed during the revision of the ePrivacy Directive:

- A number of highly relevant topics such as the security of data processing (including data breach notifications), the treatment of location data and the treatment of traffic data are governed in a comparable but different way between the GDPR and the ePrivacy Directive. These differences do not only result in an unlevel playing field between telecom operators and OTT players but also cause telecom operators to be confronted with a dual compliance regime.
- As most provisions of the ePrivacy Directive are not applicable to OTT players, there is a risk that if no legal action is undertaken at a European level to dissolve the current asymmetry, it is to be expected that Member States will start regulating OTT players on a national level, leading to a fragmentation of the market and a patchwork of diverging national legislations. In this regard it should be emphasised that Finland is already engaging in unilateral efforts to address the regulatory asymmetry created by the co-existence of the Data Protection Directive and the ePrivacy Directive. Finland in particular adopted its 'Information Society Code' – which entered into force on 1 January 2015 – pursuant to which OTT players are subordinated to a more stringent set of obligations. This legislation will amongst others oblige social media platforms to ensure the confidentiality of messages exchanged over their messaging services. If more Member States follow suit, this will add further uncertainty for business and consumers and will lead to further inconsistency and lack of harmonised regulation. It underscores again the urgency of addressing this matter.
- Due to diverging ways in which Member States have implemented key provisions of the ePrivacy Directive, it must be observed that there are significant inconsistencies in the way in which Member

States have for instance regulated the confidentiality of communications and the use of cookies as well as in the legislative instruments (telecom, data protection or consumer protection legislation) that have been chosen for the implementation of the ePrivacy Directive.

Key message

To ensure consistency, the idea of having a dual data protection regime consisting of diverging rules in the GDPR and the ePrivacy Directive needs to be abandoned.

4 HOW THE REVISION OF THE EPRIVACY DIRECTIVES FITS IN THE LONG-TERM OBJECTIVES

Against the background of the long-term objective of repealing the ePrivacy Directive, as detailed in Section 3 of this Study, this Section further explains how the upcoming revision of the ePrivacy Directive fits into that long-term objective (*Section 4*). More in particular an analysis will be made of the key provisions of the current ePrivacy Directive, notably of the privacy-related provisions that overlap with the GDPR (*Section 4.1*), the privacy-related provision that requires a clarification (*Section 4.2*) and the non-privacy-related provisions of which the need and relevance can be questioned (*Section 4.3*). For each topic, a recommendation will be formulated that is to be taken into account when evaluating and reviewing the ePrivacy Directive.

4.1 Overlap with the GDPR

In this section the most important inconsistencies and unjustified differences that are created by the co-existence of and overlap between a horizontal data protection regime and a sector-specific regime focused on the telecom sector will be further detailed.

4.1.1 Security of processing

4.1.1.1 Security

Article 4(1) of the ePrivacy Directive (*Security of processing*) obliges telecom providers to take appropriate technical and organisational measures to safeguard the security of their services, having regard to the state of the art and the cost of their implementation. In accordance with Article 4(1.a) those measures shall at least (i) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, (ii) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and (iii) ensure the implementation of a security policy with respect to the processing of personal data.

This Article 4 of the ePrivacy Directive is highly similar to Article 32 of the GDPR (*Security of processing*), which obliges data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, while taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. These measures shall including inter alia as appropriate (i) the pseudonymisation and encryption of personal data, (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

As both Article 4(1) and Article 4(1.a) of the ePrivacy Directive as well as Article 32 of the GDPR focus on the security of personal data, there undeniably is an overlap between both instruments that cannot be justified or that at least is no longer required. As the data processing security obligations included in the

GDPR offer the same or even a higher level of protection as the ones included in the ePrivacy Directive, it makes more sense to only retain that more advanced and horizontal regime.

Moreover, in the unlikely event that Article 4 of the ePrivacy Directive would erroneously be interpreted as not being limited to the security of personal data processing but would concern the security of electronic communications services in general, it should be stressed that Articles 4(1) and 4(1.a) of the ePrivacy Directive can still be repealed, as such obligations are already included in Article 13.a of the Framework Directive obliging telecom providers to take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services, whereby those measures shall ensure a level of security appropriate to the risk presented. This Article 13.a also obliges telecom providers to notify the competent national regulatory authority of a security breach that has had a significant impact on the operations of networks or services.

Key message

Maintaining dual rules on the security of personal data processing would create an overly complex situation requiring telecom providers to comply with two set of rules, depending of the activities involved. Hence, as the regime currently included in the GDPR offers the highest level of protection, only this one should be retained.

4.1.1.2 Data breach notifications

For many years the European Data Protection Supervisor advocated for the extension of the applicability of the data breach notification rules set out in Article 4 of the ePrivacy Directive to a wider scale of data controllers (notably providers of information society services) and to other sectors than the telecom sector. Indeed, the reasons that justify imposing the data breach notification obligation upon telecom providers also exist regarding other organisations processing massive amounts of personal data of which the disclosure may be particularly harmful to data subjects (e.g. online banks, data brokers and online providers processing health data or other sensitive data).[29]

The European Commission answered the European Data Protection Supervisor's call and included in the GDPR articles on the security of processing (Art. 32 GDPR), the obligation to notify data breaches to the supervisory authority (Art. 33 GDPR) and to data subjects (Art. 34 GDPR). The principles set out in those articles are clearly based upon Article 4 of the ePrivacy Directive and on Regulation 611/2013 in which the principles of Article 4 of the ePrivacy Directive are further developed. This is even explicitly confirmed by the European Commission by noting that at the time data breach notification obligations were only compulsory in the telecommunications sector.[30]

[29] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, 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), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf.

[30] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Safeguarding Privacy in a Connected World, A European Data

Although the European legislator already indicated during the discussions on the GDPR that the data breach notification regime included in the GDPR should be consistent with the ePrivacy Directive, this clearly is not the case:

- While a data controller under the GDPR, where feasible, has 72 hours to notify a data breach to the supervisory authority, a telecom provider under the ePrivacy Directive only has 24 hours to notify a data breach to the 'competent national authority' (whereby it is uncertain whether the 'competent national authority' is the national telecom regulator or national data protection authority);
- Where a data controller under the GDPR cannot provide all the information required within 72 hours, he may provide some specific information later "*without undue further delay*", while if a telecom provider under the ePrivacy Directive cannot provide all information required within 24 hours, he is only granted a 'grace period' of 3 days for some specific information;
- While a data controller under the GDPR needs to notify a data breach to the supervisory authority "*unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons",* a telecom provider will under the ePrivacy Directive need to notify every breach to the competent national authority; and
- While a data controller under the GDPR needs to notify a data breach to the concerned data subject in case of a "*high risk for the rights and freedoms of natural persons*", a telecom provider will under the ePrivacy Directive need to notify a data breach to the subscriber in case of a "*particular risk for the security of the network*".

Although the data breach notification regime included in the GDPR is based upon the regime set out in the ePrivacy Directive (as further specified in Regulation 611/2013), there are a number of differences that are unjustified. A dual data breach notification regime will lead to complexity for telecom operators who will have to assess for each data breach event which notification procedure they have to apply (e.g. application of the GDPR principles for cloud services, application of e-Privacy Directive principles for internet access services, and uncertainty in relation to events that affect both types of services). Moreover, due to the diverging implementation of the ePrivacy directive in national law, currently in a number of Member States telecom providers are obliged to notify data breaches to different regulators (notably data protection authorities and telecom regulators), which even increases the regulatory complexity for actors in those Member States.

There are no objective reasons to maintain such differences and to create operational complexity, Hence, Article 4 of the ePrivacy Directive and Regulation 611/2013 should be entirely repealed and substituted by the corresponding articles of the GDPR.

Key message

Maintaining dissimilar data breach notifications rules would create an overly complex situation for telecom providers, data subjects, stakeholders and regulating authorities. Hence, only the regime currently included in the GDPR should be retained.

Protection Framework for the 21st Century", COM(2012) 9 final, 25 January 2012, 6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF.

4.1.2 Location data

The ePrivacy Directive contains a specific regime for the processing of location data (other than traffic data). This regime may have made sense in 2002, when such data were still somewhat specific to the telecom sector, but since then the situation has changed significantly, and OTT players are now collecting vast amounts of location data for the performance of their online VOIP and messaging services.

In accordance with Article 9 of the ePrivacy Directive, telecom providers may process location data when they are made anonymous or with the consent of the users/subscriber insofar as necessary to provide a value added service. Moreover, users/subscribers must be informed prior to obtaining their consent of the type of location data that is being processed, of the purposes and duration of the processing and of whether the data will be transmitted to a third party (for providing the value added service). Finally, users/subscribers need to be given the opportunity to withdraw their consent at any time.

Whereas in the past there might have been uncertainty as to whether location data are personal data, the GDPR has taken away all doubts in this respect by including an explicit reference to 'location data' in the definition of 'personal data' (Art. 4(1) GDPR). Consequently, data controllers processing location data – that allow to identify a data subject directly or indirectly – will need to comply with the provisions of the GDPR.

With regard to the processing of personal data, the Article 29 Working Party adopted in 2011 an opinion on geolocation services on smart mobile devices, in which it observed that with the rapid technological development and wide uptake of smart mobile devices, a whole new category of location based services is developing. In this respect, the Article 29 Working Party explicitly confirmed that the Data Protection Directive applies in every case where personal data are being processed as a result of the processing of location data, whereas the ePrivacy Directive only applies to the processing of location data (for example base station data) by telecom providers.[31] Hence, it is clear that the ePrivacy Directive does not apply to the processing of location data by information society services, such as for example Skype and Whatsapp.

It is interesting to note that the Commission today still seems to be of the opinion that an 'enhanced' protection of location data under the ePrivacy Directive remains justified by the fact (i) that such data, in particular when stored over time, allow very precise conclusions to be drawn concerning the private lives of individuals and (ii) that the needs of a modern society require that people have access to electronic communication services for most part of their daily lives.[32] Furthermore, the authors of the Commission Study state that it is difficult to justify why location data should receive different legal protection if they are processed in the context of very similar services from a functional perspective. Therefore, to ensure consistency and a level playing field, they propose to extend the scope of the provision on location data to publicly available services in public or publicly accessible private communications networks in the Union, including information society services.[33]

---

[31] Article 29 Working Party, "Opinion 13/2011 on geolocation services on smart mobile devices", WP 185, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

[32] European Commission, "Background to the public consultation on the evaluation and review of the ePrivacy Directive", 9, https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review.

[33] P. 81-82 of the final report of the study "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071), as prepared for the European Commission, https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

Treating location data that are processed in the context of functionally-equivalent services differently can indeed no longer be justified, as for instance precluding telecom providers from engaging in data analytics while OTT providers would be allowed to so leads to a competitive disadvantage for the first category. Although we understand the need for a high level of protection and support the idea of levelling the playing field, extending the scope of the ePrivacy Directive to information society services does not seem to be the right approach:

- As set out above, sector-specific data protection legislation is to be avoided and the main aim should be horizontal data protection legislation applying throughout all sectors. Hence, extending the scope of the ePrivacy Directive from the telecom sector to the entire online industry, does not seem the right way forward, to the contrary.

- Including information society services in the scope of the ePrivacy Directive would also be surprising and strange in regard of the recent adoption of the GDPR. The main aim of the GDPR is to make the European data protection rules fit for a digital world, hence notably for the rise of amongst others location-based services and other online services (of which most qualify as information society services).

  As is confirmed by a recent study on online privacy[34], providers of information society services, such as social network services, search engines, webmail and messaging and mobile apps, that are only subject to the GDPR process a vast amount of data allowing to draw very precise conclusions as to the private life of its users and allowing unique insights into user activity that go significantly further than what for instance telecom providers can do. For example, the location data generated by such information society services are far more precise than the location data generated at the level of an antenna cell in a mobile network. Nonetheless the European legislator clearly did not consider it necessary to include in the GDPR specific rules on the processing of location data through information society services, although a number of specific rules on information society services have been included in the GDPR (e.g. Art. 8 GDPR).

  In other words, extending the scope of the ePrivacy Directive to the entire online sector would imply that the GDPR, as recently adopted, is already no longer considered as an appropriate tool to achieve its goal, notably offering a high level of protection in a digital age.

As already confirmed by the authors of the Commission Study, there no longer is a justification for treating telecom providers processing location data different from OTT players processing location data. However, contrary to what has been suggested in that study, we propose to delete the specific provision of the ePrivacy Directive with regard to location data and apply the horizontal regime of the GDPR to all location data being processed, notwithstanding the technology used and the actor involved.

Taking into the account the above considerations, and when analysing Article 9 of the ePrivacy Directive in light of the text of the GDPR, it must be observed that repealing the specific rules on the processing of location data set out in Article 9 of the ePrivacy Directive will not lead to a decrease of the level of protection offered to users of communication services:

[34] P. SWIRE, J. HEMMINGS, A. KIRKLAND, "Online privacy and ISPS: ISP Access to Consumer Data is Limited and Often Less than Access by Others", A Working Paper of The Institute for Information Security and Privacy at Georgia Tech, 29 February 2016, http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.

- "*Location data (…) may only be processed when they are made anonymous, or with the consent of the users or subscribers"* (Art. 9(1) EPD) – Although Article 6 of the GDPR contains six grounds for the lawful processing of personal data, allowing telecom providers to invoke each of those grounds to process location will not reduce the level of protection offered to data subjects. It cannot be denied that the GDPR foresees high standards for data protection. Moreover, as set out above, it makes no sense to limit the abilities of telecom providers to process location data compared to other market players.

  Although there are no legitimate reasons for limiting the legal grounds on the basis of which telecom providers are allowed to process location data, it is important to bear in mind that in practice consent will be the main applicable ground for processing location data. In this regard, the Article 29 Working Party confirmed that while telecom providers today must always obtain the user/subscriber's prior consent, the prior informed consent is also the main applicable ground for making data processing legitimate when it comes to the processing of the locations of a smart mobile device in the context of information society services.[35]

- "*Location data (…) may only be processed when they are made anonymous, or with the consent of the users or subscribers"* (Art. 9(1) EPD) – When the consent of the user/subscriber has not been obtained, location data may only be processed when they are made anonymous. Important to stress is that Article 9 of the ePrivacy Directive has been drafted to govern the processing of location data that is not at the same time traffic data, as Article 6 already allows the processing of location data included in traffic data for the purpose of transmitting a communication. Hence, in that regard, it should be emphasised that when location data would be processed for other purposes than transmitting a communication the GDPR contains safeguards equivalent to Article 9 of the ePrivacy Directive. In accordance with the 'purpose limitation' principle (Art. 5(1)(b) of the GDPR) personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. Moreover, in respect of the further processing of personal data for other purposes than for which they have been collected (e.g. transmitting a communication), Article 6(4) of the GDPR sets out a strict compatibility assessment that needs to be performed. As part of that assessment the GDPR requires that appropriate safeguards, such as encryption or pseudonymisation of personal data, enhancing the data subjects' privacy are put in place. This means that if data controllers would process location data under the GDPR for other purposes than for which they were collected, they should pseudonymise or encrypt those data.

- "*Location data (…) may only be processed (…) to the extent and for the duration necessary for the provision of a value added service"* (Art. 9(1) EPD) – The Commission is in particular concerned that location data, when stored over time, allow very precise conclusions to be drawn concerning the private lives of individuals. This concern however does not appear to be valid in regard of the GDPR. In accordance with the 'data minimisation' principle (Art. 5(1)(c) GDPR) the processing of personal data needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Moreover, in accordance with the 'storage limitation' principle (Art. 5(1)(e) GDPR), personal data may only kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In practice this means that data controllers may only collect personal data they really need and may only keep it for as long as they need

[35] Article 29 Working Party, "Opinion 13/2011 on geolocation services on smart mobile devices", WP 185, 13, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

it. Or in other words, personal data should be anonymised or deleted when the processing of the data is no longer lawful.

- "*The service provider must inform the users or subscribers prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added services." (*Art. 9(1) EPD) – This paragraph is a mere confirmation of the principles laid down in the GDPR. In accordance with the Articles 13 and 14 of the GDPR, data controllers have a transparency obligation and are required to provide data subjects with information on the processing of personal data, including on the purposes of the processing, the period for which the personal data will be stored and the recipients or categories of the recipients of personal data.

- *"User or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time."* (Art. 9(1) EPD) and "*Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscribers must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication*" (Art. 9(2) EPD) – These paragraphs are a mere concretisation of Article 7(3) GDPR. That Article specifies that – when the processing is based on the data subject's consent – the data subject shall have the right to withdraw his or her consent at any time and that it shall be as easy to withdraw as to give consent.

- "*Processing of location data (...) must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications services or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service."* (Art. 9(3) EPD) – This paragraph containing specific requirements as to the security and confidentiality of the processed data is a concretisation (i) of the specific obligation for data controllers and data processors to take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller (Art. 32(4) GDPR) and (ii) of the more general obligation to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality', Art. 5(1)(f) GDPR).

Key message

In a converged communications landscape, a different treatment of location data processed by telecom providers on the one hand and other data controllers (including OTT players) on the other hand can no longer be justified. As the general principles on the collection of personal data as currently set out in the GDPR offer a similar and equally high level of protection for consumers, Article 9 EPD should be repealed.

4.1.3 Traffic data

A specific regime for the processing of traffic data has already been included in 1997 in the Telecommunications Data Protection Directive (the predecessor of the ePrivacy Directive), at a time wherein telecom providers were collecting data that was deemed to be unique to that sector. Traffic data – which may comprise location data – are thus governed by specific rules, even if somewhat "lighter" than the rules applicable to location data (other than traffic data) which are referred to in Section 4.1.2 (*Location data*) above.

More particularly, in accordance with Article 6 of the ePrivacy Directive, traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Telecom providers may however process traffic data for the provision of value added or marketing services with the prior consent of the user/subscriber. Moreover, the user/subscriber must be informed prior to obtaining their consent of the type of traffic data that is being processed and of the purposes and duration of the processing. Finally, users/subscribers need to be given the opportunity to withdraw their consent at any time.

The GDPR does not contain any explicit reference to traffic data in the non-exhaustive list of examples for personal data (Article 4 (1) GDPR). Such data however must be qualified as personal data:

- Article 2 b) of the ePrivacy Directive defines traffic data in a broad way as "*any data processed for the purpose of the conveyance of a communication on an electronic communications networks or for the billing thereof*". In the background document to the public consultation, the Commission lists the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services as key examples of traffic data.[36] As those data allow to identify data subjects, they all qualify as personal data.

- The Data Retention Directive – which has been invalidated by the European Court of Justice of the European Union[37] – required the retention of following categories of data: data necessary to trace and identify the source and destination of a communication, data necessary to identify the date, time and duration of a communication, data necessary to identify the type of communication, data necessary to identify user's communications equipment or what purports to be their equipment and data necessary to identify the location of mobile communication equipment. In its judgment the Court explicitly considered that the listed data – which are all traffic data – qualify as personal data.[38]

- In an opinion prepared by the Article 29 Working Party in the context of an earlier revision of the ePrivacy Directive, the Article 29 Working Party explicitly stated that "*the processing of traffic data falls within the scope of the Data Protection Directive*".[39] Although the restrictions of the current Article 6 of the ePrivacy Directive are different, this key conclusion remains valid.

[36] European Commission, "Background to the public consultation on the evaluation and review of the ePrivacy Directive", 9, https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review.

[37] CJEU 8 April 2014, C-293/12 and C-594/12, 29, www.curia.eu.

[38] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ.L.*105, 13 April 2006, 54-63.

[39] Article 29 Working Party, "Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)", WP 159, 7, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf.

As to the necessity of stricter rules for the processing of traffic data by telecom providers, the Commission and the authors of the Commission Study have the same view as set out in Section 4.1.2 (*Location data*) above. Hence, the arguments developed to counter such view, as set out in the above Section, apply *mutatis mutandis* to the processing of traffic data.

In line with our arguments in support of repealing the specific treatment of location data, we propose to delete the specific provisions of the ePrivacy Directive with regard to traffic data and apply the horizontal regime of the GDPR to all traffic data being processed, notwithstanding the technology used and the actor involved.

As we demonstrated above that it is feasible that the more strictly regulated category of location data would only be governed by the GDPR, this *a fortiori* is the case for the less strictly regulated category of traffic data. More in particular, taking into account the considerations set out in Section 4.1.2 (*Location data*) and when analysing Article 6 of the ePrivacy Directive in light of the text of the GDPR, it must be observed that repealing the specific rules on the processing of traffic data set out in Article 6 of the ePrivacy Directive will indeed not lead to a decrease of the level of protection offered to users of communication services:

- "*Traffic data (…) must be erased or made anonymous when it is no longer needed for the purpose of the transmissions of a communication"* (Art. 6(1) EPD) – As set out above with regard to the processing of location data, the 'storage limitation' principle (Art. 5(1)(e) GDPR) provides equivalent safeguards.

- "*Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may be lawfully challenged or payment pursued"* (Art. 6(2) EPD) – This Article is a mere application of Article 6 of the GDPR on the lawfulness of processing. Indeed, in accordance with Article 6(1)(b) of the GDPR, personal data may be processed when necessary for the performance of a contract to which the data subject is party, and the processing of traffic data would be permitted for the purposes of billing a subscriber under a contract and handling interconnection payments. Moreover, in accordance with the 'storage limitation' principle (Art. 5(1)(e) GDPR), traffic data may indeed no longer be processed when this would no longer be needed for the intended purposes.

- "*For the purpose of marketing electronic communications services or for the provisions of value added services, the provider (…) may process the data (…) to the extent and for the duration necessary for such services or marketing."* (Art. 6(3) EPD) – As set out above with regard to the processing of location data, the 'data minimisation' principle (Art. 5(1)(c) GDPR) and the 'storage limitation' principle (Art. 5(1)(e) GDPR) provide equivalent safeguards.

- *"For the purpose of marketing electronic communications services or for the provisions of value added services, the provider (…) may process the data (…) 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."* (Art. 6(3) EPD) – As set out above with regard to the processing of traffic data, there are no legitimate reasons for limiting the legal grounds on the basis of which telecom providers would be allowed to process traffic data. More in particular, as to the marketing of electronic communications services, there is no objective justification for excluding the legitimate interests ground (Art. 6(f) GDPR) –

as endorsed by the Article 29 Working Party[40] – and deviating from the general opt-out mechanism for direct marketing as set out in Article 21 of the GDPR

- *"User or subscribers shall be given the possibility to withdraw their consent for the processing of data at any time."* (Art. 9(1) EPD) – This paragraph is a mere concretisation of Article 7(3) GDPR, which specifies that – when the processing is based on the data subject's consent – the data subject shall have the right to withdraw his or her consent at any time and that it shall be as easy to withdraw as to give consent.

- *"The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3."* – As set out above with regard to the processing of location data, this specific obligation is a mere confirmation of the transparency principles laid down in the Articles 13 and 14 of the GDPR.

- "*Processing of traffic data (…) must be restricted to persons acting under the authority of providers of the public communications networks and publicly available communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added services, and must be restricted to what is necessary for the purposes of such activities." (*Art. 6(5) EPD) – In line with what has been set out with regard to the processing of location data, this Article is a mere concretisation of the security and confidentiality obligations included in the Articles 5(1)(f) and 32(4) of the GDPR.

  "*Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes*" (*Art. 6(6) EPD*) – To the extent a law would oblige a telecom provider to share traffic data with a regulator with a view to settling disputes, the GDPR would allow such processing of traffic data in accordance with its Article 6(1)(c), allowing the processing of personal data when this is necessary for compliance with a legal obligation to which the data controller is subject.

Key message

In a converged communications landscape, a different treatment of traffic data processed by telecom providers on the one hand and other data controllers (including OTT players) on the other hand can no longer be justified. As the general principles on the collection of personal data as currently set out in the GDPR offer a similar and equally high level of protection for consumers, Article 6 EPD should be repealed.

[40] Art. 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC", WP 217, 25, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

4.1.4 Cookies and other tracking mechanisms

In 2009, the European legislator adopted the so-called Cookie Directive[41], which modified the ePrivacy Directive. Different from the previous version of the ePrivacy Directive which was based on an opt-out requirement, the Cookie Directive introduced in Article 5(3) of the ePrivacy Directive an opt-in requirement for the use of cookies and related technologies in the terminal equipment of a subscriber or user (e.g. computers, smart phones, etc.), hence requiring the free, specific, informed and unambiguous consent for installing cookies.[42]

Although the aim of the ePrivacy Directive has initially been to harmonise the processing of personal data in the telecom sector, it should be noted that this cookie provision (i) applies to all website operators placing cookies and similar technologies and as such is not limited to the telecom sector and (ii) failed to reach its harmonisation objective, as the cookie provision has been implemented in national laws by Member States in diverging ways.

Furthermore, it is difficult to deny that the consent rule did not reach its objective, which is most likely due to the fact that users are currently receiving a warning message about the use of cookies on almost every website. The impact of such warning messages would considerably increase if they would only appear when websites contain cookies that are not related to the purpose for which the user is navigating on the said website (e.g. third party advertising cookies).

The relevance and need of the cookie provision can be questioned in light of the text of the GDPR. Whereas before it often has been argued that cookies do not constitute personal data – and thus are not directly subject to the Data Protection Directive – this has changed with the introduction of the GDPR. In the GDPR the definition of 'personal data' has been enlarged, and now includes an explicit reference to 'online identifiers' (Art. 4(1) GDPR). Moreover, Recital 30 of the GDPR further specifies that "*natural persons may be associated with online identifiers (…) as internet protocol addresses, cookie identifiers or other identifiers, such as radio frequency identification tags*", and that such online identifiers "*may leave traces which, in particular when combined with unique identifiers and other information received by the servers may be used to create profiles of the natural persons and identify them*".

It follows from the above that cookies or other identifiers that are uniquely linked to a device and capable of identifying a natural persons or singling him or her out (even without identifying) are to be considered as personal data, and are thus subject to the provisions of the GDPR. Only subjecting the use of those cookies to the provisions of the GDPR instead of to specific rules would allow to remedy the difficulties surrounding the current consent rule. As under the GDPR, consent would not be the only available ground for lawful processing, website operators could justify the placing of cookies on other legal grounds as well, i.e.:

[41] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&rid=3.

[42] However, two derogations to the consent rule exist. One exception concerns information used (i) "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network*", and the other exception covers information which is (ii) "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

- Placing cookies for carrying out the transmission of a communication over a communications network or for allowing an information society provider to provide a service – as currently exempted from the consent rule by Article 5(3) of the ePrivacy Directive – could become possible under Article 6(1)(b) of the GDPR, allowing the processing of personal data when necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract.
- Placing cookies for IT security or fraud detection could become possible under Article 6(1)(f) of the GDPR, allowing the processing of personal data when necessary for the purposes of the legitimate interests pursued.
- Placing first party cookies, such as session cookies, authentication cookies, user centric security cookies, load balancing cookies, etc., could also become possible under Article 6(1)(b) and/or Article 6(1)(f) of the GDPR.

The above would also be in line with the Article 29 Working Party's Opinion on cookie consent exemption[43] in which it stated that first party analytics cookies, such as listed in the third bullet above, do not require user's consent as they are not likely to create privacy risks. In that Opinion the Article 29 Working Party also stated that third party advertising cookies cannot be exempted from consent, as those cookies are more privacy-intrusive. We understand the Article 29 Working Party's concern in this regard. However, repealing Article 5(3) of the ePrivacy Directive is unlikely to have any adverse effects in this regard, as we fail to see how website operators would be able to install third party advertising cookies on other grounds than consent (Art. 6(1)(a) GDPR).

Moreover, it must be emphasised that cookies could be used for building detailed user profiles. In regard of profiling, which is defined as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*" (Art. 4(4) GDPR), the GDPR foresees a number of specific safeguards. Those safeguards include notably (i) the right for the individual not to be subject to decisions based solely on automated processing of his personal data; (ii) the need to inform individuals to the maximum extent possible about the profiling operations, the consequences of such profiling and the right of the individual to object to such processing; (iii) the need to have a legal basis for such processing; (iv) the required continuous validation of the profiles and the underlying algorithms; (vi) the necessity of providing human intervention were appropriate; and (vii) the prohibition for profiling measures to concern children. Moreover, data subjects can at any time object to the processing of their personal data for the purposes of profiling.

It follows from the above that there is undeniably an unnecessary overlap between the GDPR and the ePrivacy Directive with respect to the rules applicable to cookies or related technologies. As the provisions included in the GDPR offer the same or even an enhanced level of protection compared to the ones included in the ePrivacy Directive, it makes more sense to only retain that more advanced and horizontal regime. In particular, the GDPR already provides for a comprehensive protection of data subjects and allows to remedy the existing difficulties with the consent rule while still providing for appropriate safeguards, notably when third party advertising cookies are placed and cookies are placed for profiling purposes. .

[43] Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption", WP 194, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Key message

The cookie provision in its current form has not reached its intended objective. Moreover it has been implemented by Member States in diverging ways, leading to fragmented cookies rules. As cookies (that are capable of identifying a natural persons or singling him or her out) are covered by the GDPR and as the GDPR offers a high level of protection, there no longer is a need to keep a specific cookie provision in the ePrivacy Directive.

4.1.5 Unsolicited communications

Article 13(1) of the ePrivacy Directive sets forth the basic rule 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 notion of electronic email is defined more broadly than email as it is described 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*". Although the definition includes traditional voice and messaging services, it does not cover messages exchanged via information society services (such as Facebook, LinkedIn, Skype or Twitter).

Article 13(2) of the ePrivacy contains the only exception to Article 13(1). If service providers have acquired an end-user's contact details in the context of a sale of products or services, they can send direct marketing by e-mail to advertise their own similar products or services, provided that the end-user is given the possibility to object.

In relation to 'other forms of direct marketing', such as telephone calls for direct marketing purposes carried out by non-automated calling machines (i.e. individuals making calls), Article 13(3) of the ePrivacy Directive leaves some discretion to Member States. For such commercial communications, they are allowed to choose between either requiring the prior consent of the subscribers/users on the one hand, or giving the opportunity to subscribers/users to express their wish not to receive such communication. However, such a flexibility has led to discrepancies amongst the national legislation of the Member States.

Although the legislative efforts undertaken to protect consumers against the sending of unsolicited commercial communications (or 'spam') are appreciated, it can be questioned whether Article 13 of the ePrivacy Directive provides for additional safeguards that are not already provided by the GDPR and whether there are reasons to apply different rules to direct marketing, depending on the technology used.

Indeed, anyone using automated calling and communication systems without human intervention, fax and e-mail for direct marketing will inevitably need to process an online identifier of the recipient and thus process personal data. Hence, before a company could engage in unsolicited communications, it will need to ensure that there is a legal ground available for such processing. In this respect, the data subject's consent (Art. 6(1)(a) GDPR) will be the most common ground for the processing of personal data for direct marketing purposes. However, it should be remarked that Recital 47 of the GDPR specifies that the processing of personal data for direct marketing purposes may also be regarded as carried out for a legitimate interest. This however is only allowed to the extent the legitimate interests pursued by the data controller or by a third party are not overridden by the interests or fundamental rights and freedoms of the data subjects which

require protection of personal data (Art. 6(1)(f) GDPR). Important to emphasize is that this latter approach has been endorsed by the Article 29 Working Party, which states that data controllers may indeed have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalize their offers, and ultimately, offer products and services that better meet the needs and desires of the customers. In light of this, the Article 29 Working Party confirms that the legitimate interests of the data controller may be an appropriate legal ground to be used for online and offline marketing, provided that appropriate safeguards are in place (such as a workable mechanism to object).[44]

In regard of the foregoing, data controllers processing personal data for direct marketing purposes will be required to ask the data subject's consent or to take into account and protect the interests and fundamental rights of said data subjects, notably the reasonable expectations of data subjects, when the processing of data is based on the legitimate interests ground. In our view allowing data controllers to apply this last ground to engage in direct marketing, is unlikely to reduce the data protection standards. As the reasonable expectations of data subjects are to be taken into account, it will not be possible to base every form of direct communications on this ground. A concrete application of Art. 6(1)(f) GDPR could be the case in which data controllers may want to use personal data for direct marketing of its own similar products or services, and thus replace Article 13(2) of the ePrivacy Directive.

Moreover, the GDPR provides for additional and appropriate safeguards, as in accordance with Article 21 of the GDPR data subjects whose personal data are processed for direct marketing purposes shall have the right to object at any time to the processing of personal data concerning him or her for such marketing (including profiling to the extent that it is related to such direct marketing). In such case, the concerned personal data shall no longer be processed for direct marketing purposes. While the ePrivacy Directive today foresees in an opt-in mechanism, it must be observed that the application of the GDPR, which contains an opt-out mechanism, would lead to the same result as the one of the ePrivacy Directive since users will be able to object at any time to the processing of his/her personal data for direct marketing purposes.

As the direct marketing regime included in the GDPR offers an equivalently high level of protection as the Privacy Directive, there is no longer a need to put in place specific rules in the ePrivacy Directive.

Key message

To ensure a consistent application of the rules on unsolicited communications, the specific rules on unsolicited communications should be repealed, and only the horizontal rules on direct marketing included in the GDPR should apply.

4.2 Privacy-related provision requiring clarification

In this section we will further analyse the confidentiality of communications principle (Art. 5(1) EPD), which is the only privacy-related provision of the ePrivacy Directive that could still be considered as relevant, and discuss the clarifications that are required to said principle.

[44] Art. 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC", WP 217, 25, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

4.2.1 Confidentiality of communications

Article 5(1) of the ePrivacy Directive obliges Member States to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services. In particular, the listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users is prohibited. Article 5(2) of the ePrivacy Directive – introducing the so-called business exception – however offers Member States the possibility to allow the recording of communications when 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 (e.g. calls to call centres). Article 5 of the ePrivacy Directive further specifies that in any event the principle of confidentiality of communications does not prevent technical storage which is necessary for the conveyance of a communication.

In addition to the ePrivacy Directive, the confidentiality of communications is also guaranteed in accordance with constitutions of Member States and the international instruments relating to human rights, in particular Article 7 (*Respect for private and family life*) of the EU Charter on fundamental rights and Article 8 (*Right to respect for private and family life*) of the European Convention on Human Rights (ECHR). Contrary to Article 7 of the EU Charter, Article 8 ECHR does not contain an explicit reference to a right to communications. Nevertheless, in regard of the technological advancements registered in the field of communication, the European Court of Human Rights has adopted an evolutive interpretation of the word 'correspondence', and considers this concept also to cover (i) telephone conversations[45], including information relating to them, such as their date an duration and the numbers dialled[46], (ii) pager messages[47], (iii) electronic messages (e-mails) and information derived from the monitoring of personal Internet use[48], (iv) private radio communications (but not when it is on a public wavelength and is thus accessible to others)[49].[50]

In regard of the fact that the confidentiality of communications is already protected by the aforementioned legal instruments and that the GDPR also contains provisions on the confidentiality of data processing, the question can be raised whether Article 5 of the EPD still is required. In this respect the GDPR indeed specifies the following:

- The processing of personal data to the extent strictly necessary and proportionate for the purpose of ensuring network and information security, inter alia the ability of a network or an information system to resist accidental events or unlawful or malicious actions that compromise the confidentiality of stored or transmitted personal data and the security of the related services offered by amongst others providers of electronic communication networks and services constitutes a legitimate interest of the data controller concerned (Recital 49 GDPR).

- In order to maintain security of processing systems and services and to prevent processing in infringement of the GDPR, the controller or processor needs to evaluate the risk inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should in any event ensure an appropriate level of security, including confidentiality, taking into account the state

[45] *ECHR, Malone v. the United Kingdom,* 2 August 1984, hudoc.echr.coe.int.
[46] ECHR, *P.G. and J.H. v. the United Kingdom*, 25 September 2001, hudoc.echr.coe.int.
[47] ECHR, *Taylor-Sabori v. the United Kingdom,* 22 October 2002, hudoc.echr.coe.int.
[48] ECHR, *Copland v. the United Kingdom*, 3 April 2007, hudoc.echr.coe.int.
[49] ECHR, *Camenzind v. Switzerland* and *B.C. v. Switzerland*, 27 February 1984, hudoc.echr.coe.int.
[50] I. ROAGNA, "Protecting the right to respect for private and family life under the European Convention on Human rights – Council of European human rights handbooks", Council of Europe, Strasbourg, 2012, 33.

of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected (Recital 83 GDPR and Art. 32 GDPR).

- The GDPR contains a number of key 'principles relating to processing of personal data', of which the principle of 'integrity and confidentiality' is one. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Art. 5(1)(f) GDPR).

In regard of the foregoing it could be argued that the confidentiality obligations included in the GDPR mirror the confidentiality of communications principle included in Article 5(1) of the ePrivacy Directive. However when applying those obligations in practice a number of questions arise:

- To the extent the communication would not exclusively contain personal data but also business information that is confidential but not personal data, the question arises to which extent such content would still be protected. While trade secrets and market practices legislation could protect certain communications, said legislation is not likely to be able to protect business communications.

- Whereas Article 5 of the ePrivacy Directive explicitly states that listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data are prohibited without the consent of the users concerned, a similar clause is not included in the GDPR. One might however deduct indirectly from the provisions of the GDPR that such behavior would be illegitimate. Furthermore, in the absence of clear provisions, there is a risk that Member States will continue to adopt and enforce fragmented rules in this regard.

- Whereas Article 5 of the ePrivacy Directive stipulates that it does not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality, no similar provision exists in the GDPR. However, we consider that even without such explicit provision in the GDPR, data controllers should also be able do so on the basis of the necessity to process such data for the performance of the contract with the user (Art. 6(b) GDPR).

- Whereas Article 5(2) of the ePrivacy Directive introduces the so-called business exception, it is unclear whether the recording of a communications when 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 could also be justified (for the users) on the basis of the necessity to process the data for the performance of a contract (Art. 6(b) GDPR).

Notwithstanding the foregoing considerations there are a number of arguments to justify that the GDPR and fundamental rights conventions sufficiently protect the confidentiality of communications. However, in light of the above questions, considering a possible deletion of the principle of confidentiality of communications will require a further reflection. In any event, during the further evaluation of this principle, the following is to be taken into account:

- The confidentiality of communications principle – whether in relation to natural or legal persons – concerns all sectors, and should not be limited to traditional telecommunications services. Therefore it should be technology-neutral and not dependent on the chosen technology or service, and more in particular the scope of said principle should not remain limited to publicly available electronic communications services;

- The confidentiality of communications principle should consequently be transferred to more horizontal legislation covering all services that allow interpersonal communication.
- The extent of the business exception, which has been implemented in diverging ways by the Member States, should be clarified and further harmonised.

Key message

The principle of confidentiality of communications plays a vital role in today's society. It is protected by the EU Charter of Human Rights, the ECHR, and it is in essence also reflected in the GDPR. A possible deletion of Article 5 of the ePrivacy Directive raises certain questions and requires further reflection. If still required, the revised principle should in any event be technology-neutral, not be limited to traditional telecommunications services and be transferred to more horizontal legislation covering all services that allow interpersonal communications.

4.3 Necessity of the non-privacy-related provisions?

In addition to the privacy-related provisions discussed above, the ePrivacy Directive contains a set of non-privacy-related provisions governing topics such as non-itemised bills (Art. 7 EPD), control over call line identification (Art. 8 EPD), automatic call forwarding (Art. 11 EPD) and subscribers directories (Art. 12 EPD), that all aim to protect consumer rights.

It can be sincerely questioned whether provisions on those topics are still needed and/or relevant in today's digital society. In this respect it must be remarked that:

- The telecom sector is highly competitive and that there are no indications that the rights of consumers would be harmed or even forgotten if the provisions referred to above would no longer be regulated by specific laws. In case there would still be a demand by consumers to have such rights or services, it is very likely that the market functioning will drive telecom operators to provide such rights or services to consumers.
- No similar obligations apply to providers of OTT services and there are no indications that customers of OTT services demand for such rights or services.

More in specifically with regard to the four specific provisions the following can be remarked.

- **Non-itemised bills –** Article 7 of the ePrivacy Directive allows subscribers to have the right to receive non-itemised bills. As set out in Recital 33 of the ePrivacy Directive, itemised bills make it easier to verify if the fees charged are correct, but if the service is used by various persons, this may jeopardise users' privacy.

  Today, prescriptive regulation of cost control and provisions on itemised billing appear outdated, in view of the penetration of cost flat rates as well as considering the increase of communications service providers that do not provide any of such controls. Although the reasoning underpinning of the respective ePrivacy clause is in theory understandable, it should indeed be questioned whether said legislative

intervention is strictly necessary. Even without the existence of such a provision, we deem it unlikely that a provider of a communications service would manifestly refuse to provide non-itemised bills to its customers when requested. If that would not be the case, the market would drive said customer to a competing provider of communications services that offers such possibility.

- **Control over call line identification** – Article 8 of the ePrivacy Directive gives callers the right to prevent the presentation of the calling-line identification if they wish so to guarantee their anonymity. In accordance with Article 10 of the ePrivacy Directive that decision can be overridden when a subscriber requests the tracing of malicious calls or in the case of organisations engaged in emergency calls, law enforcement authorities, ambulance fire brigades, for the purpose of responding to such calls.

  Although indeed no corresponding provisions exist in the GDPR, it can again be questioned whether the absence of such provisions would have distorted the market or would have led to a less optimal result. If such rules would be considered as indispensable, they should apply equally to all services that allow interpersonal communications. This particularly refers to obligations that are indispensable for ensuring a reliable and meaningful emergency service and which, if kept, should be transferred to the legislation which includes respective rules on emergency service.

- **Automatic call forwarding** – Article 11 of the ePrivacy Directive grants subscribers the possibility to stop automatic call forwarding by a third party to their terminals.

  In line with what has already been stated, it is unlikely that providers of communications services would refuse to act against the nuisance which may be caused by automatic call forwarding by others.

- **Subscribers directories** – Article 12 of the ePrivacy Directive grants subscribers the opportunity to determine whether their personal data is included in a public directory. Moreover they must be informed about any further usage possibilities based on search functions in electronic versions of the directory.

  Although this provision is specific to the telecom sector, it must be observed that there is an overlap with the GDPR, as any person providing a directory would be required to comply with the GDPR, which protects subscribers in a similar way. Moreover, it must be remarked that directories envisaged by Article 12 have become outdated. Due to the development of powerful search engines, the ability to search for persons and professional service have changed significantly. In that regard, it also is relevant to remark that already a high number of Member States have removed the obligation to provide directories and directory enquiry services from the scope of the Universal Service obligations.

In regard of the foregoing, specific provisions on non-itemised bills, control over call line identification, automatic call forwarding and subscribers directories do no longer seem to be required and therefore can be repealed.

However, only to the extent that the European legislator would not share that view for all provisions, the provisions still deemed relevant and/or necessary should not be retained in the ePrivacy Directive, but should be transferred to the updated regulatory framework covering a broader range of communication services. In this regard it cannot be denied that:

- The provisions on non-itemised bills, control over call line identification, automatic call forwarding and subscribers directories stem from the existing Telecom Framework, as a result of which the updated regulatory framework covering a broader range of communication services and replacing the Telecom Framework seems to be the most appropriate legal instrument to host those provisions, only if still considered necessary of course.
- It would not make sense and would not be adequate to retain any non-privacy-related provisions in a revised ePrivacy instrument, as the aim of the ePrivacy Directive has initially been to harmonise the

processing of personal data in the telecom sector (Art. 1(1) EPD) and to particularise and complement the provisions of the Data Protection Directive as regards the telecom sector (Art. 1 (2) EPD).

Key message

Given the current state of the market, the non-privacy-related provisions of the ePrivacy Directive are no longer required and can be repealed. However, in case those provisions would still be considered relevant by the European legislator, they should be transferred to the updated regulatory framework covering a broader range of communication services

5 PROPOSED LEGISLATIVE CHANGES

5.1 Overview of the proposed legislative changes

In regard of the considerations set out in the previous Sections, the ePrivacy Directive and Regulation 611/2013 can be repealed in their entirety:

- The privacy-related provisions of the ePrivacy Directive that overlap with the GDPR, notably the clauses on security of processing (Art. 4 EPD), traffic data (Art. 6 EPD), location data (Art. 9 EPD), cookies (Art. 5(3) EPD) and unsolicited communications (Art. 13 EPD) as well as Regulation 611/2013 on the notification of personal data breaches under the ePrivacy Directive[51] are no longer required.
- The non-privacy-related provisions of the ePrivacy Directive that govern general telecom and/or consumer protection topics, i.e. the articles on non-itemised bills (Art. 7 EPD), control over call line identification (Art. 8 EPD), automatic call forwarding (Art. 11 EPD) and directories of subscribers (Art. 12 EPD) can be repealed, or to the extent still deemed relevant by the European legislator moved to the updated regulatory framework covering a broader range of communication services.
- Only one privacy-related provision of the ePrivacy Directive, i.e. the article on confidentiality of communications (Art. 5 EPD), may still be relevant today. Following further assessment of this issue, and if still deemed required, we propose in any event to move this to a more horizontal legislation covering all services that allow interpersonal communications.

Only to the extent that the European legislator would decide not to transfer the confidentiality of communications principle to the updated regulatory framework covering a broader range of communication services and/or to repeal the privacy-related provisions considered no longer relevant, the considerations set out in the following Sections should be taken into account:

- Should the new ePrivacy instrument be a regulation or a directive? (*Section 5.2.1*)
- How should the scope of that new ePrivacy instrument be defined? (*Section 5.2.2*)
- Which regulatory bodies should be competent? (*Section 5.2.3*)

5.2 Changes to the ePrivacy Directive

5.2.1 Legal instrument: Regulation vs. Directive

If the European legislator would not follow the proposed changes but decide to retain an ePrivacy instrument, it is necessary to consider what would be the most appropriate legal instrument for said ePrivacy instrument: a directive or regulation?

In our opinion a regulation would be the right choice for several reasons:

[51] Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, *OJ. L.* 173, 26 June 2013, 2–8.

Consistency and legal certainty – A regulation will exclude the risks on inconsistencies in the implementation of the rules in national laws and will enhance legal certainty and guarantee a more consistent application of the rules within the single market. As a regulation is directly applicable in all Member States, all data controllers and consumers will more easily know their rights and obligations, regardless of where the data controller is established.

While the ePrivacy Directive has been transposed in national laws, resulting in 28 different implementations and interpretations of the same directive, issues of interpretation are likely to be reduced when said rules are placed in a regulation, that is not to be further transposed by the Member States.

For the sake of completeness, it is remarked that already today several provisions of the ePrivacy Directive are formulated in a directly binding way, e.g. Art. 4 EPD (*Security or processing*), Art. 6 EPD (*Traffic data*), Art. 7 EPD (*Itemised billing*), Art. 8 EPD (*Presentation and restriction of calling and connected line identification*), Art. 9 EPD (*Location data other than traffic data*) and Art. 13(1) EPD (*Unsolicited communications*).

Supervision and enforcement – The choice for a regulation would considerably facilitate the application of the supervisory and enforcement mechanism of the GDPR to the new ePrivacy instrument.

Relationship with the GDPR – The relationship with the GDPR would be considerably less complex if the revised rules would result in a regulation, hence a legal instrument at the same level as the GDPR. Although Article 95 of the GDPR and recital 173 of the GDPR delimit the scope of both the ePrivacy Directive, it must be remarked that the ePrivacy Directive, as long as it is a directive, cannot particularise the GDPR. As a regulation has a general application, is binding in its entirety and directly applicable in the ePrivacy Directive, Member States cannot be requested in a directive to derogate from rules contained in a regulation.

Furthermore, it might be appropriate to rename the ePrivacy Directive (or "*Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy on electronic communications*") in a way that is better linked to its content.

Key message

The choice for a regulation for the revised ePrivacy instrument will ensure a more consistent application of privacy rules across the European Union.

5.2.2 Scope

To the extent a revised ePrivacy instrument would be retained by the European legislator, it is relevant to analyse how the scope of that instrument should be defined.

For the sake of completeness, we will not specifically limit this analysis to the confidentiality of communications principles (Art.5 EPD), but start our analysis on the basis of the existing scope-defining provisions of the ePrivacy Directive.

5.2.2.1 Material scope

The aim of the ePrivacy Directive has initially been to harmonise the processing of personal data in the telecom sector (Art. 1(1) EPD) and to particularise and complement the provisions of the Data Protection Directive as regards the telecom sector (Art. 1 (2) EPD). Hence, in accordance with Article 3 EPD, the ePrivacy Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

Not only related to the telecom sector – Although the main idea underpinning the ePrivacy Directive clearly has been to put in place sector-specific data protection rules for the telecom sector, it must be observed that the ePrivacy Directive contains several provisions that have a scope that is not limited to the telecom sector:

- The principle of confidentiality of communications (although limited to electronic communications services and networks) applies to any person that would intercept users' communications, and not only to telecom providers (Art. 5(1) EPD);
- The cookie provision applies to all website operators placing cookies (Art. 5(3) EPD); and
- The anti-spam provision applies to anyone considering to send unsolicited communications (Art. 13 EPD).

As the scope of those privacy-related provisions is not limited to the telecom sector or to telecom providers, it would have been more logical to include them in horizontally applicable legislation, such as for example the GDPR (as has been proposed in our previous study on the ePrivacy Directive).

Not only related to privacy and data protection – In addition, it must be observed that the ePrivacy Directive also contains a significant number of articles that are not directly related to the processing of personal data, and as such do not complement the Data Protection Directive, but are however related to the telecom sector.

Said articles are notably related to non-itemised bills (Art. 7 EPD), control over call line identification (Art. 8 EPD), automatic call forwarding (Art. 11 EPD) and directories of subscribers (Art. 12 EPD). As detailed in Section 4.3 above. It would have made more sense to have included such rules in another more appropriate directive of the Telecoms Package.

Way forward – Although the aim of the ePrivacy Directive has initially been to particularise and complement the provisions of the Data Protection Directive as regards the telecom sector, the material scope today is not limited to the protection of personal data nor to the telecom sector. Hence, to reduce the regulatory complexity and ensure consistency, a revised ePrivacy instrument should no longer contain non-privacy related provisions, but only privacy-related provisions that are still relevant today and that do not overlap with the GDPR. Any still relevant non-privacy-related provisions should be moved to the updated regulatory framework covering a broader range of communication services.

Key message

To reduce the regulatory complexity and ensure consistency, the scope of the ePrivacy Directive needs to be limited to the privacy-related provisions that are still relevant today, and that are not yet regulated by the GDPR.

5.2.2.2 Personal scope

Not only the material scope of the ePrivacy Directive and the GDPR is not aligned. Also the beneficiaries of both legal instruments are not aligned. While the GDPR offers protection to data subjects (meaning "*identified or identifiable natural persons*") the ePrivacy Directive aims to protect:

- 'subscribers' (meaning "*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*"); and
- 'users' (meaning "*any natural person using a publicly available electronic communications services, for private or business purposes, without necessarily having subscribed to this service*"). In this respect it is interesting to remark that although Article 2 of the ePrivacy Directive stipulates that the definitions of the Framework Directive shall also apply in the context of the ePrivacy Directive and that the concept of 'user' had already been defined in the Framework Directive as "*a legal entity or natural person using or requesting a publicly available electronic communications service*", the European legislator deemed it required to exclude legal persons from this definition for the purpose of the ePrivacy Directive.

Such limitation to natural persons seems to make sense in the context of the ePrivacy Directive, which aims to complement and particularise the Data Protection Directive. Although the ePrivacy Directive also aims at protecting the legitimate interests of legal persons, it cannot be denied that the three main objectives are focused on the protection of natural persons, notably:

- The full respect of the fundamental rights set out in Article 7[52] (*Respect for private and family life*) and Article 8[53] (*protection of personal data*) of the Charter of fundamental rights of the European Union, including the fundamental right of confidentiality of communications as guaranteed under Article 7;
- In line with the Data Protection Directive, the harmonisation of legal, regulatory and technical provisions adopted by Member States concerning the protection of personal data and privacy; and
- The free movement of electronic communication terminal equipment and services in the EU, by harmonising the rules on privacy and confidentiality in the telecom sector and providing specific rules on technical features and standardisation.

[52] Article 7 of the Charter: "*Everyone has the right to respect for his or her private and family life, home and communications*.".

[53] Article 8 of the Charter: "1. *Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority*."

As the main objectives of the ePrivacy Directive are the protection of fundamental rights and freedoms of natural persons as guaranteed by the Charter of Fundamental Rights of the European Union and the further harmonisation of the processing of 'personal' data, it makes sense to limit the concept of 'user' to natural persons. Therefore it should not surprise that many recitals and provisions on privacy-related provisions only refer to the concept of 'user', for example:

- The recitals 4, 5 and 6 of the ePrivacy Directive only refer to the "*protection of personal data and privacy of the user*";
- Recital 14 on the definition of location data only refers to the "*latitude, longitude and altitude of the user's terminal equipment*";
- Recital 22 on the confidentiality of communications refers to the "*prohibition of storage of communications and the related traffic data by persons other than users"* and to "*any data referring to the individual subscribers or users"*; and
- Recitals 24 and 25 on the cookie provision state that "*terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users"* and that "*'so-called 'cookies', can be a legitimate and useful tool, for example in verifying the identity of users engaged in on-line transactions."*

However, for the concept of 'subscriber' the ePrivacy Directive does not provide for a specific definition that would deviate from the definition included in the Framework Directive and that would exclude legal persons. Hence, the question should be raised whether this has been the right choice or whether this definition could also be limited to natural persons.

For provisions of the ePrivacy Directive in which the term 'subscriber' is used in connection with the processing of personal data, the question should be raised whether a reference to 'subscriber' can be read as referring to legal persons, or whether such references should always be read as only being related to natural persons, as is the case in the following examples:

- Recital 22 on the confidentiality of communications refers explicitly to "*individual subscribers or users*", which by the addition of the word 'individual' creates the impression that in this regard legal persons are excluded from the concept of 'subscriber'.
- Article 5 of the ePrivacy Directive on the confidentiality of communications states that the concerned subscriber or user has been provided with clear and comprehensive information "*in accordance with the Data Protection Directive, inter alia, about the purposes of the processing*". As this article cross-references to the Data Protection Directive, this could be interpreted as meaning that the information obligation only applies to the extent that the subscriber would be a natural person/data subject, as in accordance with the Data Protection Directive legal persons are not beneficiaries of that directive.

Article 9 of the ePrivacy Directive allows the processing of location data, which are to be considered as personal data, with the consent of the users or subscribers. This clause only makes sense to the extent that the concept of 'subscriber' would only be interpreted as a natural person, as we fail to see how a legal person could be legally entitled to consent to the processing of personal data of natural persons or users, without the consent of those natural persons.In our view it would not make sense to extend the protection of personal data, which is inherently linked to natural persons/data subjects, to legal persons. Moreover, it is

unclear how in practice such extension would increase the level of personal data protection and/or how legal persons could be involved. For instance, Article 9 of the ePrivacy Directive on location data allows that location data relating to users or subscribers can be processed with the consent of the users or subscribers. Does this mean that only a subscriber/natural person can consent to the processing of such data? Or does this mean that a subscriber/legal person could consent to the processing of location data on behalf of its users/natural persons (e.g. its employees)? The second interpretation does not seem to be in line with the principles set out in the GDPR giving data subjects control over their personal data.

For the non-privacy-related provisions of the ePrivacy Directive the definition of the concept 'subscriber' does not result in the same difficulties as is the case for the privacy-related provisions. If the European legislator would move the still relevant non-privacy-related provisions, if any, to the updated regulatory framework covering a broader range of communication services, the question as to the personal scope will no longer need to be addressed, as said framework is most likely to apply to naturals persons and legal persons.

In any event, the problem of the personal scope of the ePrivacy Directive, is, just like the problem related to the material scope, a problem of definitions. It cannot be denied that mixing up definitions stemming from the telecom legislation on the one hand and from the data protection legislation on the other hand creates confusion as to the interpretation of clauses: are the definitions indeed limited to natural persons or do they extend to legal persons? Therefore, we propose to fully align the personal scope, and thus beneficiaries, of the revised ePrivacy instrument with the GDPR, while any remaining non-privacy-related provisions should be taken out of the scope of the ePrivacy Directive.

Key message

To remedy the inconsistencies in the personal scope of the ePrivacy Directive, it is recommended to align the beneficiaries of the revised ePrivacy instrument with the GDPR (data subjects) and to take any non-privacy-related provisions, if still relevant, out of the scope of said ePrivacy instrument.

5.2.2.3 Geographical scope

The Articles 1 (*Scope and aim)* and 3 (*Services concerned*) of the ePrivacy Directive define its material scope, but do not contain a clear determination of the geographical scope of the ePrivacy Directive. Both articles merely contain a reference to the words "*in the Community*" without any further explanation.

As the ePrivacy Directive particularises and complements the Data Protection Directive, the Article 29 Working Party is of the opinion that the territorial scope of the ePrivacy Directive is determined by a combination of both Article 3 of the ePrivacy Directive and Article 4(1)(a) and (c) of the Data Protection Directive.[54] So, in the absence of clear geographical applicability rules in the ePrivacy Directive itself, data controllers should look to the applicable rules of the Data Protection Directive.

[54] Article 29 Working Party, "Opinion 2/2010 on online behavioral advertising", WP 171, 10, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf, and Article 29 Working Party, "Opinion 1/2008 on data protection issues related to search engines", WP 148, 9-12, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

However, as the Data Protection Directive will be replaced by a regulation, which is directly applicable and does not need to be transposed in national law, the GDPR does no longer contain any clauses determining the territorial competence of each Member State and/or applicable national law. Hence, once the GDPR will enter into force, it will become nearly impossible to determine whether a telecom provider subject to the ePrivacy Directive will need to comply with ePrivacy laws on a 'country of origin'-basis, on a 'country of destination'-basis or even on another basis. Moreover, it will also be unclear if and how non-EU based players will fit in. One could assume that as the GDPR as well as the ePrivacy Directive remain silent on this question, every Member State would be free to apply its own rules, potentially leading to an even more fragmented market.

Contrary to the Article 29 Working Party's opinion, the authors of the Commission Study express the controversial opinion that the geographical application of the ePrivacy Directive is not determined on the basis of the principles set out in the Data Protection Directive. In their view, in the absence of an explicit provision on the geographical scope in the ePrivacy Directive, it should follow the same logics as the other directives belonging to the Telecoms Package. In practice this would mean that the applicable law will be determined by the territory on which the network and service providers are operating. As a result, the ePrivacy Directive would also be applicable to networks and service providers not established in the EU as long as they are providing networks and/or services on the EU territory.

In regard of the existing difficulties, during the evaluation of the ePrivacy Directive, attention is to be paid to the geographical application of the new rules, notably:

- To the extent that a revised ePrivacy instrument is still deemed necessary, the current directive should be replaced by a regulation, by which – as set out in Section 5.2.1 above – a number of difficulties, including related to the territorial scope can already be remedied; and
- To the extent that the revised ePrivacy instrument would indeed only contain the still relevant privacy-related provisions, the scope of application can be fully aligned with the GDPR.

Key message

Upon adoption of the GDPR, the territorial scope of the ePrivacy Directive can no longer be determined with certainty. Therefore updated rules on the geographical scope of the ePrivacy rules are to be included in the revised ePrivacy instrument.

5.2.3 Competent regulatory bodies

While the GDPR systematically refers to the term 'supervisory authority', meaning the national data protection authority, the ePrivacy Directive refers to the 'competent national authority', without defining that concept.

Under the Framework Directive the 'national regulatory authority', meaning the national telecom regulatory body, has been appointed for monitoring the telecom sector and specifically performing the obligations assigned to it under the Framework Directive (and the other directives of the Telecoms Package). A number of Member States also attributed the rights and obligations of the 'competent national authority' under the

ePrivacy Directive to said national regulatory authority. In other Member States the data protection authority is competent for the national implementation of the ePrivacy Directive, while in even other Member States responsibilities may be shared between the data protection authority and the telecom regulator as not all provisions of the ePrivacy Directive relate to privacy and/or telecom. Hence, it should not surprise that this has led to a fragmented approach and a considerable level of confusion and uncertainty both for telecom providers and users.

To ensure a consistent enforcement of the revised ePrivacy instrument throughout the EU, the regulatory body competent for that revised ePrivacy instrument should be harmonised and further specified. As the new ePrivacy instrument would need to be aligned with the GDPR and should be limited to still relevant privacy-related provisions, it is recommended to bring the enforcement of the revised ePrivacy instrument under the competence of the supervisory authorities/data protection authorities defined by the GDPR.

Key message

To ensure a consistent enforcement of the revised ePrivacy instrument, the enforcement of that instrument should be brought under the competence of the data protection authorities defined by the GDPR.

* *

*

www.dlapiper.com