BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 6 • N° 20 • MARCH 2020

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

THE PROPOSED ePRIVACY REGULATION: THE COMMISSION'S AND THE PARLIAMENT'S DRAFTS AT A CROSSROADS?

Elena Gil González, Paul De Hert & Vagelis Papakonstantinou

The EU's Digital Single Market Strategy aims to increase trust and security in digital services. A reform of the EU personal data protection regulatory framework through the introduction of the General Data Protection Regulation (GDPR) was a key step to increasing trust in the security of digital services. Following the reform of the GDPR, the strategy also includes the review of the ePrivacy Directive (Directive 2002/58/EC). Indeed, on 10 January 2017, the European Commission presented a proposal for an ePrivacy Regulation to be in force on 25 May 2018, simultaneously with the GDPR. However, this ambitious timeline has suffered delays and the proposal is currently going through the European Union legislative process. On 26 October 2017, the European Parliament voted in favour of the amendments proposed by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in plenary session. This chapter aims to highlight specific aspects of the ePrivacy Regulation draft, in its Summer 2019 state, to shed light upon certain of its most important elements. While the new Commission after the elections of June 2019 awaits appointment, we consider it important, during this stage of the law-making process, to take a photograph of developments so far, which include the Commission's original draft and the Parliament's response (the Council is yet to provide its final position). In this way, future comparisons with the final wording and the reasoning behind them, will be facilitated.

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
A final version of this working paper is published as Elena Gil González, Paul De Hert & Vagelis Papakonstantinou, 'The Proposed ePrivacy Regulation: The Commission's and the Parliament's Draft s at a Crossroads?' in Dara Hallinan, Ronald Leenes, Serge Gutwirth & Paul De Hert (eds.), Data Protection and Privacy. Data Protection and Democracy, in vol. 12 in the Series Computers, Privacy and Data Protection, Hart Publishing, 2020, 267-298 ; Please refer to this final text.

Disclaimer

1. Introduction

EU's Digital Single Market Strategy aims at increasing trust and security of digital services. For this, the reform of the EU personal data protection regulatory framework through the introduction of the General Data Protection Regulation[4] was a key step in order to increase trust and security of digital services.[5] Following the reform of the GDPR, the Strategy also includes the review of Directive 2002/58/EC.[6] Indeed, on 10 January 2017 the European Commission presented a proposal for a Regulation on Privacy and Electronic Communications, repealing the ePrivacy Directive.[7] The future ePrivacy Regulation aims to achieve, among others, the establishment of a new personal data protection legal framework by complementing and particularizing the GDPR.[8] The ePrivacy Regulation proposal takes account of the important technological and economic developments in the sector of electronic communications and aims to modernize existing principles according to the new practices.[9] It aims to promote a high level of protection of confidentiality in communications regardless of the technology used.[10]

While the ePrivacy Directive is formed by 49 recitals and only 19 Articles, the draft ePrivacy Regulation consists of 43 recitals and 29 Articles, being therefore a larger corpus of provisions, divided into seven chapters. The structure is as follows: Chapter I contains general provisions dealing with the subject matter, the scope and definitions. Chapter II deals with the protection of electronic communications data, information stored in terminal equipment and information rights regarding privacy settings. Further, Chapter III refers to end-users' rights regarding electronic communications. Chapter IV deals with supervisory authorities and their cooperation and consistency procedures, leaving Chapter V for remedies, liability and penalties. Subsequently, Chapter VI goes around delegated and implementing acts, while some final provisions can be found in Chapter VII.

The aim was for the new ePrivacy Regulation to be applicable on 25 May 2018, simultaneously with the GDPR. However, this ambitious timeline has suffered delays and the proposal is currently going through the European Union legislative process. On 26 October 2017, the European Parliament voted in favour of the amendments proposed by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in plenary session. The final version of the Council is not known at the time of drafting this paper (summer of 2019). In this scenario, there is an even more pressing situation towards reaching a final version of the text after the European Data Protection Board (EDPB) statement urging the Commission, Parliament and Council towards replacing the Directive "as soon as possible".[11]

1 PhD candidate at CEU San Pablo University (Madrid), Visiting researcher at Instituut voor Informatierecht (IViR), Universiteit van Amsterdam.
2 Professor at Vrije Universiteit Brussels (LSTS) and University of Tilburg (TILT).
3 Professor at Vrije Universiteit Brussels (LSTS).
4 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, 4.5.2016, p. 1–88 (the "GDPR").
5 European Commission, 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, 6 May 2015.
6 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, 31.7.2002, amended two times by Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (the "ePrivacy Directive").
7 European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.
8 See Recital 5, ePrivacy Regulation.
9 See Recital 6, ePrivacy Regulation.
10 See Recital 14, ePrivacy Regulation.
11 European Data Protection Board (EDPB), Statement 3/2019 on an ePrivacy Regulation, 13 March 2019.

Aim of this contribution is to highlight specific aspects of the ePrivacy Regulation draft, in its summer of 2019 state, in order to shed light upon certain of its, to our mind at least, most important elements. We consider it important in this stage of the law-making process, while the new Commission after the elections of June 2019 awaits appointment, to take a photograph of developments so far, which include the Commission's original draft and the Parliament's response (the Council is yet to provide its final position). In this way future comparisons with the final wording, and the reasoning behind them, will be facilitated. To this end our contribution is structured as follows. We begin by briefly reviewing the relationship between the ePrivacy Regulation and the GDPR, particularly with regard to the GDPR being ***lex generalis*** and the ePrivacy Regulation ***lex specialis***, or the fact that both normative frameworks are shaped as regulations, therefore directly applicable in all Member States (section 2).

We then comment on the material and territorial scope of the Regulation. The ePrivacy Regulation has formally expanded its scope to cover Over-The-Top providers and to deploy extraterritorial effects, so that it will de enforceable even to providers locates outside the EU or if the processing does not take place in the EU, as long as the other conditions are met (section 3).

Further, we review an important set of provisions of the ePrivacy Regulation, namely, the provisions dealing with the protection of confidentiality of communications in particular as regards information stored in and emitted by terminal equipment. For each case we describe the existing situation under the ePrivacy Directive and the changes sought with the newer reform in order to provide a context that helps explain the development of the legal framework (section 4). Our final section (section 5) focuses on the issue of consent. The Commission's proposal for an ePrivacy Regulation, departing from a general prohibition, provides exceptions that allow the processing of personal information in specific cases. In brief, these exceptions can be summarized as information being allowed to be processed when necessary or with users' consent. Indeed, the ePrivacy body heavily relies on users' consent to legitimise non-necessary uses of otherwise private data. We will remark upon this fact while commenting on how contemporary privacy settings could be affected under the proposed updated rules.

2. The relationship between the ePrivacy Regulation and the GDPR: Is there life beyond personal data processing?

Ambition of the EU during the efforts to update its data protection framework and related rules was, among others, to ensure a more coherent application of the rules in the Union, leading to a greater degree of protection for people and legal certainty for organisations. To this end, is it important that the proposed ePrivacy Regulation is aligned with different sets of rules in order to provide a high level of protection for users of electronic communications services and a level playing field for all market players.

The GDPR is apparent the elephant in the law-making room, a point of reference the ePrivacy Regulation cannot possibly ignore. As regards their relationship, a number of points can be raised:[12] ***First***, the GDPR sets the ***lex generalis*** of data protection in Europe and therefore applies to all matters related to the processing of personal data, regardless of the sector, provided that there is no sector-specific law to apply. Electronic communications is one, if not the only one, of these fields. In this sense, the Proposed e-Privacy

12 Explanatory Memorandum of the Proposal, p.2. See also the EDPB's relevant views in Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 17 March 2019.

Regulation is ***lex specialis*** to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data. In particular, the areas of unsolicited marketing, tracking technologies, such as cookies, and confidentiality are covered in a more specific way in the ePrivacy Regulation. On the other hand, in those matters where the Proposed ePrivacy Regulation does not specify anything, the GDPR will apply by default (such as certain controllers' obligations). This resulted, for instance, in the repeal of some provisions from the e-Privacy Directive, such as the security obligations of Art. 4 ePD to avoid unnecessary duplications.[13]

Second, the selection of a Regulation instead of a Directive as the legal instruments of choice or both GDPR and the new ePrivacy framework is oriented at creating a more uniform regime across Member States. Regulations eliminate the need to enact national legislation for them to be directly applicable, therefore enhancing consistency among ePrivacy and GDPR.

Most importantly, however, while the GDPR enshrines primarily Art. 8 of the Charter of Fundamental Rights of the EU[14] to protect personal data, the ePrivacy Regulation is targeted at Art. 7 of the Charter, which protects a person's private life, home and communications. Therefore, while the GDPR ensures the protection of personal data, the ePrivacy Regulation ensures the confidentiality of communications, which may also contain non-personal data and data related to a legal person. This is one of the reasons for which is purposeful having a separate instrument to ensure an effective protection of Art. 7 of the Charter.[15] However, some voices have also arisen arguing that most of the processing operations covered by the ePrivacy Regulation would entail personal data and therefore would be covered by the GDPR in a more flexible way. Under this argument, the ePrivacy Regulation would just impose unnecessary burdens over providers of electronic communications services.[16]

A final, ***fourth*** point refers to supervision: Consistency between the ePrivacy regime and the GDPR could also be enhanced through the decision to make the same independent supervisory authorities responsible for monitoring compliance of both sets of rules.

3. The material and territorial scope of the draft ePrivacy Regulation

Because internet and digital technologies know no borders, the dimension of the problem goes beyond the territory of a single member State and therefore action at the EU level is an added value.[17] With that in mind, the Commission in its proposal broadened the material and territorial scope of the ePrivacy Regulation in relation to that of the ePD. However, the Commission's proposal has raised a number of issues related to the scope of the ePrivacy Regulation, as well as its definitions and exceptions. This is why in the next few pages we will present the suggested changes relating to the material and territorial scope of ePrivacy Regulation in their current status (summer of 2019).

13 This was true in the Commission's draft of the ePrivacy Regulation. On the other hand, the Parliament's text expanded on the security obligations. Therefore, it remains to be seen what the approach will be in the final text. For further details, see section 7.
14 Charter of Fundamental Rights of the European Union [2000] OJ L C 364/01.
15 Explanatory Memorandum of the Proposal, p.5.
16 Centre for Information Policy Leadership, EPR vis-à-vis GDPR, A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation, 2018, p. 10.
17 Explanatory Memorandum of the Proposal, p.4.

3.1. Material scope (Art. 2 ePrivacy Regulation)

The ePD deploys its effects only over traditional telecom operators, which were the main providers collecting communications data at the time of its adoption. In addition, it covers only publicly available e-communications services in public networks, leaving aside the debated cases of publicly accessible private communications networks (such as wifi connections in airports or restaurants).[18] This limitation was evident even at the time of its adoption.[19] Through advances of new technologies new functionally equivalent services have arisen, making clear the scope of the ePD has become too narrow.

Due to all this, the Commission in its proposal aims to widen the ePrivacy Regulation scope to cover not only traditional telecom providers but also new market players, the so-called OTT providers such as voice over IP, text message and email providers. Art. 2 ePrivacy Regulation contains the rules on the material scope of the Regulation. Although the main principle has remained untouched among the two versions examined in this paper, the wording used by the Parliament clarifies that of the Commission.
Art. 2 is drafted by the Commission stating that the Regulation applies to "the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users". On the other hand, the ePrivacy Regulation explicitly excludes its application over electronic communications services which are not publicly available (Art. 2.2.c). These include phone calls, Facebook messenger messages, emails, etc.

While these changes already represented an expansion in the scope of the law compared to the ePD, the Parliament amendments further clarify the scope of the ePrivacy Regulation on the basis of the LIBE Report, that stated that the wording seemed too narrow.[20] Following this report, the amended version of the Parliament includes in the body of Art. 2 what was already mentioned in Recital 8. Therefore, the Parliament explicitly extended the scope of the ePrivacy Regulation to information processed by terminal equipment of end-users, the placing in the market of software permitting electronic communications (for instance, Google Chrome services), the provision of public available directories and the sending of direct marketing electronic communications.

In addition, the Commission proposal of Art. 2 seems to protect only confidential communications in ***transit***, but not when stored.[21] Under this interpretation, the ePrivacy Regulation would only apply during the time where communications are taking place, and GDPR would apply after the recipient receives the data where personal data is at stake. This is particularly relevant in the current digital environment, where data remains stored after its transmission as part of the service (as could be case for storage in the cloud or the services of WhatsApp) and the GDPR provides for more flexible options to process data than ePrivacy Regulation. In this scenario, following the recommendations of WP29,[22] the Parliament clarifies Recital 15 to make clear that also stored data is to be protected under the ePrivacy Regulation.[23]

18 European Parliamentary Research Service, Briefing on the EU legislation in process: Reform of the e-Privacy Directive, of September 2017, p. 4.
19 V Papakonstantinou and P. De Hert, 'The Amended EU Law on EPrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights', The John Marshall Journal of Computer & Information Law XXIX, no. 1 (Fall 2011): 101–47.
20 LIBE Report, p. 25. http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf
21 Although Art. 5 on confidentiality of electronic communications data mentioned stored data as well.
22 Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 April 2017, p. 26.
23 However, the Council version for the PeRP makes explicit that protection is only granted to data in transit.

As regards another Parliament intervention, the Commission's proposal uses the definition of "electronic communications services" set forth in the Electronic Communications Code in order to ensure an effective and equal protection of end-users when using functionally equivalent services.[24] Under this, the concept of electronic communications services is defined as services provided by means of electronic signals over, for example, telecommunications or broadcasting networks. The term, however, excludes services controlling editorial content and information society services which do not involve the transmission of signals.

However, the Parliament is of the idea that the ePrivacy Regulation should be a stand-alone instrument and contain its own provisions, not depending of the Electronic Communications Code. Therefore, the Parliament suggests that the definitions from the Code be incorporated in the Proposal, taking into account any adaptation needed. In this regard, for instance, the definition of communications metadata has been amended to clarify the concept.

In any event, what seems clear is that, through this definition, the ePrivacy Regulation's current draft aims to expand its scope to include now the so-called Over-the-Top (OTT) communications services, which are not clearly included in the ePD, creating unequal rules for similar service providers. OTT communications services are those provided over the public internet and are functionally equivalent to more traditional communication means and therefore have a similar potential to impact on the privacy and right to secrecy of communications of people.[25] Where years ago it was only possible to make calls through ordinary telecom means, we can now make phonecalls over the internet by using the services provided, for instance, by Skype. In addition to the OTT services covered by the definition of "electronic communications services" of the Electronic Communications Code, the ePrivacy Regulation as amended by the Parliament also covers:

interpersonal communications services, such as WhatsApp;

services consisting wholly or mainly in the conveyance of the signals, like machine to machine services and for broadcasting services, when the information can be related to the identifiable end-user receiving the information, such as Netflix;[26]

services which are not publicly available, but provide access to a publicly available electronic communications network, for instance, a VPN of a company that gives access to the outside internet.

The explicit clarification that the ePrivacy Regulation also covers machine-to-machine interactions is relevant, as connected devices that communicate with each other is rapidly increasing due to the expansion of the Internet of Things. [27] As argued by the WP29, this is a desirable fact, as those communications

24 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), amended by Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36.

25 For a deeper understanding of OTT services see Body of European Regulators for Electronic Communications, Report on OTT services, January 2016.

26 The inclusion of machine-to-machine services is of special importance in the context of the Internet of Things. Indeed, the communications between machines generate both content and metadata which needs to be protected.

27 In the Commission's proposal only Recital 12 mentioned that ePrivacy Regulation would be directed at machine-to-machine communications, but this fact was not included in any article. This concern had been reflected by both Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 April 2017, p. 28, and the LIBE report, p.47.

can also reveal personal information. However, for this same reason, WP29 also reflects that pure machine-to-machine communications should be left out of the scope of the ePrivacy Regulation when they have no impact on either privacy or the confidentiality of communications.[28]

The expansion of the ePrivacy Regulation scope to include OTT providers is a relevant change, and it was also one of the facts that questioned the most the effectiveness of the ePD to provide users' protection. It could be safe to state that, nowadays, a majority of EU consumers use OTT services on a daily basis. Nevertheless, it should also be noted that while debate has been generated around services that enable communication just as an ancillary service for another core service (e.g. videogames where players can chat or dating apps like Tinder), the version of the Commission included them in the scope of the ePrivacy Regulation, while the version of the Parliament excludes them.[29]

3.2. Territorial scope (Art. 3 ePrivacy Regulation)

One of the most important aspects of the ePrivacy Regulation proposal is the widening of its territorial scope. The ePD is directed to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community".[30] The Commission's draft for the ePrivacy Regulation, on the other hand, follows the path of the GDPR and aims at an extraterritorial effect. Art. 3 establishes that it will apply to the data processed in connection to the provision of electronic communications services provided to end users located in the EU, even if the provider is established outside the EU (that is, even if the processing does not actually take place in the EU). Moreover, in order not to deprive end-users in the Union of effective protection, the ePrivacy Regulation would also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union. Along the same lines in the Commission's original draft, In those cases where the provider is not located in the Union, a representative must be appointed in writing. Its duties would encompass provision of the necessary information to supervisory authorities and end-users on all issues derived from the ePrivacy Regulation.

The Parliament has detailed and clarified the provisions regarding the appointment of a representative to gain consistency with the changes made in relation to the activities added in the material scope. Thus, the Parliament's version states that representatives must also be named for providers not established in the Union in the case of offering of software permitting electronic communications, publicly available directories, or direct marketing electronic communications, irrespective of whether a payment of the end-user is required. Thus, it has amended this provision to state that the ePrivacy Regulation will apply to end-users in the Union, activities that are provided from the territory of the Union and the processing of information related or by a terminal equipment when the device is in the Union.[31]

Under this provision, for instance, Chinese social networks such as PengYouWan would need to name a representative if they wish to direct their services at users in the EU. This could lead, as has been the case with the GDPR, on some providers geo-blocking the EU area until they are compliant, an example of which can be seen in the image below.

28 Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 April 2017, p. 28.
29 Art. 4.2 ePrivacy Regulation.
30 Art. 3 ePD.
31 Art. 3.2 ePrivacy Regulation.

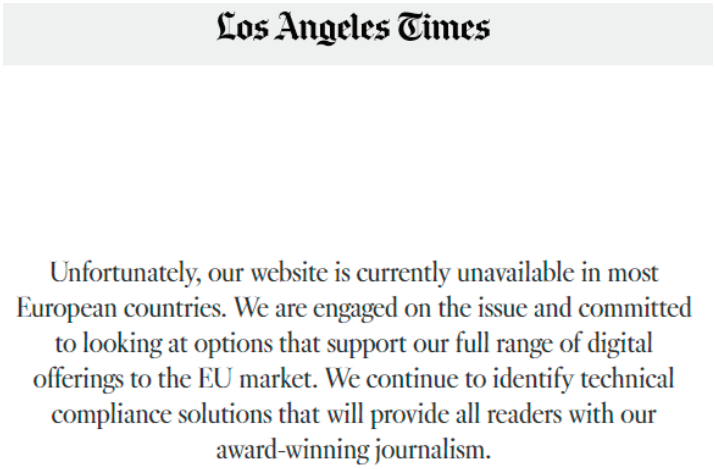

Image 1: Example of geo-blocking from Los Angeles times

4. Confidentiality of communications: Protection of electronic communications of natural and legal persons in the draft ePrivacy Regulation

Protection of the confidentiality of communications is an important part, and equally a raison d étre, for the eprivacy regulatory framework. The reason behind the protection of electronic communications data is that the content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication (personal experiences, emotions, sexual or political preferences, etc.), the disclosure of which has clear privacy implications.[32] Moreover, metadata derived from electronic communications, may also reveal very sensitive and personal information, as expressly recognised by the CJEU.[33]

The explicit protection of both content and metadata is of enormous importance nowadays. Back in the time confidentiality of content data could be seen as more relevant due to its higher potential to reveal information about end-users' behaviours, thoughts or inclination to certain ideas. However, current technologies enable easier and cheaper collection of vast amounts of metadata from which patterns and behaviours can be also been observed. Think for instance, the possibility of inferring the religious beliefs of a person if one can gain access to his phone location data, revealing that goes to a specific church every week. The examples are countless. In addition, while content data will, almost always, be in unstructured format, and therefore, more difficult to analyse, metadata can be gathered in structured formats and analyse in (near)real time. Together with this, it is important to note the ever-increasing torrents of data coming from the Internet of Things and the connected society. This widens the possibilities to analyse end-user's data in an attempt to monetise it, with the subsequent violation of privacy. The result is that individual pieces of data that may have been innocuous years ago are now can expose now private information, many of which can also qualify as personal data. These reasons justify the need of a clearer definition of metadata and its protection.

32 Recital 2 of the Proposal.
33 Explanatory Memorandum of the Proposal, p.4. See Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Secretary of State for the Home Department, ECLI:EU:C:2016:970.

In this section we will analyse the original provisions of the draft ePrivacy Regulation, as suggested by the Commission, and compare them against the Parliament's recommendations and amendments. Also, in order to understand the context that led to the ePrivacy Regulation being drafted in a specific way by the Commission, each subsection details the existing situation under the ePD, as well as, the main conclusions of the REFIT evaluation carried out by the European Commission[34] to assess the needed modifications. Overall, the ePrivacy Regulation has chosen a general approach consisting on broad prohibitions and narrow exceptions, and the targeted application of the concept of consent, which the WP29 has explicitly welcomed.[35]

4.1. Metadata in the draft ePrivacy Regulation: Is merging location and traffic data a good idea?

The ePD provides for Member States to ensure confidentiality of communications and of related traffic data in public communication networks and services. Therefore, listening, tapping, storing or engaging in other kinds of interception or surveillance of communications and the related traffic data without the consent of the citizen concerned was prohibited (except when legally authorised). This provision covered both the content of the communication (for instance, the voice in a phone call) and the related traffic data (for instance, the time of the call). That data could be used under consent of the user, or if anonymised.

In this regard, "traffic data" is defined in Art. 2.b ePD as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof" (such as the time of the call, as mentioned, or the phone number). Under Art. 6 ePD, traffic data can only be used if anonymised, for billing purposes or with consent of the user for marketing or value-added services.

In the same way, the ePD defines "location data" in Art. 2.c as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service". Location data other than traffic data can be used under the ePD when anonymised, or with consent of the user when it was intended to be used for value added services (Art. 9 ePD). An example of a value-added service using location data is a GPS on our mobile phones.

The REFIT evaluation found that these rules are not replicated in other legal instruments, such as the GDPR, therefore, being necessary under an e-privacy regulatory framework. However, under the ePD, these rules are not fully effective in protecting the confidentiality of communications. Some of the reasons are, for instance, the exclusion of OTT services[36] or the outdated wording (which did not include automatic intrusions without human intervention). For instance, in an internet environment, the same data

34 The REFIT evaluation provides the results of the study conducted by the Regulatory Fitness and Performance Programme to assess the health and state of current rules and to identify improvement areas. The results of this study were presented by the European Commission together with the Proposal for a new ePrivacy Regulation on 10th January 2017. See European Commission, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC SWD(2017) accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.

35 Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 April 2017.

36 Being true that the processing of personal data through OTT services is covered by the GDPR, confidentiality of communications needs to be guaranteed by the new ePrivacy Regulation. This is necessary to protect users and granting an even playing field for all providers regardless of the technology used, especially in the age of Internet of Things.

may constitute content for one provider while being traffic data for other. However, the definitions as set in the ePD do not reflect this situation. High protection standards of all electronic communications data are equally important, as nowadays the processing of data about the communication, such as the URL of websites accessed may be as revealing as the content of the communication itself. [37] Further, while the GDPR allows for several bases for the processing of personal data (such as consent, performance of a contract or legitimate interests) the ePD only allows for consent and restricts the processing to the provision of value-added services. Therefore, the ePD aims at a more restrictive approach than the GDPR.[38] In light of all this, the REFIT evaluation concludes that confidentiality of communications should be protected under the e-privacy rules, as they enhance people's rights. Specifically, the added value of these rules lies in the need of having a high level or protection and harmonised standards, an objective that cannot be achieved with national laws. Further, it was found that the concepts of confidentiality of electronic communications, traffic and location data needed to remain unified.[39]

In response to the above, the ePrivacy Regulation draft originally drafted by the Commission carries the aim to protect both the content of communications and the related metadata: In this context, the Commission's draft drops the concept of traffic data and location data and uses "metadata" instead. Under the Commission's draft ePrivacy Regulation the concept of metadata contraposes that of content.[40] In particular, the ePrivacy Regulation contains a more specific definition of "electronic communications metadata", as in "data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of communication".[41]

This new definition covers what the ePD defines as traffic data and location data altogether. The reason for this merge lies in the increasing generation of data and the computing capacity to store and analyse it. These technological advancements caused that, even when some electronic communications data were deleted, the analysis of traffic and location data coming from multiple sources could show emerging patterns which could subsequently lead to the creation of individual and group profiles, increasing the potential privacy impact. This is also especially important due to the covert and unexpected ways that could lead to massive collection and analysis of data. Merging rules on traffic data and location data (i.e creating metadata provisions) would therefore offer a higher degree of protection and set clearer rules for all parties.[42]

On the other hand, the definition of "electronic communications content" has been worded by the Commission in its proposal as "the content transmitted, distributed or exchanged by means of electronic communications services, such as text, voice, videos, images, and sound. *Where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using the respec-*

37 European Data Protection Supervisor, Preliminary EDPS Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC), of 22 July 2016, p. 13.
38 REFIT evaluation study, p.38.
39 In a similar way, the WP29 also recommended updating the provisions regarding traffic and location data, given the acknowledgement data may reveal very sensitive information and it is not only collected by traditional telecom providers, but also by new market players such as app developers. See Article 29 Data Protection Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, 19 July 2016, p.13.
40 The EDPS had called for adoption of the concept of metadata in European Data Protection Supervisor, Preliminary EDPS Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC), of 22 July 2016, p.13.
41 Art. 4.3.d ePrivacy Regulation, as drafted by the Parliament Proposal.
42 Article 29 Data Protection Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, 19 July 2016, p.14.

tive service, they shall be considered electronic communications content for the respective service"[43] (emphasis added). For instance, when taking a photograph, the picture itself would be content, whereas the camera settings, the time and date, would be metadata. Also, when sending an email, the body of the email, the subject and the attached documents would be the content, whereas the sender and the recipient of the email would be metadata. More complex information can also qualify as metadata, such as that which can be parsed out of the IP traffic, like website names, source and destination addresses, etc.[44] However, there is a fine-drawn detail in the distinction of content and metadata (see the emphasised sentence). In essence, the ePrivacy Regulation provides for differences, so that the same data can be considered content or metadata depending on the service provider. To understand this, we will consider the email example. What we said in the previous example is true for the email provider. However, for the internet service provider, all body of the email, subject, attached documents, sender and recipient will be content of the IP packets routed by the provider.[45]

4.2. The protection of metadata under Articles 5 and 6 of the draft ePrivacy Regulation

Taking the above into consideration, Article 5 ePrivacy Regulation has been configured by the Commission as a general rule which provides the confidentiality of all electronic communications data. Since this is a fundamental right recognised by the Charter, any interference with it must be limited to what is strictly necessary and proportionate in a democratic society. Consequently, electronic communications data can only be used in certain exceptional situations, provided in Art. 6 and 7 ePrivacy Regulation.

Under Article 6.1 of the draft ePrivacy Regulation by the Commission, electronic communications data, which encompasses both content and metadata, can only be used by providers of electronic communications networks when necessary for two situations: (i) to achieve the transmission of the communication; and (ii) to maintain or restore security of the network, or its availability, integrity or confidentiality, as well as detect technical errors in the transmission. In this later case, the Parliament's amended text introduced the possibility of data being used by both the providers or other third parties acting on behalf of them. This could be the situation, for example, when a provider contracts with an external security company to ensure the communications are held secure and free of technical errors.

The Parliament amended the Commission's ePrivacy Regulation draft to explicitly set a strict threshold for the use of electronic communications data, by requiring that data be processed "only if it is technically necessary", whereas the wording of the Commission limited the use of electronic communications data to what is "necessary". In addition to this provision, encompassing both content and metadata, the ePrivacy Regulation creates separate exceptions that allow for the use of electronic communications content and metadata.

43 Art. 4.3.b ePrivacy Regulation, as drafted by the Parliament Proposal.

44 Sophie Stalla-Bourdillon, Evangelia Papadaki, Tim Chown. Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK. Serge Gutwirth & Ronald Leenes, Data Protection on the Move, Springer 2015. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2625181.

45 See also Recital 14.a as drafted by the Parliament Proposal.

Art. 6.2 ePrivacy Regulation establishes that metadata can be used when necessary for certain purposes. Again, the Parliament amended the Commission's text to raise the bar from what is "necessary" to what is "only strictly necessary". The situations where processing electronic communications metadata is allowed are therefore the following. ***Firstly,*** for billing purposes,[46] for instance, to ensure a person benefiting from the service has not fraudulently sent the bill to another person, as well as for prevention of abusive use and subscription of electronic communications services.[47] In this case, only the necessary metadata may be kept until the end of the period during which a bill or an undue payment may be lawfully challenged or when technically necessary for security purposes described above.[48]

Secondly, metadata can be used when necessary to meet mandatory quality of service requirements[49] according to specific legislation. An example of this would be the situation when the provider needs to adapt the quality of an image to the settings of your screen. ***Thirdly***, other than in these necessary cases, metadata can only be used with the consent of the user, for the provision of specified purposes or specific services, when such services cannot be fulfilled with the data at stake. For instance, a service where the user is showed the cheapest petrol stations in the area by tracking his real time location. In this regard, the amends of the Parliament to the text proposed by the Commission try to further limit the use of consent as an exception, by only allowing consent of users (i.e. natural persons)[50] and not of all end-users (i.e natural and legal persons)[51] and by adding the obligation to conduct a privacy impact assessment and prior notification to the supervisory authority when this processing shows a high risk for individuals, as stated in Arts. 35 and 36 GDPR.[52] In these two later cases (namely, meeting quality of service requirements and providing specified purposes or services), metadata may be erased or made anonymous when it is no longer necessary for the purpose.

In light of this, if the Parliament's amendments were accepted, a provider would be able to keep anonymised metadata for secondary uses that may not entail risk for users' rights and could help developing new services in a big data scope. For instance, the Smart Steps project launched by Spanish telecom company Telefónica used aggregated anonymised metadata from their communications services to detect trends and groups' behaviour. This has enabled to get precise insights about how many tourists arrive at a city, where they come from and how they move around the territory, which has big value for the tourism sector. This has indeed turned into a new service by Telefónica to deliver information to interested local businesses, which can offer special discounts at certain times of the day for cultural, gastronomic or retailing services.[53]

On the other side of the spectrum, in the similar case when the Parliament's changes were accepted, one would be able to find also unlawful uses of metadata. For example, in a recent case, Google has been

46 Art. 6.2.b) ePrivacy Regulation, as drafted by the Parliament Proposal.
47 The WP29 called for a clarification of Art. 6.2.b) ePrivacy Regulation for which certain spam and botnet detection could be interpreted as strictly necessary for the prevention of abusive use of electronic communications services. See Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP247), of 4 April 2017, p.13. This recommendation has nonetheless not been included in subsequent versions of the ePrivacy Regulation.
48 Art. 7.3 ePrivacy Regulation, as drafted by the Parliament Proposal. In this regard, whereas the Commission's proposal made reference to "relevant" metadata, the Parliament's amends only allows to keep and store metadata that is "strictly necessary" for billing-related legal procedures.
49 Art. 6.2.a) ePrivacy Regulation, as drafted by the Parliament Proposal.
50 Art. 4.3.af) ePrivacy Regulation, as drafted by the Parliament Proposal.
51 Art. 4.3.ae) ePrivacy Regulation, as drafted by the Parliament Proposal.
52 New Art. 6.2a ePrivacy Regulation, as drafted by the Parliament Proposal.
53 Telefónica, Smart steps project. Available at: https://www.wholesale.telefonica.com/es/services/digital/big-data/smart-steps/.

found to store users' location data even when they used privacy settings to prevent Google from doing so.[54] In a similar recent episode, the Swedish data protection authority has requested information from Google on the use of dark patterns to obtain user's consent to access location data. According to it, Google may be using "deceptive design, misleading information and repeated pushing to manipulate users into allowing contact tracking of their movements".[55]

As far as content of communications is concerned, in the current draft ePrivacy Regulation, under the Parliament's amendments in the original Commission draft, it can only be processed with consent, due to its sensitive nature and the fact that no technical reason would justify such an interference with privacy.[56] As was the case with the processing of metadata, consent for the processing of content data is allowed for end-users in the Commission's proposal and only by users under the more restrictive Parliament's proposal.

In this case, however, for which purposes could consent be requested for? Consent could be requested for two scenarios. ***First***, user consent could be requested for the provision of specific services requested by the user himself, provided the service cannot be fulfilled without the processing of such content "by the provider", as added by the amended text of the Parliament. Under this provision, providers could not seek to obtain consent for the use of more content data that is necessary for the purposes of the services, which need to be specific. In addition, the specification that data must be needed "by the provider" further limits the scope of the article, in that third parties cannot use the content of communications for their services. This will prevent, for instance, your email provider to transfer your data to a third company specialised on natural language processing algorithms and which could therefore be interested in accessing the texts of your emails to enhance their service. This would also mean Google not being allowed to seek user consent to grant access to hundreds of third-party developers to your Gmail emails, and even allow those third parties to share the data with other third parties, as it seemingly currently does, according to a letter that Google itself sent to US lawmakers.[57]

Second, consent to use content of electronic communications data under the current ePrivacy Regulation draft could also be requested from all users for the provision of specified purposes, provided that the purposes cannot be achieved with anonymous information and provided that the provider has consulted the supervisory authority according to Art. 36.2 and 3 GDPR.[58] This would cover those cases where services are not requested by the user himself, but rather may be offered by the provider. An example of this situation happens when a social network presents users with a functionality under which it scans users' pictures across the network to automatically tag him on it or to send alerts when someone uploads a picture where he appears. In this regard, the Parliament amendment establishes an exception under which consent of all users will not be required, if the processing is done under a service explicitly requested by one of the users, with his consent, and when it does not adversely affect the rights and interests of the other users. This would thus simplify the obtention of consent for domestic practices and creates a sort

54 New York Times, AP Exclusive: Google Tracks Your Movements, Like It or Not, 13 August 2018. Available at: https://www.nytimes.com/aponline/2018/08/13/us/ap-apfn-us-google-location-tracking-abridged.html.

55 Note, however that, as location data related to an individual may constitute personal data, the Swedish authority is examining Google's activities under the eyes of the GDPR. See full request of information: Datainspektionen, Request for Reply and Further Clarification, 18 January 2019. Available at: https://www.datainspektionen.se/globalassets/dokument/ovrigt/google---request-for-reply-and-further-clarification---skrivelse-till-tillsynsobjekt.pdf.

56 Art. 6.3 ePrivacy Regulation, as drafted by the Parliament Proposal.

57 The Independent, Google admits giving hundreds of firms access to your Gmail inbox, 21 September 2018. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-data-sharing-email-inbox-privacy-scandal-a8548941.html.

58 In this regard, the Parliament establishes an exception under which consent of all users will not be required if the processing is done under a service explicitly requested by one of the users, and when it does not adversely affect the rights and interests of the other users.

of household exemption.[59] By means of this, the proposal shows a clear preference for consent as a lawful basis for the processing, while simultaneously trying to avoid user consent fatigue.

Lastly, regarding how long the data should be kept and when it must be erased, the Commission's proposal first indicated that providers should erase content data or make it anonymous when the transmission has been completed and the recipient has received the data, regardless of whether users could store it using a third party service. The Parliament amended this provision to establish that content shall be erased when it is no longer necessary for the service requested by the user. That is, it opted for a more protective approach by eliminating the possibility of providers keeping anonymised content data. [60] For example, when a user shares a picture through a messaging app, the app will delete the picture from its servers once it has been delivered to the recipient. However, both users can still decide to save it in a cloud provider, who will then be obliged to comply with the GDPR. This would mean, therefore, among other things, that the cloud service provider would need a lawful basis to process the data, would be obliged to respect the purpose limitation principle, to provide transparent information, attend users' rights or put in place appropriate security measures.

As a concluding remark on Article 5 ePrivacy Regulation as it stands today, without disregarding the specificities commented for each exception granted, they all share the need of being interpreted in a narrow way. For instance, some provisions allow processing of data for necessary purposes. In this regard, necessity must be limited to what is "technically necessary"[61] or "strictly necessary".[62] In addition, other provisions allow for the processing of data when users have given their consent. The situations where this is possible are restricted to a minimum, as requesting consent is limited to situations where the processing is necessary for specific purposes which cannot be achieved otherwise (for instance, by not using the data or by using anonymous data).[63] Hence, under this approach, providers would not be allowed to ask customers to waive their privacy rights by consenting to invasive practices. Therefore, these provisions show the clear vocation of the ePrivacy regime to narrow down the situations where confidentiality of communications data can be interfered. Also, by requiring consent for the processing of electronic communications data, the ePrivacy legislation opts for a more restrictive approach than the GDPR, which would potentially allow for a wider set of legal bases, such as the performance of a contract or legitimate interests, [64] as well as secondary uses of data that fall under a non-incompatible purpose.[65]

59 The WP29 had called for a domestic exception in the processing of electronic communications data (both content and metadata) for purely personal purposes, such as the use of text-to-speech services. This would mean that, for the use of electronic communications data for any other purpose, such as behavioural advertising, consent from all users should be requested. See Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP247), of 4 April 2017, p.3. The Parliament followed this recommendation only partially, in that consent from all users was not introduced as a requirement for the use of metadata, but only content. On the other hand, for the use of content data, household exemption was introduced.

60 Art. 7.1 ePrivacy Regulation, as drafted by the Parliament Proposal.

61 Art. 6.1 ePrivacy Regulation, as drafted by the Parliament Proposal.

62 Art. 6.2.a) and b) ePrivacy Regulation, as drafted by the Parliament Proposal.

63 Art. 6.2.c) and Art. 6.3 ePrivacy Regulation, as drafted by the Parliament Proposal.

64 Art. 6.1 GDPR.

65 The Council proposal for ePrivacy Regulation allows for "further compatible processing of electronic communications metadata", in other words, compatible secondary uses of metadata, in line with the GDPR, based on pseudonymous data and provided that profiling of users is not done, and that the data protection authority is consulted.

4.3. Confidentiality of information stored in terminal equipment: On "cookies" and "tracking walls"

The ePD aims at protecting confidentiality of information in users' terminal equipment, such as computers or smartphones, by requiring consent of the user before storing or accessing the information. This information includes cookies,[66] beacons, spyware, pictures and videos, content of emails, calendar, etc.

Art. 5.3 ePD (one of the most polemic provisions in the Directive, often known as the cookie provision) allows cookies and other similar tracking technologies on condition that the user had given informed consent. This led to a so-called consent fatigue, derived from the increasing cookie banners which cause users facing requests of consent that are not read or understood, while some cookies are even installed without consent. In some aspects this consent rule is over-inclusive,[67] as it covers practices that are non-privacy intrusive, such as first party session or analytic cookies.[68] However, in other aspects it is under-inclusive, as it is unclear whether newer tracking technologies are covered by the provision. This is because nowadays tracking cannot only be pursued through active means, by "storing" or "gaining access" to users' devices and obtaining information through cookies and similar technologies. Tracking can also take place in a passive way,[69] through the use of identifiers "emitted" by users' devices, like wifi tracking or device fingerprinting.[70]. This later form of tracking is not clearly included under the ePD. [71] Also, there is a need to phrase the wording of the provision in a more technology neutral way to cover future technologies, for instance, those related to the Internet of Things, so that protection of communications is not dependent on the technique used, but rather on the potential impact on user's rights. Finally, the chronological gap between the entry into effect of the GDPR and the ePrivacy Regulation left several interpretational issues open that DPAs tried to address each in its own manner.[72]

66 Recital 30 of the GDPR explicitly recognises the possibility to associate cookie identifiers with personal data by saying: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This 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".

67 Article 29 Data Protection Working Party, Opinion 4/2012 on cookie consent exemption, WP 194, 7 July 2012.

68 First party cookies are the ones served by the website being visited and can only be read by it. For instance, if we visit a bookstore's website, it may place a cookie in our computer that is only readable by that same website. Third party cookies are issued by a different website than the one being visited. Privacy issues may arise here as users may not have reasonable expectations of this processing. This is the case, for example, when Google installs cookies on your computer while you navigate through other websites or when Facebook tracks you through its "like" buttons.

Further, cookies can be used for several purposes. For instance, session cookies are the ones that expire after you end the web session. These do not normally have privacy issues and can be used, for instance, by e-commerce sites to remember the items you put in your shopping cart or to save the language preferences chosen by a user. Analytical cookies can be used to notice when a new visitor access the website, analyse the flows and track the historical activity of a user in the website (for example, its response to ads campaigns).

Persistent cookies are those set with an expiration date and will remain on your computer until that moment, even if you exit the website or close your browser. For example, almost all the Google Analytics cookies are persistent. In another level we find zombie cookies also known as super cookies, which get automatically reinstalled after the user has deleted them. These have strong privacy implications as they circumvent people's choices when they delete those cookies.

69 Article 29 Data Protection Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, 19 July 2016, p.11.

70 Device fingerprinting allows to recognise a device, without the need of cookies, by other information transmitted by the device, such as the settings (language, screen resolution, timeframe, etc.). These settings are relatively unique and therefore enable for tracking. Therefore, is a way to track users without storing an identifier in users' terminal equipment or devices.

71 Nonetheless of the lack of clarity under the ePD as regards these tracking technologies, some cases of companies have already ended up in the company being fined. For instance, a case involving unlawful device fingerprinting practices is that of the Spanish telco provider Telefónica. In 2016, the company was fined by the National Data Protection Authority (AEPD) after being found it used a browser fingerprinting technology. Telefónica alleged the practice was necessary to provide the users' premium requested services. However, in the end it confessed it had been using browser fingerprinting technology with all kind of users from 2012 until 2015. Thus, Telefónica should have informed users about the use of this technology, which it did not, therefore infringing the Spanish e-commerce Act (which transposes ePD into national legislation) and was fined 20.000 €.

72 In July 2019 both the UK's ICO and France's the CNIL published guidelines on the use of cookies (for a comparative table see Voisin G/Boardman R, ICO and CNIL revised cookie guidelines, IAPP Resource Center, available at https://iapp.org/media/pdf/resource_center/CNIL_ICO_chart.pdf .

The REFIT evaluation found that the spirit of these provisions remains relevant and the protection against tracking technologies should be kept in the new law. The value of having these rules at EU level derives from the fact that each day more information is stored by users in their equipment and tracking techniques rising from the internet may often come from companies located in other countries. This means that, when the accessed information is personal data, any subsequent processing of that data, for instance, to create users' profiles, will be subject to the obligations and rights envisaged by the GDPR. Also, the definition of consent sought in the GDPR is the one applicable for these provisions.

Taking the above into account, the draft ePrivacy Regulation prepared by the Commission calls for a simplification of the rules on tracking technologies stored in users' terminal equipment. The new rules are aimed at being more user-friendly and covering all tracking technologies. First and foremost, as regards the term "terminal equipment" itself, today this is a wide concept which includes not only computers or phones but also devices of the Internet of Things: For instance, a smart watch that captures your vital signs when you exercise, a TV that remembers your favourite series and times to watch them or a smart toilet that stores information on how often you use it or the sugar level in your urine.

Under this light, Art. 8.1 ePrivacy Regulation sets that "[t]he use of processing and storage capabilities of terminal equipment and the collection of information from end users' terminal equipment, including about its software and hardware, other than by the user concerned shall be prohibited" and provides some exceptions.[73] This provision aims at protecting information inside users' devices.[74] As such, it covers the installation of unwanted or unnecessary cookies in users' devices, but also the installation of malware, device fingerprinting or technologies that enable, for instance, an app to turn on a microphone or a camera of the device to collect information.[75]

By way of exception, Art. 8.1 ePrivacy Regulation maintains the consent rule.[76,77] Other than the user, consent, the collection of information from terminal equipment is also allowed when:

- necessary for carrying on the transmission;[78]
- necessary for providing an information society service requested by the user (e.g. a session cookie to add things to shopping cart or to log in your email account);[79]
- necessary for web audience measuring in relation to first party analytic cookies.[80] In relation to this, while the Commission's draft only allowed for the measuring done by the provider himself, the amended text of the Parliament extended the permission to third parties acting on behalf of the provider or web analytics agencies acting in the public interest. Additionally, the Parliament added increasing guarantees for users, as thus requires data to be aggregated, the user being given the possibility to object and explicitly prohibits personal data being made accessible to any third party. [81] Also, as the

73 Art. 8.1 ePrivacy Regulation, as drafted by the Parliament Proposal.
74 This would leave out the scope of this Art., for instance, the content stored in the cloud.
75 LIBE report, p.79.
76 Art. 8.1.b ePrivacy Regulation. For deeper remarks on consent, see section 5 below.
77 Notably, legitimate interest is not one of the exceptions. Although this has been a point of contention for some observers, such as the Centre for Information Policy Leadership, Comments on the Proposal for an ePrivacy Regulation, 11 September 2017; available at:
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_proposal_for_an_eprivacy_regulation_final_draft_11_september_2017.pdf. On the other hand, other stakeholders have recommended legitimate interests not to be included among the exceptions, as the LIBE Report.
78 Art. 8.1.a ePrivacy Regulation.
79 Art. 8.1.c ePrivacy Regulation.
80 Art. 8.1.d ePrivacy Regulation.
81 In any case, it seems that this exception only includes first party analytics cookies, therefore leaving out third party tracking even if for the purpose of generating anonymised and aggregated statistics. As a consequence, providers would still need to request consent for tracking done by third party providers such as Google analytics.

term "web audience measuring" is not defined in the ePrivacy Regulation, and in order to make clear that it could not be interpreted as enabling user profiling, the Parliament modified the wording of the article to allow "measuring the reach of an information society service requested by the user".[82]

The Parliament added to the above Commission's original draft of the ePrivacy Regulation a fourth and fifth exceptions, following the advice of the LIBE report. As such, the collection of information from terminal equipment would be permitted when:

- necessary to ensure security updates of terminal equipment,[83] and
- necessary in the context of employment relationships for the execution of an employee's task, provided that there are no other monitoring purposes.[84]

Here again, the Parliament amended the initial wording of the Commission to move from mere necessity to "strict" or "technically" required necessity in order to provide for higher legal certainty and to align with the requirement of Recital 49 GDPR which allows for some processing operations for security purposes when strictly necessary.[85]

Apart from these suggested amendments, the most important change the ePrivacy Regulation has suffered under the Parliament's intervention is the inclusion of an explicit ban to the so-called "tracking walls", following the recommendations of WP29[86] and the LIBE report.[87] Tracking walls present users with a "take-it-or-leave-it" choice between privacy and access to a service, that is, when service providers deny users' access to a service or functionality on the ground that have not provided consent for processing, storing and collecting information that is not necessary for the provision of that service or functionality.[88] The originally proposed wording by the Commission states that "no user shall be denied access to any information society service or functionality, regardless of whether the service is remunerated or not, on grounds that he or she has not given consent (…) to the processing of personal information (…) that is not necessary for the provision of a service or functionality". This tracking is usually made through cookies and similar technologies in order to offer more targeted advertising to users, which is unquestionably more effective than other less personalised types of advertising, thus generating higher income rates.

82 Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP 247), of 4 April 2017, p. 18.
83 Art. 8.1.da ePrivacy Regulation.
84 Art. 8.1.db ePrivacy Regulation.
85 Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP 247), of 4 April 2017, p. 20.
86 Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP 247), of 4 April 2017, p. 15.
87 LIBE report, p. 92.
88 For a deeper analysis of tracking walls and the alternatives to a total ban of them see Frederik Zuiderveen Borgesius et al. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review, Vol. 3, No. 3, 2017.

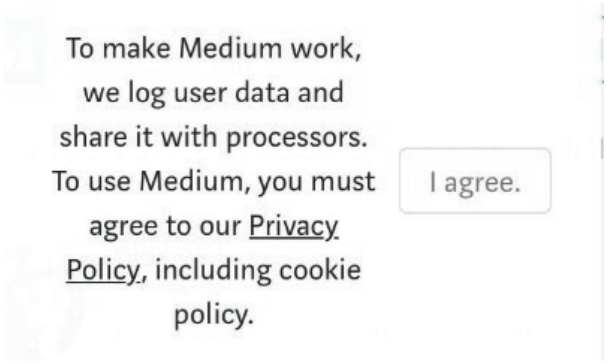

Image 2: Example of cookie wall. The online content provider Medium obliges users to accept cookies and other non-necessary data collection in order to read an article in the website.

The prohibition of tracking walls has opened a harsh debate around the ever-increasing business models based on the provision of services without any monetary exchange, and thus in exchange of valuable data that could serve to more efficient advertising, but also for other unexpected purposes. This debates also included services that indeed offer an alternative to data-paid options, such as monetary payment for subscription in the service. [89]

Further, tracking walls provisions and the possible coerced consent therein also expand to the GDPR. Specifically, Art. 6.4 GDPR on free consent as well as Art. 7 GDPR, which states that one of the factors to assess the validity of consent will be that the provision of a service is not made conditional to the provision of consent for the processing of personal data that is no necessary for such service.[90] Finally, the prohibition of tracking walls is also in line with Recital 5, under which the ePrivacy Regulation should not lower the level of protection granted by the GDPR.

4.4. Confidentiality of information emitted by users' terminal equipment

The ePD does not contain any provisions to protect confidentiality of information "emitted" by users' terminal equipment. This situation changes under the draft ePrivacy Regulation suggested by the Commission, which protects confidentiality of communications regarding wifi or bluetooth signals sent by smartphones and other devices, which enable for location tracking.[91] This protection therefore covers machine to machine communications when the information is related to a user (which has an increasing relevance in the times of internet of things).[92] For instance, in order to create a communication via wifi, devices broadcast their MAC-address in a constant manner to detect access points. The information captured by these signals can be used in different ways, from stablishing the communication between devices to other more intrusive purposes such as detection of location patterns or counting visitors.[93]

89 The Council proposal lies in an opposite path to that of the Parliament and specifically allows tracking walls in Recital 20 for websites where the content is provided without a monetary payment, provided that the visitor is presented with an alternative to tracking, such as a subscription service.
90 See Art.s 6.4 and 7 GDPR.
91 LIBE report, p. 86.
92 European Parliament, Explanatory Statement on the Proposal for a new Regulation on Privacy and electronic communications. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN&language=en#title2.
93 WP29 (Wp 240), p. 11.

In order to accomplish that Art. 8.2 of the original Commission's draft establishes that "the processing of information emitted by terminal equipment to enable it to connect to another device and/or to network equipment shall be prohibited", unless any of the exceptions apply. However, this provision has suffered what may be a significant modification in the Parliament's version. The first version, as phrased by the Commission set two exceptions where this data could be processed: (i) where it was necessary for the purpose of establishing the connection and (ii) where a clear and prominent notice is displayed to inform the user, in the same terms as under Art. 13 GDPR, that personal data is being collected together with information on the measures that the user can take to stop or minimise the collection, and provided that appropriate security measures are taken in line with Art. 32 GDPR.

Giving the sensitive and highly revealing nature of location data, it was noticeable that the provision seemed to suggest that user device location tracking was allowed without consent[94] and without requiring an opt-out right. This would have decreased the level of protection set in the GDPR, where in a similar situation an opt-out right should be granted if no consent was needed. Thus, this would contradict the aim, expressed in the preamble of ePrivacy Regulation that it should not lower the level of protection enjoyed by natural persons under the GDPR.[95] In this regard, both the EDPS[96] and the WP 29[97] called for improvements in this provision.

Thus, the amended version suggested by the Parliament substitutes the clear and prominent notice to users by the requirement of informed consent. It also builds on the measures to mitigate the risks, such as purpose limitation to mere statistical counting, limit tracking in time and space and to what is strictly necessary for the purpose, deletion or anonymization of data after the purpose is fulfilled and object rights for users. This addition is important since it significantly raises the bar for providers to be able to process users' data. Merely requiring a notice would otherwise legitimise the collection of user information captured through, for instance, wifi signals, which may reveal location and other people's private data in unnoticed ways and would incentivise the already high use of pervasive sensors.

5. The issue of consent and its effect on software architecture and settings

Consent is the central lawful ground under the e-Privacy framework, which allows for several processing activities if users have given it. However, the REFIT evaluation of the ePD showed that some provisions created an unnecessary burden on businesses and consumers. For example, the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives. There is broad acknowledgement that nowadays end-users face requests to accept cookies and other tracking technologies which are not read or understood, leading to situations where users accept terms without realising the consequences. In this way it is possi le that tracking even takes place without, lawful, consent. The consent rule under the ePD is both over-inclusive, as it covers non-privacy intrusive practices, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access or storage in the device.

94 European Parliamentary Research Service, Briefing on the EU legislation in process: Reform of the e-Privacy Directive, of September 2017, p. 7. Available at:
http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf.
95 LIBE report, p. 84.
96 EDPS 2017/6, p. 20.
97 Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP 247), of 4 April 2017, p. 11.

The Commission, in its ePrivacy Regulation proposal, aims to tackle these issues.[98] For that, Art. 9.1 ePrivacy Regulation establishes that the definition of consent shall be that of the GDPR. This follows the line of ePD, which also referred to data protection law for a definition of consent. Under the GDPR, consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art. 4.11 GDPR).

Yet, individuals often face consent requests that are not user friendly, and some of them are even designed to be unclear. For that reason, Art. 9.2 ePrivacy Regulation aims at providing more user-friendly ways to express consent. Specifically, the Art. as drafted by the Commission, states that: Art. 9.2: "Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Art. 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet" (***emphasis added***).

That is, if technically feasible, consent for cookies and other similar tracking technologies covered by Art. 8.1.b can be expressed through technical settings of your internet browser or any other software application that provides access to the internet. These are the so-called Do Not Track standards. Do Not Track standard (DNT) is a mechanism that enables people to express their choice on cookies and other tracking technologies by setting their browser accordingly (or by using similar ways that apply to any other technology to centralise consent settings). In practice, DNT standards mean that users are be able to tell their browser in one go which their cookies preferences are, rather than giving consent each time they visit a website. This would function to avoid presenting users with endless cookie banners (or similar consent requests) every time they do routine actions such as entering a website. Instead, once a user has turned on the DNT setting, the browser sends a signal to websites, analytics companies, ad networks, plug in providers, and other web services you encounter while browsing, and request that the web application refrain from that person.[99]

However, under the ePD wording, some websites can still lawfully decide to track you, as they are not compelled to respect those settings. Even worse, some websites would choose to act upon DNT signals as if they meant "do not send ads" rather than "do not collect and process data about me and this device".[100] The Commission therefore claims that centralising consent in software together with expanding the exception for cookie consent (i.e. not requiring consent for necessary or innocuous cookies) would significantly reduce the amount of notices users face, avoiding the current consent fatigue, and leading to saving costs for many businesses that could work with no cookie banners.[101]

98 Explanatory Memorandum of the Proposal, p.5.
99 Future for Privacy Forum. See https://allaboutdnt.com/.
100 Lilian Edwards, p. 19.
101 Explanatory Memorandum of the Proposal, p.6.

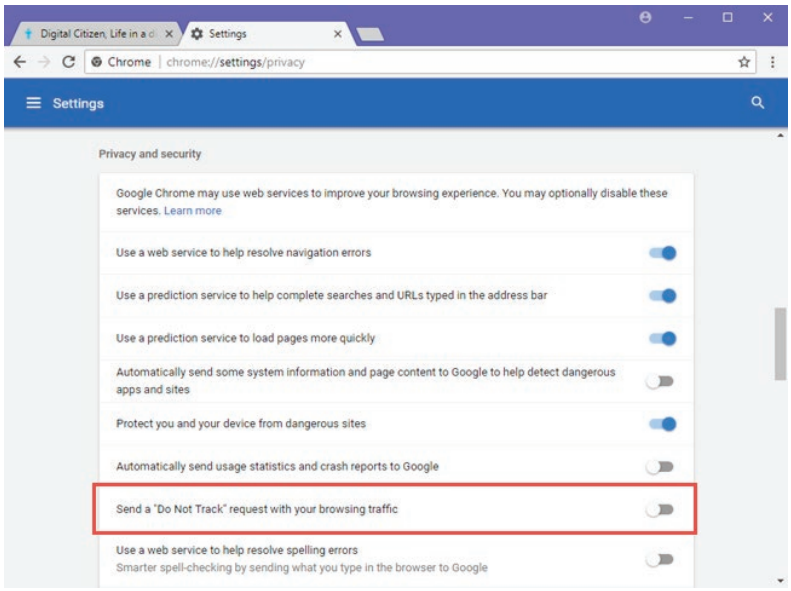

Image 3: Example of how to enable Do Not Track (DNT) in Chrome, Firefox, Edge, Opera and internet Explorer.[102]

The LIBE report however highlighted that the wording of the Commission had the important drawback of making DNT standards optional. Accordingly, the report advised making them obligatory to comply with. It also recommended that DNT standards should apply to all tracking technologies, to cover other contexts such as the Internet of Things. Construing from that advice, the Proposed text of the Parliament reads:
Art. 9.2: "Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Art. 8(1), consent may be expressed or withdrawn by using technical specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1. When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party" (***emphasis added***).

In this way the Parliament reinforces the provisions on DNT standards in several ways. Firstly, making them binding rather than optional. Secondly, by asking that the wording be more neutral from a technological perspective, as it does not refer to software application anymore but rather to the broader expression of "technical specifications". Third, granular consent is now provided for by allowing "for specific consent for specific purposes and with regard to specific service providers". Finally, the settings can be used not only to give consent but also to withdraw it.

Still, it is noticeable that both the Commission and the Parliament direct the DNT standards only to Art. 8.1.b, that is, granting protection only to information stored in terminal equipment (like cookies and similar trackers). This would leave out of the protection of DNT standards the activities covered by Art. 8.2 ePrivacy Regulation, that is, information emitted by terminal equipment (such as wifi and similar signals). This would be true even after the Parliament rephrased Art. 8.2 in order to require informed consent instead

102 See: https://www.digitalcitizen.life/enable-do-not-track-dnt-chrome-firefox-edge-opera-internet-explorer

of giving a mere clear and prominent notice for cases other than when it is necessary for establishing the connection. Following these changes, and in line with the protection granted under Art. 9, we argue that this provision should be amended to also include Art. 8.2 in order to provide the ePrivacy Regulation with internal coherence.[103]

Finally, Art. 9.3 ePrivacy Regulation states that end-users will be given a right to withdraw consent. The text of the Commission restricted the scope of this right to the consent given in the processing of content from electronic communications (Art. 6.3.a and b ePrivacy Regulation) and its related metadata (Art. 6.2.c ePrivacy Regulation) and provided for users being reminded of their right of withdrawal every six months. In this regard, the LIBE report advised that the provision be amended to also include the possibility to withdraw consent to use cookies and similar tracking technologies, and that the reminder applied also to browser settings. Lastly, the report also added on the necessity for banning cookie walls. This integral protection is seen as a way to better guard consumers against the intrusive nature of online behavioural advertising and the current extended profiling activities.

The Parliament indeed followed this recommendation to expand the scope of Art. 9.3 and established that the right to withdraw consent will also cover the processing of information stored in terminal equipment, such as cookies (Art. 8.1.b) and the processing of information emitted by terminal equipment (such as wifi and bluetooth) (Art. 8.2). The Parliament also suggests that cookie walls be banned, although this provision was inserted in Art. 8 (as has been already seen above) rather than in Art. 9. As regards the reminders, the Parliament eliminated this obligation for providers. Lastly, it also added that, any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and the protection of personal data.

Art. 10 ePrivacy Regulation then deals with the information and options for privacy settings to be provided. The Commission's proposal established the obligation of providers of software permitting electronic communications to "offer the option to prevent third parties from storing information on the terminal equipment of an end user or processing information already stored on that equipment". This provision is directed at providers of software such as internet browsers or app developers. This would entail changes for providers of browsers to develop these options so as to require a clear affirmative action from the end-user to signify agreement. In addition, software providers should offer the option to prevent third party cookies, informing the user and requiring making an election about the preferred privacy settings before finalising the installation. By means of this, providers should give users several options to choose from and configure their settings to accept or reject being tracked by third parties. This is done by giving options such as:[104]

- ☐ Always accept cookies.
- ☐ Never accept cookies.
- ☐ Reject third party cookies.
- ☐ Only accept first party cookies.

103 In relation to this, the authors of the LIBE Report sent a communication to MEPs highlighting the need of amending Art. 9.2 ePrivacy Regulation in the sense discussed, so as to grant the same level of protection to information emitted by terminal equipment.

104 See recital 23.

Consequently, if the Commission's proposal is adopted, more users would become aware of existing tracking techniques and different options to protect themselves from their behaviour being tracked. The problem of this wording as shaped by the Commission is that, nowadays, the default settings for cookies are configured in most current browsers to accept all cookies. This means, only providing options to change the pre-set "accept all cookies" option infringes the GDPR principles of data protection by design and by default (see Art. 25 GDPR), as, if these principles were followed, the pre-selected option should be the most privacy protective one (i.e "reject all cookies").

In view of these shortcomings in the Commission's original wording the Parliament suggested that this provision be amended as follows. First, providers of software permitting electronic communications must pre-configure their systems to have, by default, the most protective options. No options would be given (as no consent would be required) for information that is collected from end-users' terminal equipment when it is strictly necessary for carrying out the transmission or for providing an information society service requested by the end-user (for example to adapt the screen size to the device, or to remember items in a shopping basket). Second, the user would be given granular options to choose from and to consent distinct category of purposes. These options would be presented upon installation of the software but would also be available after it. Third, it is provided that, even if the user has indicated his preferences on the general settings, he should be allowed to make exceptions and give specific consent (for instance, allowing the storing of cookies from a specific website although your preferences are set in a more protective way for other websites). Finally, information should be easily accessible and allow users to give informed consent.[105]

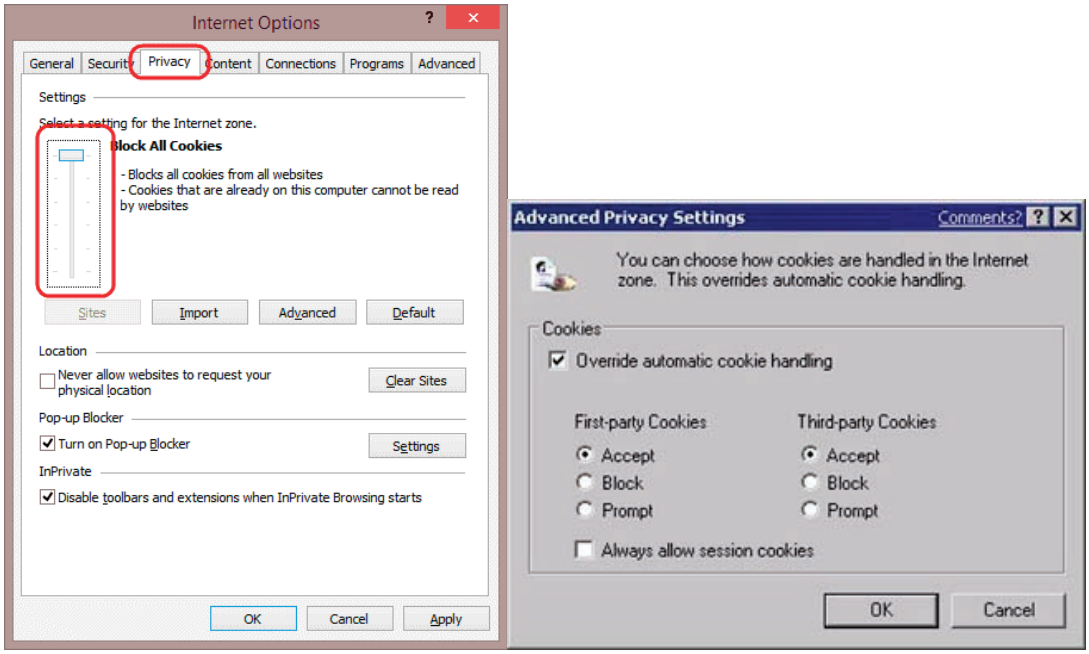

Image 4: Example of browser cookie settings.

In essence, the e-Privacy framework relies on consent to legitimise uses of data that are otherwise not necessary. This follows from the traditional European data protection rules, heavily based on consent as a means for individuals to exercise their autonomy and show self-determination.

105 The Council text, however, proposes to delete Art. 10 on privacy settings, which would cause that s significant smaller number of users would be aware of the existence of more protective privacy settings.

Consent, however, has shown shortcomings in online environments. Take as an example the consent fatigue mentioned before in this paper. Some authors have even argued against keeping consent as a key tool for protecting individuals. In this regard, one would immediately think of Helen Nissebaum and her statement "stop thinking about consent: it isn't possible and it isn't right".[106] Lillian Edwards has also shared a similar opinion by stating that "real consent may in fact be the ultimate luxury good of the elite: well-educated, time-rich and with access to various options".[107] Critiques have also been made that consent places the responsibility on the individual to understand the information is being served and provide a means of probe for the controller that the election made by providing consent was informed and free.

On the other hand, leaving consent aside as a means to reflect one's preferences may provide for a playing field where controllers process data by default, on the assurance that few users would exercise their rights or by providing insufficient information about obscure practices. In the preliminary stages of the drafting process of the ePrivacy Regulation, the EDPS explicitly argued that consent as a basis for processing data provides a higher level of protection than other grounds observed in the GDPR: "[b]y requiring consent for the processing of traffic and location data, the current ePrivacy Directive offers a higher level of protection than the GDPR. The GDPR, at least potentially, allows other legal grounds, such as legitimate interests or performance of a contract. (…) In order to better protect the confidentiality of electronic communications, the EDPS recommends that the ePrivacy Directive maintains and strengthens the current consent requirement (…)".[108]

No matter what, in the end it seems that, at least for the moment, consent may be determined as the basis to enable uses for electronic communications data that are not necessary. The EDPB already showed that other options were not forgotten by any means, but just not considered viable, when stated that "[u]ser consent should be obtained (…) before processing electronic communications data (…). There should be no exceptions to process this data based on the 'legitimate interest' of the data controller, or on the general purpose of the performance of a contract".[109] These tensions between the arguments for and against consent gave raise to principle of data protection by default, enshrined in Art. 25 GDPR and reflected in Art. 10 ePrivacy Regulation, and which are expected to be solve or, at least, reduce strains.

106 Scott Beritano, Stop Thinking About Consent: It Isn't Possible And It Isn't Right. Interview to Helen Nissebaum for Harvard Business Review, 2018.

107 Lilian Edwards, Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling. L Edwards ed Law, Policy and the Internet, Hart, 2018, p. 50.

108 European Data Protection Supervisor, Preliminary EDPS Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC), of 22 July 2016, p. 17.

109 European Data Protection Board (EDPB), Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 25 May 2018, p. 3.

6. Conclusions

In recent years, the European Union has been immersed in the thorough task of modernizing key norms in order to boost the Digital Single Market. 2016 was the kick off date for the future e-Privacy Regulation, when the first assessments for a modification of the e-Privacy Directive were made. In the beginning of 2017 European Commission presented a proposal for ePrivacy Regulation with the aim for it to be applicable on 25 May 2018, simultaneously with the GDPR. However, this due date has suffered several postponements and at the moment of drafting this paper (summer 2019), after the June 2019 elections and the appointment of a new Commission there is no foreseeable end.

Purpose of this contribution has been to explain the raison d etre and wording of certain of the Commission's originally drafted provisions in juxtaposition with the Parliament's views. While the intervention of the Council would have offered a more complete picture, at the time of drafting this paper its official position was not available yet. In this way we believe that research will be facilitated, once the final ePrivacy Regulation provisions have seen the light.

Our choice of provisions was based on two factors: First, our perception of what is important, or at least more important than others, in the draft of the ePrivacy Regulation; and, Second, what has already attracted the attention of parties relevant to the law-making process (DPAs, the EDPS, academics, the industry, NGOs, etc.). While the ePrivacy Regulation promises to be an important text of many layers, given its aim and importance of the electronic communications field, certain of it aspects seem to prevail from others. Having said that, a critical analysis of all the ePrivacy Regulation provisions under the same light (Commission's draft vs the Parliament's amendments) we believe that would have been equally important and useful in the field.

Our examination of the above provisions has demonstrated that the Commission has succeeded in updating the e-privacy regulatory framework onto current circumstances taking into account accumulated know-how and the technological state of the art, such as extended digitization, the Internet of Things or big data. It remains however to be seen whether provisions drafted in 2017 retain their relevance once the final ePrivacy Regulation is released. The e-privacy framework is specific and connected to one of the most dynamic fields of technology. As such, it needs constant updating in order to remain relevant, as after all evidenced by its frequent updates in comparison to general data protection law. Whether, therefore, the Commission has achieved its purpose of specificity and granularity remains debatable.

From its part, the Parliament has intervened in a useful and relevant manner, strenghtening the protection of individual rights and providing clarifications wherever needed. In this way it confirms its role as an important player in the EU law-making process. The evolution of the text from the Commission's version to the Parliament's one has shown an increased tightening of providers' obligations to protect user's rights. Although the final wording is not known yet, and significant changes may occur, we consider it important that the ePrivacy Regulation maintains its current vacation for durability and technology-neutral approach, so that advances in the future years will not undermine the protection granted to users.

References

Article 29 Data Protection Working Party, ***Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)***, WP 247, 4 April 2017.

Article 29 Data Protection Working Party, ***Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)***, WP 240, 19 July 2016.

Article 29 Data Protection Working Party, ***Working Document 02/2013 providing guidance on obtaining consent for cookies***, WP 208, 2 October 2013.

Article 29 Data Protection Working Party, ***Opinion 4/2012 on cookie consent exemption***, WP 194, 7July 2012.

Big brother Watch. Briefing Note: ***Why Communications Data (Metadata) Matter***, 2014.

Body of European Regulators for Electronic Communications, ***Report on OTT services***, January 2016.

Case C-582/14 ***Patrick Breyer v Germany***, ECLI:EU:C:2016:779.

Case C-673/17 ***Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände***.

Cases C-293/12 and C-594/12 ***Digital Rights Ireland and Seitlinger and Others***, ECLI:EU:C:2014:238.

Cases C-203/15 and C-698/15 ***Tele2 Sverige AB and Secretary of State for the Home Department***, ECLI:EU:C:2016:970.

Centre for Information Policy Leadership, ***EPR vis-à-vis GDPR, A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation***, 2018.

Centre for Information Policy Leadership, ***Comments on the Proposal for an ePrivacy Regulation***, 11 September 2017.

Council of the European Union, Outcome of the 3623rd Council meeting, Transport, Telecommunications and Energy, Luxembourg, 7 and 8 June 2018. Available at: https://www.consilium.europa.eu/media/35597/st09810-en18.pdf

Danhoé Reddy-Girard, ***European ePrivacy Regulation: What non-European companies need to know***, 31 May 2018.

Datainspektionen, Request for Reply and Further Clarification, 18 January 2019. Available at: https://www.datainspektionen.se/globalassets/dokument/ovrigt/google---request-for-reply-and-further-clarification---skrivelse-till-tillsynsobjekt.pdf.

Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

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, 31.7.2002, amended two times by Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009

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 [1995] OJ L 281/31.

European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.

European Commission, 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, 6 May 2015.

European Commission, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC SWD(2017) accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.

European Data Protection Board (EDPB), ***Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications***, 25 May 2018.

European Data Protection Supervisor (EDPS), ***Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)***, of 24 April 2017.

European Data Protection Supervisor (EDPS), ***Preliminary Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC)***, of 22 July 2016.

European Parliament, Report on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 20 October 2017.

European Parliamentary Research Service, Briefing on the EU legislation in process: Reform of the e-Privacy Directive, of September 2017.

Frederik Zuiderveen Borgesius, Sanne Kruikemeier, Sophie C Boerman and Natali Helberger, ***Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation***. European Data Protection Law Review, Vol. 3, No. 3, 2017.

Frederik Zuiderveen Borgesius, Joris van Hoboken, Ronan Fahy, Kristina Irion, Max Rozendaal, ***An assessment of the Commission's Proposal on Privacy and Electronic Communications***, Study for the LIBE Committee of the European Parliament (LIBE Report), 2017.

Gerrit-Jan Zwenne, Quinten Kroes and Joost van Eymeren, ***EPR vis-à-vis GDPR A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation***, Study prepared for Centre for Information Policy Leadership, 19 July 2018.

Lilian Edwards, ***Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling***. L Edwards (ed.), Law, Policy and the Internet, Hart, 2018.

New York Times, AP Exclusive: Google Tracks Your Movements, Like It or Not, 13 August 2018. Available at: https://www.nytimes.com/aponline/2018/08/13/us/ap-apfn-us-google-location-tracking-abridged.html.

Vagelis Papakonstantinou, Paul de Hert, 'The Amended EU Law on EPrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection

of Intellectual Property Rights', *The John Marshall Journal of Computer & Information Law* XXIX, no. 1 (Fall 2011): 101–47

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 Government of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

Scott Beritano, Stop thinking about consent: it isn't possible and it isn't right. Interview to Helen Nissebaum for Harvard Business Review, 2018. Available at: https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right

Sophie Stalla-Bourdillon, Evangelia Papadaki, Tim Chown. *Metadata, traffic data, communications data, service use information…What is the difference? Does the difference matter? An interdisciplinary view from the UK*. Serge Gutwirth & Ronald Leenes, Data Protection on the Move, Springer 2015.

Telefónica, Smart steps project. Available at: https://www.wholesale.telefonica.com/es/services/digital/big-data/smart-steps/.

The Independent, Google admits giving hundreds of firms access to your Gmail inbox, 21 September 2018. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-data-sharing-email-inbox-privacy-scandal-a8548941.html.

The Inquirer, Google is being sued over 'privacy-invading' location data collection, 21 August 2018. Available at: https://www.theinquirer.net/inquirer/news/3061399/google-is-being-sued-over-privacy-invading-location-data-collection.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

BRUSSELS PRIVACY HUB