
# Comments on the Proposal for an ePrivacy Regulation

Centre for Information Policy Leadership
GDPR Implementation Project
11 September 2017

# CIPL's TOP TEN MESSAGES ON THE PROPOSAL FOR AN ePRIVACY REGULATION

1. **Because of its over-reliance on consent and its broad scope, the Proposal will have the unintended consequence of undermining the GDPR, as well as legitimate, necessary and beneficial processing of data and business practices within the Digital Single Market. Its effect will be to carve out from Article 6 GDPR a huge area of online services and digital data processing relating to electronic communications and use of data on and about devices, which is only going to increase in the future.**

2. **The scope of the Proposal should be limited to core communication services and to electronic communications data within the GDPR definition of personal data.**

3. **The rules on confidentiality should only apply during the transmission of communications, targeting genuine surveillance of individuals and communications.**

4. **The need for a specific provision for the collection of personal data via cookies should be reconsidered. Processing of information about devices (software and hardware), and of information emitted by devices, should not be subject to the ePrivacy Regulation.**

5. **The Proposal should add to the protections of the GDPR only where there is evidence that the relevant GDPR provisions do not offer sufficient protection. The legislator should refer to this evidence.**

6. **Consent should be required only in relation to intrusive or harmful processing with potentially high risks for the individual's privacy that cannot be effectively mitigated against and in cases where the provider is in a position to provide meaningful information and choices to the end user.**

7. **In other circumstances, legitimate interest should be recognised as a ground for processing, consistent with the GDPR. This is critical to ensure ePrivacy rules are future proof and enable data-driven innovation and competitiveness in the Digital Single Market.**

8. **The exceptions to end user's consent in Articles 6 and 8 of the Proposal should be widened. In addition, economic actors other than providers of electronic communications networks and services should also be covered by the exceptions included in Article 6. The exceptions to end user's consent in Articles 6 and 8 should include a wide household exemption, as well as other exemptions where a specified public interest or a business continuity or development would require processing of data without consent. In addition, legal obligation and vital interests of the data subject should be recognised as grounds for processing, consistent with the GDPR.**

9. **Flexible tools should be included to make the ePrivacy Regulation future proof. This includes codes of conduct, empowering the Commission to further extend the list of exemptions and authorising the EDPB to issue guidance on the exemptions to consent in Articles 6 and 8. Industry should be engaged and have input in the development of these tools.**

10. **The adoption of and the effective date of application of the ePrivacy Regulation should be postponed. A transitional period should be allowed, similar to the two-year implementation period of GDPR.**

## A. Introduction

On 10 January 2017, the Commission adopted a proposal for an ePrivacy Regulation[1] (Proposal), as a further step in the reform of the EU data protection framework. The Proposal aims to replace and modernise the privacy framework for electronic communications contained in the ePrivacy Directive 2002/58[2] and to align it with the GDPR.

The new ePrivacy Regulation targets a wide variety of digital communications, extending the scope of the rules to internet service providers and over-the-top services (such as messaging, email platforms and VoIP communications). Its reach will also include, for instance, many Internet-of-Things (IoT) applications and machine-to-machine (M2M) communications. Finally, the Proposal even covers non-personal data, such as electronic communication metadata, which is not always personal data.

The Centre for Information Policy Leadership (CIPL)[3] has serious concerns relating to Chapter II[4] of the Proposal because of its broad scope, uncertainties around its alignment with the GDPR and its over-reliance on consent as ground for processing.[5] The over-reliance on consent will have the unintended consequence of undermining the GDPR, as well as legitimate, necessary and beneficial processing of data and business practices within the Digital Single Market.

Consent should be required only in relation to intrusive or harmful processing with potentially high risks for the individual's privacy that cannot be effectively mitigated against and in cases where the provider is in a position to provide meaningful information and choices to the end user. In other circumstances, legitimate interest should be recognised as a ground for processing, consistent with the GDPR.

The exceptions to end user's consent in Articles 6 and 8 of the Proposal should be widened, while at the same time safeguarding a high level of privacy and data protection. This would not only ensure a high level of protection of the individual, but also increase trust in (the security of) digital services.[6] The exceptions should extend unambiguously to situations where a legitimate interest—including a legitimate business continuity or development—would require processing of data without consent.

---

[1] 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.

[2] 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 201/37, as amended by Directive 2009/136/EC, OJ L 337/11.

[3] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and more than 54 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. For more information, please see the CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm Hunton & Williams.

[4] Chapter II – Protection of Electronic Communications for Natural and Legal Persons and of Information Stored in their Terminal Equipment.

[5] These comments build on CIPL's Response to the European Commission's Public Consultation on the ePrivacy Directive (5 July 2016) and on CIPL's paper "Understanding the Core Principles of Transparency, Consent and Legitimate Interest" (19 May 2017).

[6] Explanatory Memorandum to the ePrivacy Regulation, beginning of Section 1.1 ('Reasons for and objectives of the Proposal').

In addition, the Commission should be empowered to further extend the list of exemptions by way of delegated or implementing acts where this proves necessary over time.

Finally, CIPL is also concerned that the Proposal will thwart the vital policy aims of the Digital Single Market strategy.[7] Throughout this document, we provide examples of how the Proposal does not align with—and sometimes even contradicts—the goals and policy areas of the Digital Single Market.

This document is a reaction on the Commission proposal. In meantime, the legislative procedure in the European Parliament and the Council of Ministers is progressing.[8] Just a few days ago, the Estonian Council Presidency presented a revised text.[9] It does not affect the recommendations in this paper.

## B. The scope of the Proposal should be significantly limited

### 1. *The scope of the Proposal is too wide and will have unintended effects*

In the Commission's view, while the objectives and principles of the ePrivacy directive remain sound, its limited scope over only traditional telecommunications is out of pace with technological developments, requiring an extension of coverage to over-the-top communications services (OTTs). However, the scope of the Proposal reaches significantly beyond covering OTTs. This is a result of the stated broad scope of Article 2(1), the definitions in the Proposal and the internet-related developments of the fourth industrial revolution.[10] Services merge, devices are connected and communication features are becoming integral to many applications and services. The extended scope of the Proposal thus affects a wide range of online service providers including websites and online applications,[11] IoT and M2M communications.[12] This covers a wide range of communications between connected devices, including household appliances, wearables and connected cars.

This widening of the scope creates at least three types of problems:

a. **Incongruous and unclear relationship between ePrivacy and the GDPR.** CIPL recalls that Article 6(1) of the GDPR provides that processing of personal data is lawful if it is based on one of the six grounds of processing, all having equal status. Article 6(1) creates an appropriate and balanced mechanism in a digital landscape which is complex and dynamic. In contrast, the proposed

[7] See https://ec.europa.eu/digital-single-market/en/economy-society and https://ec.europa.eu/commission/priorities/digital-single-market_en. In these documents, the Commission points at helping to make the EU's digital world a seamless and level marketplace to buy and sell; designing rules which match the pace of technology and support infrastructure; and ensuring that Europe's economy, industry and employment take full advantage of what digitalisation offers.

[8] On 9 June, the Rapporteur for the European Parliament, Marju Lauristin, presented her draft report to the Committee on Civil Liberties, Justice and Home Affairs (LIBE), (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)). LIBE is the leading parliamentary committee; members of this committee were able to table amendments to this draft until 10 July 2017. Other involved committees in the EP are JURI, ITRE and IMCO. The draft reports for these committees are available on the EP website.

[9] Council Doc 11995/17, 8 September 2017.

[10] As understood by the World Economic Forum.

[11] As confirmed by Recital 8 of the Proposal stating, "This Regulation should also apply to natural and legal persons who use electronic communication services to send direct marketing commercial communications or *collect information related to or stored in end-users' terminal equipment*." (emphasis added)

[12] As confirmed by Recital 12 of the Proposal. The Draft Report of 9 June 2017 of the Rapporteur in the European Parliament explicitly supports this wide scope (in the Explanatory Statement).

ePrivacy Regulation relies on consent with exceptions. This does not reflect the complexity and dynamics of the digital landscape. Individual control through consent is not the only means to protect the individual. This is recognised in the GDPR, even for the special categories of data in Article 9 thereof. Also the case law of the CJEU provides support for the importance of collecting and using personal data relating to users of online services on the basis of legitimate interest.[13] Data protection is not an absolute right and requires a balancing with the rights of others and the public interest. For example, the rules on data protection should also enable the free flow of information and innovation and recognise other fundamental rights, such as freedom of expression.

Because the Proposal has such broad scope and application, the GDPR's balanced approach runs the risk of becoming irrelevant in the digital economy in which a wide range of situations would become subject to a requirement of consent by the ePrivacy Regulation.[14] We recall that the Proposal is presented as a *lex specialis* to the GDPR. However, its effect is to carve out from the general rule of Article 6 GDPR a huge area of online services and digital data processing relating to electronic communications and use of data on and about devices. This is only going to increase in the future.

In addition, Recital 19 and Article 6(3)(b) of the Proposal state that where content is processed with consent of the end users, the DPA needs to be consulted in accordance with the GDPR. However, under the GDPR, such consultation is only required if there is a high risk to individuals that cannot be mitigated. Thus, one of the GDPR's primary objectives of limiting the administrative burden of prior authorisations and consultations with DPAs is not recognised in the ePrivacy Regulation and, in fact, would be undermined by it.

Finally, key concepts in the GDPR, such as pseudonymous data, are not recognised in the Proposal. Pseudonymous data is an important measure of data protection, and in many ways the enabler of a risk-based approach.[15] Electronic communication data, such as cookies and online identifiers, are often pseudonymised, and hence pose less risk to their processing (GDPR Recital 28).

b. **Unintended negative consequences.** Digital services are fundamentally different from traditional telecommunication services. Regulating them like traditional services by heavily relying on consent will undermine their functionality, as well as their further development and improvement. The very essence of new online services is that they are data-driven and data-dependent. Their features, usability and attraction to users depend on the ability of providers to use the data, including content and metadata, to provide the features that are the hallmarks of the service and also to develop new features and to improve a service. Users often expect these new functionalities from the services and choose to use them for this very reason. If covered by the ePrivacy Regulation, a substantial number of completely safe and beneficial processing activities will be made impossible or subjected to undue regulatory hurdles. Thus, while we

[13] Case C-582/14, Breyer, ECLI:EU:C:2016:779, at 63.
[14] Recital 18: End users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing data usage, location, and customer account in real time).
[15] White Paper on Pseudonymous Data, Interior Ministry of Germany, presented at the Digital Summit 2017 (in German) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/IT_Netzpolitik/digital-gipfel-one-pager-fokusgruppe.pdf;jsessionid=F122CE60A48F161C5A979597E698C9F6.2_cid364?__blob=publicationFile.

understand that novel services may entail access by third parties to potentially sensitive personal information,[16] we do not believe that these services should be covered by the ePrivacy rules in addition to the GDPR.

The following (categories of) examples illustrate this. They include processing that would be severely limited by an ePrivacy consent requirement, but (in contrast) permitted under the GDPR's legitimate interest ground for processing.

*Data analytics, mostly based on pseudonymised or de-identified data*

- Access to metadata where the access is automated and performed only by a computer with the intention to improve the service through impersonal evaluation of pseudonymised or de-identified data by machines (for example, volumes of people using public roads or train stations or passing near buildings or premises).

- Monitoring of content for data analysis such as, for example, filtering spam, phishing and other malware in a public or in a semi-private network.

- Processing electronic communications content for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, as envisaged under GDPR.[17]

*Value-add services using machine learning*

- Messaging and communication features of online services that use content or metadata to provide features that are the very essence of that service, such as smart features of online services that are based on machine learning (e.g. personal assistant services, chat bots and voice-activated services).

- Value-add services that provide additional convenience to users, such as spam filters, previews of third-party content, translation services and calendar scheduling.

- Search functionalities within communications services (e.g. within email services) that require the processing and indexing of communications data, such as the indexing of emails that allows users to search their mailbox using a keyword, or functionalities allowing users to group emails according to sender or subject line.

- Features designed to enrich electronics communications content, including visual effects and augmented reality.

*Incidental and ancillary data processing*

- Services that enhance terminal equipment performance or consumer experience, but are not strictly "necessary" for the service, such as storing location-related data on the device to improve device location, speed and battery conservation.

[16] This is argued in the EDPS Opinion on the Proposal of 24 April 2017.
[17] See also EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), 24 April 2017.

- Smartphones' use of nearby Wi-Fi MAC addresses to help determine location which is critical for indoor positioning and aiding emergency services.

- Remote connections with machines (such as ATMs) where there is no identifiable end user to grant consent.

*Prevention of technical faults and errors in networks and prevention of illicit activities; prevention of fraud; and the protection of system and information security*

- Processing electronic communications content to prevent fraud and protect the security of terminal equipment.

- Prevention of technical faults and errors in networks and services by others than providers of electronic communications networks and services.

- Network and application security activities by parties that are neither telecommunications network nor online services provider. For example, financial institutions, payment systems and utility services such as healthcare, energy suppliers or transport services will lose their ability to deploy their own content filters and anti-fraud tools to analyse and prevent the circulation of malware, malicious attacks and infiltrations, and, more generally, to protect the end user from fraud and identity theft. For financial institutions and payment systems in particular, there are specific needs to ensure the security of money wallets, internet/mobile banking and mobile payments and more widely the security in the context of the nascent industry of FinTech applications. These activities are usually conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies, as recognised in Recital 71 of the GDPR.

- Protection by providers of Wi-Fi hotspots for the following purposes: prevention of illicit activities and fraud, protection of system and information security, and detection of harmful electronic traffic or access of dark-web or other illicit sites or activities.

*Processing in increasingly mobile work environments*

- Employee login tracking to monitor work and location by staff working from different locations in increasingly mobile working environments.

c. **Ambiguity and uncertainty.** The scope of the Proposal also creates ambiguity. It refers to the definitions in the Directive Establishing the Electronic Communications Code (EECC).[18] However, this is a directive which is not yet adopted by the EU legislator.

Central concepts used in the ePrivacy Regulation need clear definitions in order to achieve the Regulation's goals.[19] The lack of precision and clarity of many of the terms in the proposed Regulation, in addition to the dependency on the EECC Proposal, undermines the effectiveness of the Regulation itself and may negatively impact the rights of individuals in an unjustified manner.

[18] See Article 4(1)(b) of the Commission Proposal for EECC.
[19] This is also argued in the EDPS Opinion on the Proposal of 24 April 2017.

Finally, services where communications are just an ancillary component but not the core of the service should not be covered independently of the outcome of the negotiations on the EECC.

2. *There is no justification for the stricter and more specific requirements in the Proposal*

CIPL recognises the need to protect against unwarranted and harmful intrusions to private electronic communications between individuals. We also recognise that Article 7 of the Charter (Respect for private and family life) protects the confidentiality of communications outside the scope of the GDPR, that the EU Court of Justice emphasised the sensitive nature of communications content and metadata,[20] and that the Proposal seeks to implement these broader protections in light of the sensitive nature of the communications at issue. However, we believe that the aim of the Proposal and the case law of the Court do not justify further specifications of the general rules of the GDPR, especially not specifications of such a broad scope of application as included in the Proposal. Indeed, Article 7 of the Charter itself guarantees the respect for private and family life, including individuals' private communications, without further implementation by the ePrivacy Regulation. And, even more on point, the GDPR, which applies to the processing of all personal data, also protects the confidentiality of these communications in an appropriate and sufficient manner.

To the extent the rules of the ePrivacy Regulation add further necessary protections against interference in individuals' communications covered by the GDPR, such additional rules are justified only with respect to interference with core communications between private individuals (with the appropriate modifications outlined in this paper) where there is evidence that the GDPR remains too general. Outside the scope of the GDPR there is no need for such additional rules under any circumstances because the privacy risks are limited. As mentioned in the Explanatory Memorandum of the Proposal, Article 7 of the Charter already covers not only private communications but also "professional activities of legal persons" (i.e. communications between companies or other legal entities), which are not covered by the GDPR. Thus, we believe that there is no need to additionally protect such communications via ePrivacy for reasons relating to the right to privacy.

Moreover, in many contexts, the processing of communications data is not sensitive and is undertaken for legitimate, common and expected purposes. These CIPL comments provide numerous examples.

Furthermore, we emphasise that, apart from the legal basis for processing under the GDPR, the GDPR's other requirements and protections continue to apply to all processing within the scope of the ePrivacy Regulation. In particular, this includes specifically DPIAs for high-risk processing, data quality, purpose specification, data protection by design, information and transparency, DPO oversight and rights of individuals (including a right to object), and serious sanctions for infringements. Hence, there is no need to "increase" the protections under the ePrivacy Regulation by insisting on individuals' consent for such a wide variety of processing. Individuals will still get effective protection by virtue of application of the GDPR requirements mentioned above.

[20] Joint Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others; Case C-362/14, Schrems; and Joint Cases C-203/15 and C-698/15, Tele2 Sverige and Watson and Others.

In any event, the Proposal should add to the protections of the GDPR only where there is evidence that the relevant GDPR provisions do not offer sufficient protection. The legislator should refer to this evidence**.**

3. *CIPL's recommendations to address the concerns relating to the scope of the Proposal*[21]

- **Limit the scope to core communication services:** The material scope of the Proposal should be restricted to core "communications services" (i.e. voice telephony, text messages, emails, chats etc.). Thus, the definition of electronic communications services should refer to traditional and digital voice telephony, text and media messaging services, and email services. The scope should exclude services that merely use electronic communication networks or services as a means to provide other services. Thus, the following services should specifically be excluded from the scope of the Proposal:

    - Monitoring activities by banks, financial institutions and payment systems, in so far as they are required by specific sectorial rules (as explicitly recognised in Recital 71 of the GDPR);

    - Monitoring activities for security and safety (which may not be provided by either telecommunication or other online service providers), including for the purpose of authenticating the end user;

    - Machine-to-machine communications and Internet of Things communications; and

    - Value-add and ancillary services that use communication networks to provide their services, but are not communication services in and of themselves.

- **Limit the scope to electronic communications data within the GDPR definition of personal data:** Not all electronic communications data, in particular "electronic communications metadata", is personal data. In addition, the processing of anonymous data should be explicitly excluded from the scope. Pseudonymous data could be subject to a lighter regime (by providing an exception for it from consent rules).

- **Include a definition of "electronic communication services":** The definition of "electronic communications services" should be included in the Proposal itself, instead of referring to another instrument.[22] This would facilitate the understanding of the Proposal and would make it possible to appropriately tailor its scope to the specifics of electronic privacy. This definition should also specify the meaning of "publicly available" to exclude finite networks (e.g. within the scientific context, networks such as patient groups, research groups or research participants).

[21] The recommendations in connection with the over-reliance on consent, closely linked to the wide scope of the regulation, are included in Section C below.

[22] The Draft Report of 9 June 2017 of the Rapporteur in the European Parliament also requests including a proper definition (in the Explanatory Statement).

- **Include a definition of "end user":** The definition of "end user" should be included in the Proposal, as it has a central function in designating the entity whose fundamental rights are to be protected.

- **Apply the rules only during the transmission of communications:** Articles 5 and 6 should only apply during the transmission of communications. The text should also define the notion of transmission, as messages travel for only fractions of seconds. The term should be defined as transit between the terminal equipment of the end users and between the end user(s) and the provider(s) facilitating the communication.

  This would exclude the storage and use of metadata (traffic, locations) from the scope of the Proposal and subject such data solely to the GDPR. The specific regime of Article 7 (erasure of data when it is no longer needed for the communication, save for billing purposes) would then no longer be relevant and protection would be sufficiently provided by the GDPR, in particular by Article 5(1)(e) GDPR (Retention no longer than necessary), Article 17 GDPR (Right to erasure and right to be forgotten) and Article 21(1) (Right to object to processing).

- **Target genuine surveillance of individuals and communications:** The notion of interference in Article 5 should be better defined and focus on situations where there is a genuine surveillance of the individual, especially where there is unauthorised access or acquisition of communication data while that data is in transit.[23] Presently, the notion of interference comprises not only the interception of communications, but also any form of processing in relation to a communication and provision of value-add and ancillary services, including, for example, personal assistant services, spam filters and translation services. In addition, it also compromises legitimate access to, and review of, professional emails for compliance audits and corporate documentation to conduct M&A transactions, and the ability to defend interests in administrative, arbitration or judicial claims, provide evidence of blackmail, protect IP and trade secrets or protect against unauthorised access to other protected assets (including personal data) through Data Loss Prevention programmes.

- **Reconsider the need for including a specific provision for the collection of personal data via cookies:** Article 8(1) of the Proposal prohibits—with exceptions—the use of processing and storage capabilities of terminal equipment and the collection of information from end users' terminal equipment. Article 10 would require browsers and other software providers to offer end users the option to choose during setup whether to receive cookies from third parties. The main purpose of these provisions is to regulate the use of cookies. However, CIPL wishes to underline that the subject matter of the processing of personal data by cookies and other tracking technologies is fully covered by the GDPR. We note that the definition of personal data in the GDPR covers online identifiers and the GDPR contains strict rules on profiling. Strong protections concerning the collection of personal data via cookies is most needed when cookies are used for profiling purposes. This topic is extensively regulated in the GDPR, calling into question the need for these specific rules of the Proposal.

  If Article 8(1) of the Proposal is kept, it is crucial to limit its scope, since it covers processing operations that have nothing to do with the protection of individuals against cookies and

[23] Reference can be made to the CJEU (C-293/12) - Digital Rights Ireland and Seitlinger a.o., where it mentions situations where people have the feeling that they are under constant surveillance.

other tracking technologies. Article 8 prohibits processing of information stored in and related to end-user terminal equipment, which is all information about any device or equipment that you can imagine and is much wider than cookies and other tracking technologies. If Article 10 is kept, it should be amended to allow service providers to determine when and how to offer choices about cookies to end users. More flexibility is appropriate given the broad range of entities (e.g. browser makers, operating system providers and mobile app developers) to which this provision could apply.

## C. Consent as required by the Proposal is often not meaningful and is counterproductive

**The Proposal's over-reliance on consent**, with limited and narrow exceptions, is unnecessarily restrictive; hampers innovation, SMEs and European competitiveness; and will ultimately render individuals' consent meaningless. Research has shown that the more often people are asked to provide consent to data processing, the less meaningful each request for consent becomes.[24] Given that the proposal would drastically increase the number of consent requests end users would receive, the Regulation could possibly undermine people's control over their information, rather than strengthening it.

Recital 19 of the Proposal formulates a presumption that the processing of content and metadata results in high risk for the individual. However, this is just a presumption. CIPL contends that although personal communications may be sensitive, access to these communications does not necessarily result in high risk for individuals. The various examples in this paper illustrate this.

Requiring consent across the board regardless of context, function or actual risk to individuals may result in actually eroding individual and system protections, and prevent many types of legitimate and safe data processing. A repetitive stream of individuals' consents will not only call into doubt how "informed" such consents can be, but may result in friction in the user experience and ultimately result in customer attrition and stifle innovation, digital progress and benefits for individuals, society and other stakeholders within the Digital Single Market.

More specifically, the consent approach of the Proposal poses a number of problems:

- **Requiring consent as legal ground for processing may be excessive and counterproductive.** Instead, because communications data may be sensitive, the legislator should permit the most effective protection under the circumstances, taking into account the developments in the information society. Consent may not be necessary or the most useful or effective protection, for example, in cases where privacy risk is limited or consent may not provide effective protection to the individual[25]; or in situations where consent may not be practicable (e.g. where there is no ability to seek or provide consent), is counterproductive (e.g. processing to prevent criminal activity such as impersonation, operations with stolen metadata or equipment) or not meaningful, because there is no choice.

[24] See e.g. Bart W. Schermer, Bart Custers and Simone van der Hof, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, Ethics and Information Technology, June 2014, Volume 16, Issue 2, pp. 171-182.

[25] See also CIPL's paper "Understanding the Core Principles of Transparency, Consent and Legitimate Interest the Madrid workshop". Further read: Bart W. Schermer, Bart Custers and Simone van der Hof, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, Ethics and Information Technology, June 2014, Volume 16, Issue 2, pp. 171-182.

- **Individuals expect that digital services become smart and provide convenience and added value.** They expect that service providers not only ensure a connection between two individuals or devices wanting to communicate, but also enhance these communications by adding additional convenient services to them.

  For example, various email services offer automatic alternative responses or automatic translation developed through machine learning and based on access to the content of messages. Services like speech-to-text and text-to-speech are good examples of services which are not just convenient, but may also facilitate the accessibility of electronic communications to people with disabilities. Other examples of value-add services based on access to content or metadata include automatic calendaring, transition between voice and text, previews of external images and online content, automatic directions and traffic alerts, friend suggestions, user activity information and alerts, product and venue information and the exchange of metadata between devices.

  All these services provide real benefits to users. They do not create specific privacy harms for individuals, and individuals, in any case, would have rights under GDPR in respect of processing of their data, such as right to object or right to block or erasure. It is important that the rules stay technology-neutral and able to reflect and adapt to the changing realities of the information society.

- **Even in situations where individuals have a choice and can be asked for consent, such consent may be disproportionately burdensome**, especially given the high bar for validity of consent under the GDPR. This will be particularly the case where a processing operation creates a low risk for the individual's fundamental rights or the processing enables additional value and benefits for individual users, as mentioned above. There may be many instances where individuals simply will not be willing or able to keep providing consents as they interact with the information society in their daily life and work, even where they might not have an objection to the processing. In other words, an internet environment in which individuals are constantly asked to provide specific consent would impact the usability of services and lead to consent fatigue, thus decreasing the value of consent. In the modern information age, this will be the inevitable result of consent regimes as envisioned by the Proposal.[26] The practical implications of the cookie-consent requirements in the current ePrivacy Directive are a case in point.

- **Obtaining valid consent may require disproportionate efforts from organisations** and unnecessarily slow down the development and deployment of new products. An example is Article 6(3)(b) of the Proposal, which allows the processing of electronic communications content with consent of all end users concerned. In addition, this could not reasonably work in a situation where two individuals exchange emails using different email providers. In that situation, the provider has a customer relationship with only one of those persons. To make it even more complex, consent may be impossible in respect of email exchanges that include multiple end users who may be anywhere in the world, or for uses of smart features of IoT

[26] The Proposal also includes an obligation to remind users of the possibility of withdrawal of consent every six months, a requirement not found in the GDPR. This imposes additional disproportionate burdens and cost on companies, especially in connection with no- or low-risk processing activities. As mentioned, an internet environment in which individuals are constantly asked to provide specific consent would impact the usability of services and lead to consent fatigue, thus decreasing the value of consent.

appliances. Equally, the requirement to seek specific consents presents a barrier to entry to the European market for smaller participants, limiting start-ups and new businesses to their national markets, and favouring larger multinationals with resources to occupy a larger market segment. To conclude, the processing of communications should not require the consent by *all* parties to the communication but rather by *at least one* of the parties to this communication. It should also be clarified that the individuals other than the communicating parties are not protected by the secrecy of communications; the processing of their data would be governed by the GDPR as the case may be, and, if so, justified by the legitimate interest ground.

- Article 8(1) of the Proposal contains specific rules on collecting or storing information about and on end users' terminal equipment (including, but not limited to tracking technologies and software, such as cookies). The article is wide in scope and regulates "the use of processing and storage capabilities of terminal equipment and the collection of information from end users' terminal equipment, including about software and hardware". Storing or retrieving data from electronic devices is ubiquitous and done for many legitimate purposes, such as using online shopping carts, detecting language settings to display appropriate language text or collecting IP address for online security, including personalised ads tailored to the preferences and interests of individuals. Moreover, information about devices is routinely processed in many contexts, to enable functionality, diagnostics and troubleshooting and will only increase with IoT-connected devices. While the Proposal requires consent of individuals based on the notion that individuals must decide whether they wish to be tracked (including via their devices), CIPL believes that a more nuanced approach is warranted, whereby consent should be limited to high-risk processing that cannot be effectively mitigated, and other processing grounds, such as legitimate interest (see below), should be allowed.

- Article 8(2) prohibits the collection of information emitted by terminal equipment except if the collection is to establish a connection or with prominent notice. While the Commission envisioned the practice of tracking the physical movements of consumers in retail environments when including this requirement,[27] the definition of "terminal equipment" is broadly defined as "equipment directly or indirectly connected to the interface of a public telecommunications network".[28] Some have interpreted "terminal equipment" to include Wi-Fi routers.[29] In addition to the scenario envisioned by the Commission (smartphones emitting signals), stationary Wi-Fi routers also emit signals and it is common for smartphones to collect the MAC addresses emitted by nearby Wi-Fi routers to determine location. Indeed, the ability of smartphones to determine location while indoors is severely limited (and in many cases impossible) without using the signals emitted from Wi-Fi routers. There is a significant public safety policy in ensuring that this practice continues. However, under the Proposal there is no viable path for compliance, because smartphones would not be collecting information emitted by Wi-Fi routers to establish a connection, nor could they give notice to the Wi-Fi router owner.

[27] Proposal, Recital 25.
[28] Proposal, Article 4(1)(c) citing Directive 2008/63/EC, Article 1(1)(a).
[29] E.g. German Act on the Selection and Connection of Telecommunications Terminal Equipment (23 January 2016); Directorate-General for Internal Policies, "An Assessment of the Commission's Proposal on Privacy and Electronic Communications" (May 2017) at 44.

- In some instances, where the purposes of processing are in the public interest or other legitimate interest and cannot be fulfilled by processing anonymous information, the failure of individuals to give consent would harm that public or other legitimate interest without good reason. For instance, the measuring industry and the use of smart grids in the energy sector are examples where the absence of consent could prejudice the reliability of the business, as well as the public interest (e.g. scientific research).

To address these problems, CIPL proposes the following:

- **The Proposal must better reconcile effective privacy protections for the individual with the need to process electronic communications data without consent**, for example for purposes of providing personal assistant services, fighting illicit and fraudulent activity, and favouring product improvement, and for value-add services that benefit end users.

- **The Proposal must recognise that processing of information about devices, including about software and hardware, and of information emitted by devices, should not be subject to the ePrivacy Regulation,** unless the information constitutes personal data. And even then, such processing should not be solely subject to consent and its very limited exceptions. This change is necessary to enable the wider ecosystem of service providers to be able to deliver their services and is essential for the infrastructure of the IoT and connected devices to function properly.

- **The Proposal must specify that consent need only be used as legal ground for processing in situations where there is high risk that cannot be mitigated, where a controller is in a position to provide clear and understandable information and where individuals have a genuine choice** to make decisions about the use of their personal data.

- **To ensure that the rules are future proof, the Proposal must otherwise allow for legitimate interest-based processing** (see discussion below). This ground for processing is better suited for the context of cookies and similar tracking technologies and other services or processing that may be covered by the ePrivacy Regulation.

**D. <u>The concept of "legitimate interest" must be included in the ePrivacy Regulation</u>**

It is a significant shortcoming of the Proposal that it does not provide for legitimate interest as a ground for processing in line with GDPR. CIPL believes it is necessary to further align the ePrivacy Regulation and GDPR by including legitimate interest as a ground for processing in Articles 6 and 8 of the Proposal, for the following reasons:

- It would allow companies to innovate in data-driven services that are critical for Digital Single Market and EU competitiveness, while ensuring a high level of privacy protection for individuals.

- In many contexts, legitimate interest can be more protective than consent for individuals, as it requires organisations to be accountable, to understand the interests involved in a given processing operation, to conduct a full assessment of potential risks and harms for

individuals, to perform a balancing between the interests at stake and to implement tailored and context-specific mitigations and safeguards for individuals.[30] In addition, it requires organisations to be able to demonstrate that they have taken each of these measures. Indeed, this type of protection is what individuals reasonably expect from organisations in most cases, rather than being constantly asked for consent. It would help make the ePrivacy Regulation future proof, similar to the GDPR. The legitimate interest test, in all cases, will be context specific and equally applicable to any and all current and future technologies, processing and business practices that might be subjected to its analysis. This is important, especially as the option to keep extending the exceptions (discussed below in section E) is not likely to achieve this goal on its own.

- The importance of legitimate interest as processing ground in the online context was also recognised by the Court of Justice of the European Union in its Breyer ruling[31] where it underlined that website owners "have a legitimate interest in ensuring, in addition to the specific use of their publicly accessible websites, the continued functioning of those websites" when using the IP addresses of their site visitors for security purposes without obtaining prior consent.

- There are many examples of services that provide benefits to end users in which consent will neither be possible nor effective, where the absence of consent will not be harmful and where the legitimate interests of the business or a third party do not prejudice the rights of individuals (providing that appropriate safeguards are implemented). They include the following processing of electronic communications data or information stored and related to end-user equipment:

    - Smart and value-add features such as translation and personal assistant services;
    - Spam filters;
    - Customer service chat bots;
    - IoT devices; smart appliances and wearables;
    - Satellite and indoor location technologies or location-based services (LBS) for smartphones;
    - Wireless device performance-enhancing or battery conservation technologies;
    - Malware detectors and other security features;
    - Quality of service technologies which are not provided by an Electronic Communications Network (ECN) or Electronic Communications Service (ECS) under Article 6;
    - Monitoring or capturing certain employee email content for security purposes, data loss prevention and quality assurance purposes;

[30] See CIPL's paper "Understanding the Core Principles of Transparency, Consent and Legitimate Interest" (19 May 2017).
[31] Case C-582/14, Breyer, ECLI:EU:C:2016:779, at 60.

- Collection of metadata (e.g. location data) and device information (e.g. device fingerprinting) for authentication and security purposes; and
- Connectivity technologies for automated vehicles.

**E. <u>More exceptions to consent are needed</u>**

The Proposal includes exceptions to the prohibition of processing of communications data and information stored in, and related to, end-user terminal equipment without end users' consent, which are set forth in Articles 6 and 8. These exceptions are too narrow to even cover all the legitimate processing situations that are common today, let alone those that will be developed in the future.[32] The personal scope of the exceptions included in Article 6 should not be limited to providers of electronic communications networks and services. Furthermore, the exceptions to consent in Articles 6 and 8 should be widened as follows:

a) **A wide household exemption should be included in the Proposal** for services that do not pose a threat to the private life of the user, in addition to the services that are already outside the scope because they are not publicly available (see Article 2(2)(c) of the Proposal). This exemption should exclude from the scope of the ePrivacy Regulation:
   - IOT solutions in a private household where different appliances communicate;
   - Machine-to-machine communications between personal devices (e.g. a wearable device and mobile phone);
   - Internal networks of (groups of) undertakings; and
   - "Personal assistant" functions.

b) **The exemptions of Articles 6 and 8 should extend to other, precisely formulated, situations where a specified public interest, business continuity or development would require processing of data without consent**. Such exemptions include:
   - Data used in the public interest for the purposes of filtering spam, malware and ransomware and other security protection purposes, as well as for fraud and abuse prevention and detection and combating child pornography or other forms of exploitation of children, or illegal content.
   - Metadata and device information used to determine the accurate identity of the end user ("authentication") and, more generally, to protect the end user from fraud and identity theft.
   - Machine processing of exchanged data for a beneficial purpose (including a societal benefit) using algorithms.

[32] Also the EDPS identified the need to have in the ePrivacy Regulation further specific exceptions to consent, e.g. regarding the scientific research processing ground set forth in the GDPR as well as the need for including other grounds for processing such as vital interests, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), 24 April 2017, p. 16.

- Access that is automated and performed only by a computer with the intention to improve the service through impersonal evaluation of pseudonymised or de-identified data by machines.

- Smart features that are based on machine learning, such as the personal assistant functions and voice activation services.

- Satellite and indoor location technologies or location-based services (LBS) for smartphones and technologies that provide connectivity for automated vehicles.

- Prevention of technical faults and errors in networks and services.

- Cookies necessary for running security updates (provided such updates do not alter privacy settings set by the user, the user is informed and the user has the possibility to turn off automatic updates);

- Cookies necessary in the context of employment relationships, provided they pertain to employer-provided equipment, the employee is the user of such equipment and the use of cookies is strictly necessary for the use of the equipment by the employee.

- Collection of anonymous data that has little to no impact on the private life of the user.

c) **The exemptions of Articles 6 and 8 should extend to legal obligations and vital interests of the data subject or others.** The GDPR recognises that there may be situations where companies may be legally obligated to collect, process or share personal data.[33] An example could be companies' being legally obligated to collect or provide access to personal data to law enforcement. The GDPR also includes an exception for data collection, processing or sharing where "necessary in order to protect the vital interests of the data subject or of another natural person."[34] An example could be the collection or sharing of health data to save the life of the data subject. The same public policy basis for including these exceptions in the GDPR also holds true for Articles 6 and 8 of the Proposal. For example, an electronic communications network provider (Article 6) or a terminal equipment manufacturer (Article 8) could be ordered by law enforcement to process electronic communications data or collect or store data in order to aid a criminal investigation. Likewise, with connected health devices becoming more prevalent, a connected health device manufacturer (or the network upon which the data travels) could need to collect or store data to save the life of the user.

d) **The exemption of Article 6(1)(b) should be extended** to the security of end users' terminal equipment and networks as well as the facilities and other services of the electronic communications service provider. The wording of Article 6(1)(b) of the Proposal prevents service providers from processing content to warn end users about malicious third-party content without express consent.

[33] GDPR, Article 6(1)(c).
[34] GDPR, Article 6(1)(d).

## F. Specific suggestion on Article 8(1)(d)

The Proposal differentiates between services by first and third parties (Article 8(1)(d)) for web audience measuring, opening the way for a more flexible approach than the current rules.[35] While the provider of a web service is entitled to track the number of visitors without consent, they need consent before allowing others to collect this information.

However, the practice is more complicated, as illustrated by the examples in the footnote.[36] Requiring consent for third-party services does not always make sense, for instance where organisations have outsourced this measuring activity to third parties that do not have any additional interest in using the personal data.[37] A difference between first-party cookies and third-party cookies also largely favours existing browser and mobile equipment suppliers and disadvantages small- and medium-size enterprises that do not have their own capacity to measure. What matters is the specific context and nature of cookie use (e.g. who is getting what data for what purpose and how intrusive are the means of getting it), not whether it is first or third party. CIPL therefore recommends that third-party services should be treated on equal footing as first-party services.[38] Neither of these services should be based on mandatory consent .

## G. Specific suggestion on Article 8(2)

Article 8(2) sets forth rules about the collection of information emitted by terminal equipment to connect to another device or to a network. These rules also impact tracking the location of individuals (through Wi-Fi tracking or Bluetooth tracking) who are linked to the devices. Although

[35] The Article 29 Working party even states that it is more flexible than the GDPR. WP 247, p. 11.

[36] Four examples are:

1. A company collects data on how people use its app using in-house technology to produce metrics, for instance on numbers of users (in specific countries), uses of specific features or devices or how long it took to perform a particular function. The raw data used to produce the metrics would be considered personal data as it singles out users, but there is no information (or desire) to tie any activity to any specific identifiable user. Some of the metrics are aggregate as well. The company uses a third-party tool to collect some of the same data for similar metrics (while it builds its in-house capability), and the third party gets some of the data for its own purposes, although it claims to be aggregate and not tied to identifiable users. In short, first- and third-party tools both aggregate data, but the third party gains some use from the data.
2. A company uses a third-party tool to get aggregate data on which platforms users came to its app from, such as a Twitter ad, a Facebook ad and so on. The third party hashes the phone identifiers it uses and does not use the data for its own purposes. This is a third-party tool where both parties have aggregate data and the third party does not gain any use from the data.
3. A company uses a third-party tool that partners with advertising platforms to do retargeting—the user installs an app, does not use a particular feature, 30 days later sees an ad on a social network for that feature. This is an example of a third-party tool doing targeted advertising. The company using the tool gets no data on users. The third-party tool only uses identifiers to target ads for clients and does not use the data for its own purposes.
4. A company uses its own and third-party cookies on its website to do usual things like remember preferences, know whether the visitor has seen/dismissed the cookie banner, create heat maps to show most visited parts of website/pages and so on. It also uses third-party cookies to do retargeting—a corporate user visits the corporate sections of the website but doesn't fill in 'contact us for more info' form. The corporate user then sees the ad on other websites directing them to the 'contact us' form. These are first- and third-party cookies used to make the website work, to collect anonymous statistics on use and for retargeting ads.

[37] See WP29 Opinion 04/2012 on Cookie Consent Exemption, WP194.

[38] This problem is recognised in Amendment 80 of the Draft Report of 9 June 2017 of the Rapporteur in the European Parliament.

tracking can be sensitive since it may reveal the location and behavioural patterns of individuals, there may be instances when this information is useful for the individual, society and the organisation without any risks or harm to individuals.

For example, certain satellite and indoor location technologies or location-based services (LBS) for smartphones that are necessary for optimal functioning of such devices, as well as technologies that provide connectivity for automated vehicles, cannot be made dependent upon consent, particularly where the provider has no direct relationship with the individual.

The Proposal should recognise the necessity of such services and enable processing of data based on legitimate interest. As stated above, in order to rely on legitimate interest, organisations will have to conduct risk assessments, DPIAs and mitigations, as appropriate, thereby ensuring effective protection of the individual consistent with the GDPR.

### H. Specific suggestion on Article 10

Article 10 would require browser makers and other software providers—including, potentially, all app developers—to offer end users the option to choose whether to accept cookies from third parties. As noted above, the GDPR provides comprehensive protections for personal data collected via cookies, so this provision is not necessary.

If, however, the provision is maintained, it should be amended to provide greater flexibility as to when and how to present choices related to cookies. This is particularly important given the range of entities (e.g. browser makers, operating system providers and app developers) to which Article 10 may apply. These entities have different relationships with end users, manage cookies (and similar technologies) differently and offer people different kinds of controls. Article 10, which contains requirements for service providers on when and how to present choices regarding cookies, should be amended and allow these service providers more flexibility to give people the information they need to make informed choices about cookies.

### I. Suggestions in relation to the concept of unsolicited communications (Article 16)

The wording of Article 16 should be more specific to ensure that it only applies to unwanted communication such as spam, phishing and other malicious communication.

However, there should be some flexibility to allow start-ups and new market entrants to promote their products and services, in both B2B and B2C contexts. Indeed, customer acquisition activities, which in many cases are unsolicited in nature, are essential for gaining and sustaining business relationships also for existing companies. CIPL suggests aligning the text with the Unfair Commercial Practices Directive,[39] which prohibits "persistent and unwanted commercial communications".

We also suggest to clarify that Article 16 only applies to unsolicited communications that use services that enable people to make private communications that are directed to specified recipients. These are services such as email, SMS and messaging.

[39] Annex I, pt 26 of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, ('Unfair Commercial Practices Directive'), OJ L 149/22.

The provisions on unsolicited commercial communications must be consistent with the appropriate legal grounds under the GDPR, in particular (i) the legitimate interest ground and Recital 47 of the GDPR[40]; and (ii) the contractual ground (which would exclude from the consent requirement those communications that are relevant for the execution, performance and control of a contractual relationship with the data subject).

## J. Adding flexibility to make the ePrivacy Regulation future proof

A good and flexible instrument for the domain of the ePrivacy Regulation would be a code of conduct. This instrument is included in Articles 40 and 41 of the GDPR. We suggest that reference to these articles is made in the ePrivacy Regulation, encouraging the drawing up of codes of conduct, also in the domain of the ePrivacy Regulation. Codes could be specifically useful for specifying further cases of legitimate interests or uses of electronic communications data and other data covered by the ePrivacy Regulation.

Moreover, the EDPB should be given the task to issue guidelines, recommendations and best practices in relation to applying the exemptions to consent in Articles 6 and 8. If provided, this task must be subject to mandatory consultation and involvement of relevant industry, to ensure that justified views of impacted controllers and various interests at stake are taken into account.

In addition, the Commission should be empowered to further extend the list of exemptions by way of delegated or implementing acts if this proves necessary over time. Given the dynamic nature of the scope of the ePrivacy Regulation and its impact on information society services and the Digital Single Market, there should be a formal procedure established for organisations to propose such delegated or implementing acts and for the EDPB to intervene. There must be a process to enable the impacted industry to engage fully and work collaboratively with the Commission and EDPB in shaping these additional instruments.

## K. Postponing the application of the regulation

CIPL recommends postponing the adoption and the effective date of application of the ePrivacy Regulation and allowing for a transitional period, similar to the two-year implementation period of GDPR. The main reasons are as follows:

- Organisations are currently busy with GDPR compliance and implementation and this is likely to continue past the deadline of 25 May 2018. They must be able to prioritise this goal, without the need to add another major compliance burden at the same time. We believe that a tight implementation deadline would disproportionately impact SMEs who are already stretched with the GDPR and do not have the sophistication and resources to fully consider the impact of, or work towards compliance with, a new ePrivacy Regulation.

- The additional conditions under the ePrivacy Regulation will require a further adaptation of business practices, processes, systems and technologies. There should be a reasonable timeframe for organisations to reconfigure their systems to make them compliant with the new requirements, also in view of the inconsistencies between the ePrivacy Regulation and the GDPR. Implementing two new sets of requirements at the same time would be unduly burdensome and counterproductive.

[40] Recital 47 of the GDPR: "(…) *The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest*."

- Organisations are currently not in a position to begin adapting their business practices and technologies to a new ePrivacy regime, since the Proposal is still in the EU legislative process and a final text will probably not be available any time soon. Organisations require sufficient time to adapt their practices to any new rules.