First the GDPR, Now the Proposed ePrivacy Regulation

By W. Gregory Voss

On January 10, 2017, less than nine months after the General Data Protection Regulation (GDPR) was adopted by the European Union,[1] the European Commission issued its proposal for a new ePrivacy Regulation.[2] In analyzing this new proposal, this article first places European Union ePrivacy legislation in context before detailing the main points of the proposed ePrivacy Regulation, then discusses reactions to the proposed Regulation, and outlines the legislative process.

INTRODUCTION

The current ePrivacy Directive[3] is European Union legislation that is complementary to the Data Protection Directive,[4] soon to be repealed and replaced by the GDPR, in the field of European Union privacy and data protection laws, in that it deals with privacy in the electronic communications sector, much as the separate sector-specific communications privacy legislation in the United States affecting the telecommunications sector complements other privacy legislation.[5] In the European Union, the line of demarcation is slightly blurred in the sense that in addition to other issues such as traffic and location data collected by providers of electronic communications services (an expansion from earlier legislation's coverage of "telecommunications services"), the ePrivacy Directive applies to e-marketing, as does the GDPR:

> The e-Privacy Directive applies to e-marketing, dealing with a gamut of issues in this sector such as (a) an opt-in requirement to receive commercial communications and the concept of prior consent, (b) spam or "unsolicited communications" and the existing customer exception, (c) recent guidance on the existing customer exception to the general rule, and (d) notice and transparency requirements.[6]

The 2009 amendments to the ePrivacy Directive specifically addressed the use of cookies in the e-marketing context, providing that informed consent has to be obtained prior to installing a cookie on a computer or other device such as a tablet or a smartphone, with an exception being made for certain technical cookies, and those strictly necessary in order to provide a service that the user requested.[7] In order to obtain informed consent for collection of information using cookies for online behavioral advertising, ad network providers should provide information interactively, directly on the screen, in a visible and understandable manner, in accordance with guidance from the European Union's Article 29 Data Protection Working Party (an independent advisory panel that will be replaced by a new European Data Protection Board under the GDPR).[8]

Later, in 2015, the European Commission issued the results of a study that it had commissioned on the implementation, effectiveness of the ePrivacy Directive and its compatibility with the GDPR, which indicated some flaws in the implementation (or "transposition") of the ePrivacy Directive into national European Union Member State law.[9] It is worth remembering that, according to the Treaty on the Functioning of the European Union (TFEU), as in force today, it is left up to the "national authorities" of the Member States to choose the "form and methods" of the implementation of directives, unlike

W. Gregory Voss *is a Professor of Business Law at Toulouse Business School, University of Toulouse, in France. He is a member of the Research Institute in European, International and Comparative Law (IRDEIC), and a member of the board of directors of the French Academy of Legal Studies in Business. He may be contacted in connection with his research at* g.voss@tbs-education.fr.

regulations that are directly applicable in all of the Member States of the European Union in the same form.[10]

The study led to a public consultation[11] and review of the ePrivacy Directive in 2016. The result of this work was the proposed ePrivacy Regulation, which is part of the European Commission's Digital Single Market strategy, intended to help Europeans benefit from the Digital Single Market (DSM), with its expected positive effects on society, the economy, and individual citizens' lives.[12] More specifically, the proposed ePrivacy Regulation is meant to make "protection of privacy and personal data a reality in the internet," according to the European Commission:

> The proposal for a revised ePrivacy **Regulation** would complement the GDPR while also ensuring alignment with the relevant rules of the GDPR. It will further increase legal certainty and **the protection of users' privacy online**, while also increasing business use of communications data, based on users' consent. (citations omitted)[13]

MAIN POINTS OF THE PROPOSED ePRIVACY REGULATION

This discussion of the main points of the proposed ePrivacy Regulation focuses on those main issues that are of interest to players other than the traditional telecommunications companies (whether fixed-line or cellular), namely: territorial scope; material scope; the interface of the proposed ePrivacy Regulation with the GDPR; provisions on cookies; confidentiality of communications; application of the concept of consent; unsolicited direct marketing communications; and enforcement measures.

TERRITORIAL SCOPE

The proposed ePrivacy Regulation would apply when electronic communications services (*see* definition in section below) are provided to end-users in the European Union, and when they are used, as well as to the protection of information related to the terminal equipment of end-users located in the European Union, whether or not the provider of the service is established in the European Union. If the service provider does not have an establishment in the European Union, it would have to designate a representative established in one of the EU Member States where the end-users of such services are located.[14]

Thus, this drafting of the territorial scope article results in the proposed ePrivacy Regulation having a worldwide scope, if adopted in this form, so long as the end-users of electronic communications services are in the European Union. This is similar to the extension of the territorial scope in the GDPR.

MATERIAL SCOPE

The proposed ePrivacy Regulation is stated to apply "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."[15] The term "electronic communications service," is defined by cross-reference to the proposed Directive Establishing the European Electronic Communications Code,[16] as are several other terms. There, "electronic communications service" means:

> a service normally provided for remuneration via electronic communications networks, which encompasses 'internet access service' as defined in Article 2(2) of Regulation (EU) 2015/2120; and/or 'interpersonal communications service'; and/or services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.[17]

By the use of this definition, it is meant to bring within the scope of the proposed ePrivacy Regulation, and its requirements regarding confidentiality, "Voice over IP, messaging services and web-based e-mail services,"[18] often referred to as "over-the top" (OTT) services, and machine-to-machine communications in the Internet of Things (IoT).[19] The extension of the ePrivacy Regulation to new actors such as

so-called OTT players, who are seen increasingly to compete with existing telecommunications players, without being required to respect the same rules, is a policy issue within the DSM strategy. The idea is to update legislation so as to create a "level playing field," with the principle that "comparable digital services should be subject to the same or similar rules."[20]

Nonetheless, the proposed ePrivacy Regulation does not apply to "closed groups of end-users such as corporate networks," as access to those are limited to members of the group,[21] and not made available to the public.

INTERFACE OF THE PROPOSED ePRIVACY REGULATION WITH THE GDPR

Succinctly put, while "the GDPR ensures the protection of personal data, the ePrivacy Directive ensures the confidentiality of communications, which may also contain non-personal data and data related to a legal person"[22] (only individuals or "natural persons," and not legal persons, are protected by the GDPR). A similar comment could be made about the proposed ePrivacy Regulation, meant to repeal and replace the ePrivacy Directive. The proposed ePrivacy Regulation refers to definitions in the GDPR,[23] including for the key concept of consent (discussed below) of end-users.

In addition, security requirements of the GDPR (as well of those of the European Electronic Communications Code) will apply under the proposed ePrivacy Regulation.[24] This may be seen, for example, as a requirement for the collection of information emitted by an end-user's terminal equipment to enable it to connect to another device or network equipment,[25] in which case the information requirements of the GDPR also would apply. Furthermore, reference to the supervisory authorities defined in the GDPR also is made,[26] and will be discussed briefly below.

Finally, the GDPR (referred to in the legislative proposal as "Regulation (EU) 2016/679") is referred to through the text of the proposed ePrivacy Regulation, which may be considered normal, as the provisions of the proposed ePrivacy Regulation "particularize and complement" the GDPR, "by laying down specific rules" for the purposes of protecting fundamental rights and freedoms in the provision of electronic communications services, and ensuring free movement of electronic communications data and electronic communications services within the European Union.[27] As a recital explains, the proposed ePrivacy Regulation "does not lower the level of protection enjoyed by natural persons" under the GDPR.[28]

PROVISIONS ON COOKIES

The general rule that consent is required for the use of cookies, is maintained in the proposed ePrivacy Regulation. However, the process has been simplified. As summarized in a press release from the European Commission:

> The so called "cookie provision", which has resulted in an overload of consent requests for internet users, will be streamlined. New rules will allow users to be more in control of their settings, providing an easy way to accept or refuse the tracking of cookies and other identifiers in case of privacy risks. The proposal clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (*e.g.*, to remember shopping cart history). Cookies set by a visited website counting the number of visitors to that website will no longer require consent.[29]

Some of the aspects of this simplification are seen in Article 8 of the proposed ePrivacy Regulation. There the general prohibition against using terminal equipment processing and storage capabilities and collecting information from end-user terminal equipment, without end-user consent, is subject to exceptions where necessary to carry out the transmission of the electronic communication over a network, or where necessary for providing an information society service requested by the end user, or where necessary for web audience measuring when carried out by the provider of such information society service.[30]

In addition, the proposed ePrivacy Regulation requires providers of software permitting electronic communications (such as Web browsers), or those allowing retrieval and presentation of information to make an option available to prevent third parties from storing information on the end-user's terminal

equipment, or processing such information. Upon installation of the software, the end-user should be informed about privacy settings, and his or her consent collected for a setting. If the software already is installed on a terminal, the provisions must then be complied with on the software's update, but no later than within three months of the date when the ePrivacy Regulation becomes applicable.[31]

CONFIDENTIALITY OF COMMUNICATIONS

The general rule is that electronic communications data is to be kept confidential, and that "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing" of such data by anyone other than the end-user is prohibited.[32] A recital to the proposed ePrivacy Regulation makes it clear that the principle of confidentiality applies generally: "to current and future means of communication, including calls, internet access, instant messaging applications, email, internet phone calls and personal messaging provided through social media."[33]

The proposed ePrivacy Regulation then goes on to enumerate exceptions to the general rule, where processing by providers of electronic communications networks and services is permitted in the case of electronic communications data: Where necessary for transmission of the communication (for so long as necessary), or where it is necessary for network or service security and technical purposes (for so long as necessary).[34] In addition, certain exceptions also exist to allow providers of electronic services to process electronic communications metadata when: necessary to meet mandatory quality of service requirements under the Directive establishing the European Electronic Communications Code or under Regulation (EU) 2015/2120 (for so long as necessary for that purpose); necessary for billing, interconnection payment calculations, or detecting or stopping fraudulent or abusive use of, or subscription to, electronic communications services; or end-user has given consent for one or more specified purpose(s), so long as the purpose(s) could not be fulfilled by processing anonymous information.[35]

Finally, certain exceptions also exist to allow providers of electronic services to process electronic communications content: (1) for the sole purpose of providing a specific service to an end-user where the latter has given their consent, and (2) where such provision cannot be fulfilled without such processing, or (3) where all end-users concerned have given their consent to the processing for specified purposes, and that cannot be fulfilled by processing anonymized information. In the latter case, the service provider must consult the relevant supervisory authority (and certain of the conditions for prior consultation of the GDPR are applicable).[36]

Thus we see that there is some flexibility built into the proposed ePrivacy Regulation for processing of electronic communications data and metadata, but that EU data protection law principles such as purpose limitation, and data quality—fair and lawful processing (where consent is required for a lawful basis for processing), or proportionality (where there is a requirement that the processing is not excessive to the purposes and where some other method such as using anonymous information does not fulfill the purposes) apply.

Article 7 of the proposed ePrivacy Regulation complements this regarding data retention, by providing that once electronic communication content is received by the intended recipient(s), the provider of electronic communications content shall erase or anonymize such content, that electronic communications metadata shall be erased or anonymized by the electronic communications service provider when it is no longer needed for transmission of the communication, and that when the processing of electronic communications metadata is needed for billing, the metadata will be kept only for so long as the bill may lawfully be challenged or payment pursued under national law.[37]

APPLICATION OF THE CONCEPT OF CONSENT

In the section above, there are two cases enumerated where the consent of end-users may serve as a legitimate basis for processing of electronic communications metadata or electronic communications content. That consent may be withdrawn by the relevant end-user at any time, without such withdrawal affecting the lawfulness of the processing based on

consent before its withdrawal. The end-user is to be reminded at periodic intervals of six months of the possibility of withdrawing consent, for so long as the processing continues.[38]

When consent of an end-user is required this means consent as defined in the GDPR.[39] That instrument provides that consent means:

> any freely given, specific, informed and unambiguous indication of the [end-user's] wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing ….[40]

In a provision that would add new flexibility in the law, discussed above, the proposed ePrivacy Regulation allows that consent for the use of processing and storage capabilities of an end-user's terminal equipment (hardware and software) may be obtained by using "technical settings of a software application enabling access to the internet."[41] This could be the case when an end-user sets their Web browser options to accept cookies, for example.

UNSOLICITED DIRECT MARKETING COMMUNICATIONS

Consent, discussed immediately above, may be the basis for allowing the sending of direct marketing communications to end-users who are natural persons.[42] An exception, that already existed under the ePrivacy Directive, as amended in 2009, has been continued, with few changes: When email contact details are obtained from existing customers in connection with a sale or purchase of a product or service, these details may be used for direct marketing communications regarding the same person's similar goods or services, so long as the customers are given an easy way to object, free of charge, both when the details originally are collected and then at each time a message is sent.[43]

When electronic communications services are used to send the direct marketing messages, the marketing nature of the communication must be indicated and the person on whose behalf the message is sent must be identified. End-users shall be informed about how to exercise their right to withdraw their consent for receiving such messages.[44]

ENFORCEMENT MEASURES

The enforcement measures contained in the proposed ePrivacy Regulation refer often to the GDPR. The same independent supervisory authority responsible for monitoring application of the GDPR is responsible for monitoring the proposed ePrivacy Regulation,[45] and the European Data Protection Board, established under the GDPR, has the power to ensure the consistent application of the proposed ePrivacy Regulation.[46]

The end-user has the same remedies as under the GDPR: right to lodge a complaint with a supervisory authority; right to an effective judicial remedy against a supervisory authority; and right to an effective judicial remedy against a data controller or processor.[47] Other natural or legal persons who are adversely affected by an infringement of the proposed ePrivacy Regulation, who have a legitimate interest in the ceasing or prohibition of alleged infringements, may bring legal proceedings. This may include the relevant electronic communications services provider.[48] An end-user who has suffered damages as a result of an infringement, will have a right to compensation for the damages from the infringer unless the latter proves that it is not in any way responsible for the triggering event.[49]

In a similar manner to the GDPR, administrative fines may be assessed for an infringement of the proposed ePrivacy Regulation, going up to a maximum of €10,000,000, or in the case of an undertaking, the greater of that figure and 2 percent of the total worldwide annual turnover of the preceding financial year, in the case of certain infringements under Articles 8, 10, 15, and 16 of the proposed ePrivacy Regulation.[50] In the event of certain infringements under Articles 5, 6, and 7 of the proposed ePrivacy Regulation, the maximum fine that may be assessed is €20,000,000, or in the case of an undertaking, the greater of that figure or 4 percent of the total worldwide annual turnover of the preceding financial year.[51] The latter also is the case for non-compliance with an order by a supervisory authority under Article 18.[52] Furthermore, Member States may assess penalties, in particular for infringements where there are not administrative fines.[53] Thus, as is the case with the GDPR, the large potential fines of the proposed ePrivacy Regulation should incite companies whose activities fall under such proposed legislation to develop adequate compliance measures.

Now, our attention will shift to reactions to the proposed ePrivacy Regulation from the Article 29 Data Protection Working Party, and industry.

REACTIONS TO THE PROPOSED ePRIVACY REGULATION

Although only proposed half a year ago, the Proposed ePrivacy Regulation has received great attention.

ARTICLE 29 DATA PROTECTION WORKING PARTY AND CERTAIN OTHER EUROPEAN UNION REACTIONS

In its opinion on the matter, the Article 29 Data Protection Working Party (WP29) initially describes positive aspects of the proposed ePrivacy Regulation. Included among these are certain aspects regarding the form of the instrument and its relationship with the GDPR. For example, the choice of the form of a regulation for the legislative proposal, the choice of keeping the legislation as a complementary legal instrument to the GDPR, the approach of broad prohibitions and narrow exceptions in the draft legislation, and having the same authority for enforcement as under the GDPR are praised. Also the alignment of administrative fines under the proposed ePrivacy Regulation with those of the GDPR, the removal of data breach notification requirements under the proposal, to prevent "unnecessary overlap" with those of the GDPR, and the equal treatment of all end-users in the proposed ePrivacy Regulation are applauded.[54]

In addition, WP29 agrees with the expansion of the material scope of the legislation to include OTT providers and machine-to-machine interaction. Also considered positive points are the fact that the proposed legislation covers electronic communications content and metadata, recognizes that metadata may reveal very sensitive data, and acknowledges that content analysis is high-risk processing (which should result in required prior consultation with the relevant supervisory authority under the GDPR). Also appreciated are the provisions indicating the importance of anonymization, provisions which would require consent for "device fingerprinting" because of the broad way that the provision on the protection of terminal equipment is drafted in Article 8, and the continued inclusion of legal persons in the scope of the proposed legislation. Among other points, the fact that certain non-intrusive interference with terminal equipment (such as Web traffic/Web audience measurement) will benefit from an exception from the general prohibition on use of processing and storage capabilities of terminal equipment and collection of information there from without end-user consent, is considered laudable.[55]

However, WP29 does note several "points of grave concern." First, it considers that several provisions undermine the level of protection of the GDPR; as an example, it sees the obligations in the proposed ePrivacy Regulation regarding the tracking of the location of terminal equipment as not complying with the GDPR, by giving the impression that information on the physical movement of natural persons may be tracked (through "WiFi-tracking" or "Bluetooth-tracking") without their consent. Secondly, it considers that conditions for allowing content and metadata analysis must be elaborated. WP29 considers these categories of data as being highly sensitive, and that there should be a general prohibition against processing metadata and content without receiving the consent of both sender and recipient.[56]

Next, WP29 believes that the proposed ePrivacy Regulation does not require terminal equipment and software to, by default, offer privacy protective settings, so as to discourage, prevent and prohibit unlawful interference. Thus, the GDPR concept of data protection by design and by default seems not to have been adopted. In addition, "the practice whereby access to a website or service is denied unless individuals agree to be tracked on other websites or services," known as "tracking walls," should explicitly be prohibited by the proposed ePrivacy Regulation, according to WP29. In sum, WP29 does not believe that the proposal provides an equal or higher level of protection than the GDPR.[57]

WP29 lists another 18 or so points of concern, and terminates its opinion with several points for clarification,[58] which will not be discussed here. In addition, it should be noted that the European Data Protection Supervisor also has issued an opinion on the proposed ePrivacy Regulation, likewise detailing certain positive points, before entering into similar concerns, commenting in the Executive Summary on the way that "the complexity of the rules, as

outlined in the Proposal, is daunting," prior to making recommendations.[59]

INDUSTRY REACTIONS

Industry reaction to date has tended to be rather strong, which is nothing to be surprised about when news sources such as *The Guardian* title articles with headings such as "WhatsApp, Facebook and Google face tough new privacy rules under EC proposal."[60]

IAB (Interactive Advertising Bureau) (US)'s statement on the proposal was succinct, focusing on a risk of "harming the livelihood of millions of websites and apps that rely on digital advertising…" and claiming that the ability to innovate will be diminished.[61]

ETNO—European Telecommunications Network Operators' Association begins its position paper by stating that "it has consistently pleaded for a repeal of the ePrivacy framework," regretting a double set of rules (with the GDPR), thus taking the opposite view of WP29. While acknowledging the introduction of OTT players into the material scope of the proposed legislation is welcome from a non-discrimination perspective, it criticizes what it identifies as a "very strict regime for processing metadata that is applicable only to electronic communications services, and not to other providers who process metadata of a similar (or even more) delicate nature, like app providers working with location data (*e.g.*, GPS data)." It similarly finds that the instrument provides "a very strict regime for the processing of e-communications data," and cites several instances where it believes that access to electronic communications data is necessary without requiring the obtaining of consent (*e.g.*, the use of usage data for product and service development).[62]

The nature of the reaction to-date portends intense lobbying efforts ahead on the proposed ePrivacy Regulation, as does the example of the GDPR in the recent past.

THE LEGISLATIVE PROCESS

The European Commission would like the proposed ePrivacy Regulation to enter into force at the same time as the GDPR: "Swift adoption of the ePrivacy Regulation will allow consumers and businesses to benefit from the full digital privacy framework when the GDPR applies in May 2018."[63] In accordance with the ordinary legislative procedure, agreement between the Council and the Parliament on the text of the ePrivacy Regulation in two successive readings is required for it to become binding and directly applicable in Member States. Once adopted (and this may occur after multiple readings and different drafts in the Parliament and the Council), the GDPR's entry into force would occur 20 days after publication in the Official Journal of the European Union.

In the European Parliament, the same committee that had responsibility for the GDPR has the main responsibility for the proposed ePrivacy Regulation—LIBE (Civil Liberties, Justice and Home Affairs), this committee referral having been announced in February 2017. Other committees—ITRE (Industry, Research and Energy), IMCO (Internal Market and Consumer Protection), and JURI (Legal Affairs)—may issue opinions.[64] Thus, the legislative procedure is on the way, but not very far along yet. The timetable seems very tight and may be described as a challenge.

CONCLUSION

This article focused on the main Internet law provisions of the recent proposal for an ePrivacy Regulation, to replace the current ePrivacy Directive, as amended in 2009. Issues that may be seen as more strictly telecommunications ones, such as provisions in Chapter III of the proposal on presentation and restriction of calling and connected line identification, incoming call blocking, and publicly available directories, have not been discussed.

Many failings of the draft have been indicated both by WP29 and by industry associations. One only has to read the document to see that it cross-refers to another document—the Directive on establishing the European Electronic Communications Code[65]—that has not been finalized, provides for many references to the GDPR that must be studied for coherence, and to put it bluntly, has a lot of work to be done. Furthermore, for a document that has not been finalized and that is intended to have "worldwide" application, much in the way that there is an extraterritorial

effect of the GDPR, the proposed application date in May 2018 would allow very little time for companies to prepare themselves and develop compliance programs.

The extension of the material scope of the proposal to OTT players, while expected in light of the DSM strategy of the European Commission, represents an impressive expansive of the legislation and a probably a needed one. One could make a similar comment about machine-to-machine transmissions being covered by the proposed ePrivacy Regulation.

The choice of a regulation as the legislative instrument, as was the case for the GDPR, is a wise one. Moreover, one may wonder whether its finalization will be easier now that Europe prepares for Brexit.

By its very nature, this treatment of the proposed ePrivacy Regulation cannot be seen as complete and the reader is urged to review the instrument itself, and to follow closely developments on this legislative file.

NOTES

1. Regulation (EU) 2016/479 of the European Parliament and of the Council of April 27, 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), 2016 O.J. (L 119) 1, May 4, 2016 [herein, GDPR].
2. 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), COM(2017) 10 final, (Jan. 10, 2017) [herein, Proposed ePrivacy Regulation], *https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications*.
3. Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O. J. (L 201) 37, (July 31, 2002), as amended by Directive 2009/136/EC of the European Parliament and of the Council of Nov. 25, 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 (Dec. 18, 2009).
4. Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*.
5. For a discussion of sector-specific communications privacy in the United States, *see*, *e.g.*, William McGeveran, Privacy and Data Protection Law (Foundation Press, University Casebook Series, 2016) 819-846.
6. W. Gregory Voss & Katherine Woodcock, Navigating EU Privacy and Data Protection Laws (American Bar Association, ABA Section of International Law, 2015) 152. To take into account technological change, including development of the Internet, previously existing provisions on "unsolicited calls" were extended to email in the original ePrivacy Directive, as well, even prior to the 2009 amendments.
7. *Id.* at 160.
8. Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioral Advertising* (WP 171) (June 22, 2010), *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf*.
9. ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Jan. 31, 2015, *https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data*.
10. *See* Consolidated Version of the Treaty on the Functioning of the European Union, art. 288, at 171-172, May 9, 2008, 2008 (C 115) 47, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:EN:PDF*.
11. European Commission, Public Consultation on the Evaluation and Review of the ePrivacy Directive, Apr. 11, 2016, *https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive*.
12. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the Implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, COM(2017) 228 final (May 10, 2017), at 2, *http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-228-F1-EN-MAIN-PART-1.PDF*.
13. *Id.* at 6.
14. Proposed ePrivacy Regulation, *supra* n.2, art. 3 at 24.
15. *Id.*, art. 2 at 23.
16. *Id.*, art. 4(1)(b).
17. Proposal for a Directive of the European Parliament and of the Council Establishing the European Electronic Communications Code (Recast), COM/2016/0590 final/2, (Oct. 12, 2016), art. 2(4), *http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN*.
18. Proposed ePrivacy Regulation, *supra* n.2, recital (11) at 13.
19. *Id.*, recital (12).
20. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM(2016) 288 final, (May 25, 2016), at 7.
21. Proposed ePrivacy Regulation, *supra* n.2, recital (13) at 14.
22. *Id.*, explanatory memorandum at 5.
23. *Id.*, art. 4(1)(a) at 24.
24. *Id.*, explanatory memorandum at 9.
25. *Id.*, art. 8(2)(b) at 27.
26. *Id.*, arts. 18 and 19 at 31-32.
27. *Id.*, art. 1 at 23.
28. *Id.*, recital (5) at 12.
29. European Commission, Press Release, Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions, (Jan. 10, 2017), *http://europa.eu/rapid/press-release_IP-17-16_en.htm*.

30. Proposed ePrivacy Regulation, *supra* n.2, art. 8 at 27.
31. *Id.*, art. 10 at 28.
32. *Id.*, art. 5 at 25.
33. *Id.*, recital (1) at 11.
34. *Id.*, art. 6(1) at 25-26.
35. *Id.*, art. 6(2) at 26.
36. *Id.*, art. 6(3) at 26.
37. Id., art. 7 at 26-27.
38. *Id.*, art. 9(3) at 28.
39. *Id.*, recital (3) at 12.
40. GDPR, *supra* n.1, art. 4(11) at 34.
41. Proposed ePrivacy Regulation, *supra* n.2, art. 9(2) at 28.
42. *Id.*, art. 16(1) at 30.
43. *Id.*, art. 16(2) at 30.
44. *Id.*, art. 16(6) at 31.
45. *Id.*, art. 18(1) at 31.
46. *Id.*, art. 19 at 31.
47. *Id.*, art. 21(1) at 32.
48. *Id.*, art. 21(2) at 32.
49. *Id.*, art. 22 at 32.
50. *Id.*, art. 23(2) at 32-33.
51. *Id.*, art. 23(3) at 33.
52. *Id.*, art. 23(5) at 33.
53. *Id.*, art. 24(1) at 33.
54. Article 29 Data Protection Working Party, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, WP 247 (Apr. 4, 2017) at 6-8.
55. *Id.* at 8-10.
56. *Id.* at 10-12.
57. *Id.* at 14-16.
58. Id. at 16-35
59. European Union Data Protection Supervisor, Opinion 6/2017: EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Apr. 24, 2017, *https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf*.
60. Samuel Gibbs and agencies, "WhatsApp, Facebook and Google face tough new privacy rules under EC proposal," *TheGuardian* (Jan. 10, 2017 15.54 GMT), *https://www.theguardian.com/technology/2017/jan/10/whatsapp-facebook-google-privacy-rules-ec-european-directive*.
61. Dave Grimaldi (IAB U.S. Executive Vice President), *IAB Statement on New EU Privacy Proposal*, IAB. (Jan. 10, 2017), *https://www.iab.com/news/iab-statement-new-eu-privacy-proposal/*.
62. ETNO's views on the Proposal for an ePrivacy Regulation, Mar. 2017, *https://etno.eu/datas/positions-papers/2017/RD440_ETNO_views_eprivacy/RD440_ETNO_views_eprivacy.pdf*.
63. COM(2017) 228 final, *supra* n.12 at 6.
64. For the European Parliament Legislative Observatory procedure file for the proposed ePrivacy Regulation, *see http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en.*
65. The proposed Directive's procedure file is at *http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2016/0288(COD)&l=en*.