QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE E-PRIVACY DIRECTIVE

Fields marked with * are mandatory.

QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE E-PRIVACY DIRECTIVE

The e-Privacy Directive (Directive 2002/58/EC on privacy and electronic communications) concerns the protection of privacy and personal data in the electronic communication sector. The Communication on a Digital Single Market Strategy for Europe (COM(2015) 192 final) of 6 May 2015 (DSM Communication) sets out that once the new EU rules on data protection are adopted, the ensuing review of the e-Privacy Directive should focus on ensuring a high level of protection for data subjects and a level playing field for all market players.

Given that the e-Privacy Directive particularises and complements the Data Protection Directive 95/46/EC that will be replaced by the General Data Protection Regulation **(GDPR)**, this questionnaire contains several questions related to the interplay between the e-Privacy Directive and the future GDPR.

In December 2015 the European Parliament and the Council of Ministers reached a political agreement on the final draft of the GDPR. All references to the GDPR in this questionnaire and background document are based on the text adopted in December[1]. After a legal and linguistic review, which may result in small changes to the text, the GDPR will be formally adopted by the European Parliament and Council and the official texts will be published in the Official Journal of the European Union in all official languages.

The purpose of this questionnaire is twofold: First, to gather input for the evaluation process of the ePD (see Section I of the questionnaire) and second, to seek views on the possible solutions for the revision of the Directive (see Section II). The Commission invites citizens, legal entities and public authorities to submit their answers by the 5th of July 2016.

The Commission will summarise the results of this consultation in a report, which will be made publicly available on the website of the Directorate General for Communications Networks, Content and Technology. The results will feed into a Staff Working Document describing the Commission findings on the overall REFIT evaluation of the e-Privacy Directive.

This questionnaire is available in **3** languages (French, English and German). You can skip questions that you do not wish to answer, except the ones marked with an asterisk. You can pause at any time and continue later. Once you have submitted your answers, you would be able to download a copy of your completed responses as well as upload additional material.

Please note that except for responses from visually impaired, in order to ensure a fair and transparent consultation process, only responses received through the online questionnaire will be taken into account and included in the summary.

[1]
http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-

*

PRIVACY STATEMENT

Please indicate your preference for the publication of your response on the Commission's website (see specific privacy statement):

Please note that regardless the option chosen, your contribution may be subject to a request for access to documents under Regulation 1049/2001 on public access to European Parliament, council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.

- (●) **Under the name given**: I consent to publication of all information in my contribution and I declare that none of it is subject to copyright restrictions that prevent publication.
- ( ) **Anonymously**: I consent to publication of all information in my contribution and I declare that none of it is subject to copyright restrictions that prevent publication.
- ( ) **Please keep my contribution confidential**: it will not be published, but will be used internally within the Commission.

Specific privacy statement e-Privacy

Specific_20privacy_20statement_ePrivacy.pdf

Before filling in the questionnaire, we suggest that you consult the background document at the right-hand side of the survey.

Background document

05_2004_20Background_20document.pdf

GENERAL INFORMATION

*

Question I: If you answer on behalf of your organisation: Is your organisation registered in the Transparency Register of the European Commission and the European Parliament?

- (●) Yes.
- ( ) No (if you would like to register now, please click here). If your entity responds without being registered, the Commission will consider its input as that of an individual.
- ( ) Not applicable (I am replying as an individual in my personal capacity).

*

Question I A: Please indicate your organisation's registration number in the Transparency Register.

64270747023-20

*

Question II: Please enter the name of your institution/organisation/business:

DIGITALEUROPE

Question III: Please enter your organisation's address:

14 rue de la Science, 1040 Brussels, Belgium

Question IV: Please enter your organisation's website:

http://www.digitaleurope.org

*

Question V: Please enter the name of a contact person:

Damir Filipovic

Question VI: Please enter the phone number of a contact person:

+32470212983

*

Question VII: Please enter the e-mail address of a contact person:

damir.filipovic@digitaleurope.org

*

Question VIII: In which capacity are you participating in this consultation:

- ○ Citizen
- ○ Consumer association or user association
- ○ Civil society association (e.g. NGO in the field of fundamental rights)
- ○ Electronic communications network provider or provider of electronic communication services (e.g. a telecom operator)
- ○ Association/umbrella organisation of electronic communications network providers or providers of electronic communication services
- ◉ Association/umbrella organisation/ trade association (other than associations of electronic communication service provider/network providers)
- ○ Internet content provider (e.g. publishers, providers of digital platforms and service aggregators, broadcasters, advertisers, ad network providers)
- ○ Other industry sector
- ○ Government authority
- ○ Competent Authority to enforce (part of) the e-Privacy Directive
- ○ Other public bodies and institutions

*

Question IX: Please indicate your country of residence? (In case of legal entities, please select the primary place of establishment of the entity you represent)

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Sweden
- Slovenia
- Slovak Republic
- Spain
- United Kingdom
- Other

I. REFIT EVALUATION OF THE E-PRIVACY DIRECTIVE

Preliminary Question: How much do you know about the e-Privacy Directive?

	Very much	Much	Some	A little	Hardly anything	No opinion
Its objectives	◉	○	○	○	○	○
Its provisions	◉	○	○	○	○	○
Its implementation	◉	○	○	○	○	○
Its relation to GDPR	◉	○	○	○	○	○

I.1. EFFECTIVENESS OF THE E-PRIVACY DIRECTIVE

The e-Privacy Directive aims to harmonise the national provisions required to ensure an equivalent level of privacy protection in connection with the processing of data in the electronic communications sector and to ensure the free movement of such data and electronic communication equipment. This section seeks to explore the extent to which the objectives of the e-Privacy Directive have been achieved. For more information please refer to the background document (see Section III).

Question 1: Based on your experience, do you consider that the e-Privacy Directive objectives have been achieved? More particularly:

	significantly	moderately	little	not at all	do not know
Full protection of privacy and confidentiality of communications across the EU	○	◉	○	○	○
Free movement of personal data processed in connection with the provision of electronic communication services	○	◉	○	○	○
Free movement of electronic communications equipment and services in the EU	○	◉	○	○	○

Question 1 A: Please specify your reply. You may wish to focus on presenting the reasons why certain objectives were achieved/not achieved, please also consider whether factors other than the e-Privacy Directive influenced the outcome.

Text of 1 to 1500 characters will be accepted

The objectives of the ePrivacy Directive (ePD) are better served by the Data Protection Directive (DPD), and its successor the General Data Protection Regulation (GDPR), then they are by the ePD. The ePD is a complex combination of sector and non-sector specific rules that have different objectives. The provisions on confidentiality of electronic communications is one example where a lack of clarity has led to an intense debate among authorities, academics and businesses as to the exact meaning.

In addition, the lack of clarity created additional issues during the implementation phase with divergent national legislation on key provisions. This was further aggravated by the diverging interpretations of national authorities, which took inconsistent positions. These challenges impeded rather than encouraged the free movement of personal data and electronic communications services.

At the same time, the DPD essentially underwrites the confidentiality of communications and free movement of personal data. As such, the ePD serves only to create confusion by conflicting with provisions in the DPD or create unjustified additional burdens for the communications sector.

Since the ePD entered into force, other legislative instruments have been adopted or put forward that further address issues dealt with in the ePD, in particular the GDPR and the NIS Directive. A standalone Directive is therefore redundant.

Question 2: Have you encountered problems in applying/understanding the rules (in your role of provider or as individual)? More in particular in relation to:

	Yes	No	No opinion
Notification of personal data breaches	◉	○	○
Confidentiality of electronic communications	◉	○	○
Specific rules on traffic and location data	◉	○	○
Unsolicited marketing communications sent and received though the Internet	◉	○	○
Itemised billing of invoices	◉	○	○
Presentation and restriction of calling and connected line	◉	○	○
Automatic call forwarding	◉	○	○
Directories of subscribers	◉	○	○

Question 2 A: If you answered "Yes", please specify your reply.

Text of 1 to 1500 characters will be accepted

While DIGITALEUROPE's members are not technically providers, we take note of the ambiguity of scope and differences in national transpositions of the ePD, which make many of the rules difficult to understand or apply.

According to Article 3, the ePD applies to the processing of personal data in connection with the provisions of publically available electronic communication services (ECS) in public communication networks. Under Article 2 of the Framework Directive, an ECS should consist wholly or mainly in the conveyance of signals on electronic communication networks and does not include information society services.

Nevertheless, national transposition in different legal frameworks – often applicable to different industry sectors or contained in general data protection rules – mean the lines around what qualifies as an electronic communication service covered by the ePD are blurry. Examples include the implementation of the breach notification regime, Article 5 (3), or the definition of traffic data. This inconsistency created additional costs for business and led to fragmentation in the internal market. Moreover, as 'publically available' is not subject to a consistent interpretation, questions arise in relation to certain enterprise-facing services. Finally, the ePD itself is not consistent. It includes provisions that not only apply beyond electronic communication services (e.g. cookie or spam provisions), but also apply to non-personal data (e.g. confidentiality).

Question 3: It is currently up to Member States to set up the national bodies entrusted with the enforcement of the e-Privacy Directive. Article 15a of the e-Privacy Directive refers indeed to the "competent national authority" and, where relevant, "other national bodies" as the entities entrusted with supervisory and enforcement powers in relation to the national provisions implementing the e-Privacy Directive.

On the basis of your experience, did the fact that some Member States have allocated enforcement competence to different authorities lead

	significantly	moderately	little	not at all	do not know
to divergent interpretation of rules in the EU?	○	◉	○	○	○
to non-effective enforcement?	○	◉	○	○	○

Question 4: If you answered 'significantly' or 'moderately' to the previous question, has this in your view represented a source of confusion for:

	Yes	No	Do not know
Providers of electronic communication services, information society services and data controllers in general	◉	○	○
Citizens	◉	○	○
Competent Authorities	◉	○	○

Question 4 A: Please specify your reply.

Text of 1 to 1500 characters will be accepted

DIGITALEUROPE believes that the nature of the legal instrument has led to a non-harmonised implementation across Member States. This resulted in compliance challenges and confusion with regards to the 'competent authority' chosen by Member States for enforcement competence. We firmly believe that the mix between data protection authorities and telecom national regulatory authorities across the EU has proven detrimental to citizens and industry. We encourage the Commission to consult the study by DLA Piper (Proposals for an amendment to the General Data Protection Regulation and repealing the ePrivacy Directive), which specifically points to the problems surrounding the differing enforcement agencies across Member States.

As previously mentioned, the GDPR should address many of these challenges given the overlap with the ePD. The GDPR not only improves consistency of enforcement, but also sets out a comprehensive regime for penalising companies that violate EU data protection rules. This should address the concerns highlighted by the questions above.

I.2. RELEVANCE OF THE E-PRIVACY DIRECTIVE

The Data Protection Directive 95/46/EC, which will be replaced by the General Data Protection Regulation (GDPR), is the central legislative instrument in the protection of personal data in the EU. More detailed rules were considered necessary for the protection of privacy and data protection in the electronic communications sector, which led to the adoption of the e-Privacy Directive. This section seeks to assess the relevance of the objectives of the e-Privacy Directive and each of its articles, taking into account technological, social and legal developments. For more information please refer to the background document.

Question 5: In your opinion, are specific rules at EU level necessary to ensure the following objectives:

	Yes	No	No opinion
An equivalent level of protection (full protection) across the EU regarding the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector	○	◉	○
The free movement of personal data processed in connection with the provision of electronic communication services	○	◉	○
Free movement of electronic communications equipment and services	○	◉	○

Question 6: Is there an added value to have specific rules for the electronic communications sector on…?:

	Yes	No	No opinion
Notification of personal data breaches	○	◉	○
Confidentiality of electronic communications	○	◉	○
Specific rules on traffic and location data	○	◉	○
Unsolicited marketing communications sent and received though the Internet	○	◉	○
Itemised billing of invoices	○	○	◉
Presentation and restriction of calling and connected line	○	○	◉
Automatic call forwarding	○	○	◉
Directories of subscribers	○	○	◉

Question 6 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

While the provisions within the ePD are not identical to the GDPR, many of the principles aim to achieve the same goal. There are a number of examples (e.g. the GDPR includes provisions on notification of personal data breaches).The GDPR contains explicit references to the principle of confidentiality, covering many of the same grounds as the ePD (e.g. Art 5 on integrity and confidentiality; Art 32 outlining security requirements so that confidentiality of data processing is upheld.) In the GDPR, confidentiality can only be overridden if one of the legal bases under Art 6 is fulfilled. These legal bases largely mirror the exceptions to confidentiality under the ePD.

Processing of traffic data that may identify an individual, is subject to the legal bases of Article 6. Tighter restrictions are not justified by the risks presented. Location data is also called out in the definition of personal data, holding it to the Regulations' high standards, so additional provisions do not need to be maintained. To the extent consumer protection issues such as itemised billing, caller ID, call forwarding and directories are still relevant for the traditional telecoms sector, which is questionable, they are either sufficiently covered by existing legislation (e.g. eCommerce Directive) or should be transferred to other legal instruments. The review of the telecoms package provides a good opportunity to do so. These provisions should not be extended to apply to new communications platforms.

I.3. COHERENCE OF THE E-PRIVACY DIRECTIVE

This section aims to assess whether the existing rules fit with each other and whether they are coherent with other legal instruments. See background document for more details (see Sections III.3 and III.6).

Question 7: Are the security obligations of the e-Privacy Directive coherent with the following security requirements set forth in the different legal instruments:

	significantly	moderately	little	not at all	do not know

The Framework Directive (Article 13a): requiring providers of publicly available electronic communication services and networks to take appropriate measures to manage the risks posed to the security and integrity of the networks and services and guarantee the continuity of supply.	○	◉	○	○	○
The future General Data Protection Regulation setting forth security obligations applying to all data controllers: imposing on data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate, the pseudonymisation and encryption of personal data and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.	○	○	◉	○	○
The Radio Equipment Directive: imposing privacy and data protection requirements upon all terminal equipment attached to public telecommunication networks.	◉	○	○	○	○

The future Network and Information Security (NIS) Directive: obliging Member States to require that digital service providers and operators of certain essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations.	○	◉	○	○	○

Question 7 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

Article 4 of the ePD requires that publically available electronic communication service providers adopt technical and organisational measures to safeguard the security of services appropriate to the risk. This is complementary to Article 13a in the Framework Directive and the NIS Directive insofar as the focus is on security of data processing as opposed to the integrity of the network (and continuity of services) found in the other two instruments. This could lead to a degree of overlap as security incidents impacting the provision of service could have a data security element, but it is at an acceptable level.

Under the Radio Equipment Directive, the Commission has the right to introduce additional requirements for certain equipment classes to safeguard user privacy and security of the data, but we have not yet seen whether this causes significant incoherence.

The security provisions under the GDPR have the exact same objectives as those under the ePD. The only reason we opt for 'little' is that there are no direct contradictions in the legal text. Nevertheless, the ePD creates an unnecessary overlay that could lead to different security requirements and certainly gives rise to different enforcement bodies having the right to issue instructions to service providers, quite possibly in different Member States (given the OSS found under the GDPR).

Question 8: The e-Privacy Directive prohibits the use of electronic mail, fax and automatic calling machines for direct marketing unless users have given prior consent (Article 13.1). However, it leaves to Member States the choice of requiring prior consent or a right to object to allow placing person-to-person telemarketing calls (Article 13.3).

In your opinion, is the choice left to Member States to make telemarketing calls subject either to prior consent or to a right to object, coherent with the rules of Art 13.1 (which require opt in consent for electronic mail, fax and automatic calling machines), given the privacy implications and costs of each of the channels?

- ○ Yes
- ◉ No
- ○ No opinion

Question 8 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

Once more, we wish to stress that the choice left to Member States has led to a lack of harmonisation. We question the reasoning for leaving the choice to Member States as it has (and will continue to) lead to divergence on how person-to-person telemarketing is regulated. However, we do take note of the provisions related to direct marketing in the GDPR that should ensure the necessary harmonisation in this field (Recitals 47 and 70, Article 21).

Regarding question 9, messages sent over social media should not be considered as 'electronic mail', in particular under Article 13 (3), as it relates only to subscribers and users of traditional telecom providers.

Question 9: There is legal uncertainty as to whether messages sent through social media are covered by the opt-in provision applying to email (Art 13.1) or by opt-out provisions (Art 13.3). Please indicate whether you agree or not with the following statements.

	Yes	No	No opinion
I find it more reasonable to apply to marketing messages sent through social media the same rules as for email (opt in)	○	◉	○
I find it more reasonable to apply to marketing messages sent through social media opt out rules (Art 13)	◉	○	○

I.4. EFFICIENCY OF THE E-PRIVACY DIRECTIVE

In the following section we would like stakeholders to assess the costs and benefits of the e-Privacy Directive, including for citizens at large.

Question 10: The protection of privacy and personal data in the electronic communications sector is also aimed to increase users' trust in these services. **To what extent have the national provisions implementing the e-Privacy Directive contributed to raising users' trust in the protection of their data when using electronic communication services and networks?**

- ○ Significantly
- ○ Moderately
- ◉ Little
- ○ Not at all
- ○ Do not know

Question 10 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

An essential element in the creation of user trust is how national data protection authorities shape market practices in their jurisdiction. These authorities have struggled with the implementation of the ePD.

For example, the rules on the use of cookies have been implemented in a complex, fragmented manner, which was acknowledged by the study “ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation” (SMART 2013/0071) carried out for the Commission. Trust cannot be built on a fragmented implementation of an EU rule, in particular when this fragmentation leads to complex local regimes that are not fully protective of the users.

We believe that data subjects are provided with this protection under the DPD. The addition of such provisions within the ePD have only added confusion for data subjects with regards to effective enforcement if they choose to exercise their rights. Moreover, it is worth noting that certain provisions related to protection in the electronic communications sector already existed in Member State law prior to the ePD. While the objective of the ePD are laudable, many of these protections/provisions already existed in national law making the contributions of the ePD minimal in some Member States.

Question 11: To what extent did the e-Privacy Directive create additional costs for businesses?

- (●) Significantly
- ( ) Moderately
- ( ) Little
- ( ) Not at all
- ( ) Do not know

Question 11 A: Please provide an estimation of the percentage of the total cost and/or any other information.

Text of 1 to 1500 characters will be accepted

It is difficult to provide specific numbers regarding the costs for businesses to comply with the ePD requirements. It depends on the size of the company, the number of countries they are located in, and their data processing practices. However, as a general rule, it can be estimated that compliance costs range from several tens of thousands of euros to several hundreds of thousands euros; sometimes more for large multinational companies operating across the EU. In any event, the cost of compliance increases with the level of complexity of the rules, fragmentation in local implementation and overall legal uncertainty that is linked to each piece of legislation.

For the ePD, these factors can all be considered as high. This is particularly problematic for SMEs operating across the Single Market, which have faced in some cases an extreme administrative (and cost) burden to implement the cookie banner, which has failed to achieve its objective. Additional costs would include limitations of functionality of services based on the strict purposes under which traffic and location data can be used; delay in roll-out of services and cost of legal analysis based on the legal uncertainty surrounding covered services; and failure to integrate communication functionality in hybrid services in order to avoid being subject to both the ePD and the additional provisions under the Telecom Package that apply to publicly available electronic communication services.

Question 12: In your opinion, are the costs of compliance with the e-Privacy Directive proportionate to the objectives pursued, in particular the confidentiality of communication as a measure to safeguard the fundamental right to privacy?

- ( ) Yes
- (●) No
- ( ) No opinion

Question 12 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

We do not believe the compliance costs associated with the ePD are proportionate to the objectives pursued. Industry has been faced with conflicting provisions and an un-harmonised implementation across Member States. This has led to confusion and a negative impact for both industry and citizens. Moreover, the compliance costs further overshadow the objectives of confidentiality when one considers the numerous Member State laws, which have created exceptions allowing national authorities to circumvent the confidentiality requirements placed on telecoms providers.

I.5. EU ADDED VALUE OF THE ERIVACY DIRECTIVE

This section seeks to assess the EU added value of the e-Privacy Directive especially in order to evaluate whether action at EU level is needed for this specific sector. See background document for more details (see Section III).

Question 13: Do you think that national measures would have been/be needed if there were no EU legislation on e-Privacy for the electronic communication sector?

- ○ Yes
- ◉ No
- ○ No opinion

Question 14: In your experience, to what extent has the e-Privacy Directive proven to have a clear EU added valueto achieve the following objectives:

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
Increasing confidentiality of electronic communications in Europe	○	○	◉	○	○
Harmonising confidentiality of electronic communications in Europe	○	○	◉	○	○
Ensuring free flow of personal data and equipment	○	○	◉	○	○

II. REVISING THE E-PRIVACY DIRECTIVE: LOOKING AHEAD

This section covers forward looking questions to assess the possible solutions available to revise the e-Privacy Directive, in case its evaluation demonstrates the need for review.

Question 15: Based on your experience with the e-Privacy Directive and taking due account of the content of the GDPR, what should be the priorities for any future legal instrument covering privacy and data protection issues in the electronic communications sector? Multiple answers possible:

- [ ] Widening the scope of its provisions to over-the-top service providers (OTTs)
- [ ] Amending the provisions on security
- [ ] Amending the provisions on confidentiality of communications and of the terminal equipment
- [ ] Amending the provisions on unsolicited communications
- [ ] Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)
- [ ] Others
- [x] None of the provisions are needed any longer

Questions 16: In your opinion, could a directly applicable instrument, one that does not need to be implemented by Member States (i.e. a Regulation), be better to ensure an equivalent level of privacy protection in connection with the processing of data in the electronic communications sector and to ensure the free movement of such data?

- ( ) Yes
- ( ) No
- (•) Other

Question 16 A: If you answered 'Other', please specify.

Text of 1 to 1500 characters will be accepted

There is no compelling reason justifying keeping a separate legal instrument such as the ePD since its privacy provisions are covered by the GDPR, which explicitly aims at regulating the processing of personal data in the digital economy.

In this context, it is worth noting that the Commission justified the need for the revision of the DPD based on the 'rapid pace of technological change and globalisation', the 'new ways of sharing information through social networks and storing large amounts of data remotely' becoming 'part of life for many European users'. The examples the Commission brought up in its Communication, such as the right to be forgotten on 'online social networking service', data breach notification and attacks on a 'gaming service' clearly indicate that the entire review of the DPD was motivated to adjust to changes in the ICT sector.

As the overall data protection rules defined in the GDPR have now been drafted not only with this sector in mind, but with ICT being at the very heart of the reform, there seems to be no reason why a sector-specific legislation targeting this sector could be justified.

II.1. REVIEW OF THE SCOPE

The requirements set forth by the e-Privacy Directive to protect individual's privacy apply to publicly available electronic communication services (**ECS**). Such rules do not apply to so called Over-The-Top (**OTT**) services (e.g. unmanaged Voice over IP, instant messaging, web mail, messaging in social networks). This may result in both a void of protection for citizens and in an uneven playing field in this market. Although the rules to protect personal data of Directive 95/46/EC and the future GDPR apply to OTT communications services, some specific rules of the e-Privacy Directive, such as the principle of confidentiality of communications, do not apply to these services. See background document for more details (see Section III.2).

Question 17: Should the scope be broadened so that over-the-top service providers (so called "OTTs") offer the same level of protection when they provide communications services such as Voice over IP, instant messaging, emailing over social networks).

- ○ Yes
- ○ In part
- ○ Do not know
- ◉ Not at all

Question 19: In your opinion, which obligations should apply to the following types of networks (eventually subject to adaptations for different actors on proportionality grounds)?

	All networks, whether public, private or closed	Non-commercial WIFI Internet access (e.g. ancillary to other activities) provided to customers/public in, e.g. airport, hospital, mall, universities etc.	Only publicly available networks (as currently)
Security obligations	○	○	◉
Confidentiality of communications	○	○	◉
Obligations on traffic and location data	○	○	◉

II.2. ENSURING SECURITY AND CONFIDENTIALITY OF COMMUNICATIONS

The e-Privacy Directive requires Member States to ensure confidentiality of communications in public communication networks and for related traffic data. Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the consent of the citizen concerned, except when legally authorised, is prohibited. The requirement for prior consent is extended to cover the information stored in users' terminal, given that users have very sensitive information in their computers, smartphones and similar devices. See background document for more details (see Sections III.3 and III.4).

Question 20: User empowerment and the possibility for users to protect their communications, including, for example, by securing their home WiFi connections and/or by using technical protection measures, is increasingly relevant given the number of security risks.

Do you think that legislation should ensure the right of individuals to secure their communications (e.g. set forth appropriate passwords for home wireless networks, use encryption apps), without prejudice of law enforcement needs to safeguard important public interests in accordance with the procedures, conditions and safeguards set forth by law?

- ○ Yes
- ◉ No
- ○ Do not know

Question 20 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

No law should restrict individuals' ability to access and use the best possible technology/methods to secure and protect the confidentiality of the communications, a right enshrined in the Charter of Fundamental Rights.

Companies should remain free to select, adjust and enhance the security measures appropriate to the risks presented by their data processing activities (a recognised principle of the EU acquis, see GDPR or NIS).

It is not sustainable to only talk about securing communications in the commercial context. The protection granted by the Charter is universal and should also be ensured in the law enforcement context. Law enforcement and national security agencies should be able to access data – subject of course to adequate safeguards. However, many proposed or existing national legislation pose a serious threat to the right to secure communications (e.g. proposals in Hungary to prohibit use of encryption software, or in France to increase sanctions on companies failing to decrypt data for terrorism investigations).

An expansion of the ePD to cover OTT services could undermine the very privacy it is seeking to protect. Many of these services are engineered to apply the best possible encryption technology, but the ePD could have the absurd effect of undermining their ability to guarantee the security and confidentially of the communication through the use encryption due to the fact the Article 15 (1) allows Member States to restrict this right.

Question 21: While an important number of laws imposing security requirements are in place, numerous publicly reported security breaches point to the need for additional policy measures. **In your opinion, to what extent would the following measures improve this situation?**

	significantly	moderately	little	not at all	do not know
Development of minimum security or privacy standards for networks and services	○	○	○	◉	○
Extending security requirements to reinforce coverage of software used in combination with the provision of a communication service, such as the operating systems embedded in terminal equipment	○	○	○	◉	○
Extending security requirements to reinforce coverage of Internet of Things devices, such as those used in wearable computing, home automation, vehicle to vehicle communication, etc.	○	○	○	◉	○
Extending the security requirements to reinforce coverage of all network components, including SIM cards, apparatus used for the switching or routing of the signals, etc.	○	○	○	◉	○

Question 22: The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated critics that citizens do not have a real choice. **To what extent do you agree to put forward the following measures to improve this situation?**

	strongly agree	agree	disagree	strongly disagree	do not know
Information society services should be required to make available a paying service (without behavioural advertising), as an alternative to the services paid by users' personal information	○	○	○	◉	○
Information service providers should not have the right to prevent access to their non-subscription based services in case users refuse the storing of identifiers in their terminal equipment (i.e., identifiers not necessary for the functioning of the service)	○	○	○	◉	○

Question 22 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

DIGITALEUROPE is very concerned about the proposal to prescribe business models and way of operation. One of the pillars of the ePD is its technology neutral approach outlined in Article 14, which should be the case for business models as well.

Online services are too diverse to apply a one-size-fits all rule. A fee-based service may work for certain business models, but would be in direct contradiction with a large number of others. In addition, such rules would be disproportionate to the objectives pursued and goes against the freedom to conduct a business, another fundamental right granted by the Charter (Article 16).

Regarding cookies, many are necessary for operation of websites, or for full functionality, albeit they may not be “essential”. It does not make sense to demand access where such cookies are refused.

From a privacy/consumer standpoint, the key is to ensure transparency and to empower users to make informed decisions. This is ensured by the GDPR, which provides for very strict transparency requirements (including on profiling and online advertising) and rules regarding what is considered to be a valid legal ground. These rules are sufficient to allow individuals to make informed decisions about the services they decide to use. An open market will allow companies to compete and users to rely on the services, which they believe constitute the best offerings.

Question 23: As a consumer, do you want to be asked for your consent for the processing of your personal data and other information stored on your smart devices as regards the following? Select the option for which you want to be asked for your consent (several options possible):

- ☐ Identifiers placed/collected by a third party information society service (not the one that you are visiting) for online behavioural advertising purposes
- ☐ Identifiers placed/collected by an information society service you are visiting – when their purpose is website analytics, measuring number of website visitors, where visitors go within the website, etc. (e.g. "first party" cookies or equivalent technologies)
- ☐ Identifiers placed/collected by an information society service you are visiting whose purpose is to support user experience, such as language preference cookies[1]
- ☐ Identifiers collected/placed by an information society service to detect fraud
- ☐ Identifiers collected/placed by and information society service for frequency capping (number of times a user sees a given ad)
- ☐ Identifiers collected and immediately anonymised in a way that it is impossible to identify the users’ device
- ☐ Other

[1] See Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption of 7.06.2012

Question 23 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Question 24: It has been argued that requesting users' consent to the storage/access of information in their devices, in particular tracking cookies, may disrupt Internet experience. **To facilitate this process and users' ability to consent, a new e-Privacy instrument should (several options possible):**

- [ ] Require manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings (e.g. third party cookies off by default)
- [ ] Adopt legislation, delegated acts for example, defining mechanisms for expressing user preferences regarding whether they want to be tracked
- [ ] Mandate European Standards Organisations to produce standards (e.g. Do Not Track; Do not Store/Collect)
- [ ] Introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent (e.g. unsolicited recording or filming by smart home devices)
- [ ] Support self-co regulation
- [x] Others

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Under the GDPR, online identifiers are mentioned in the definition of personal data. Thus, if they are used to uniquely identify individuals, they are subject to the GDPR consent requirements.

Rather than adding yet another set of consent rules to the regulatory mix, including through delegated acts, the future European Data Protection Board (EDPB) may consider guidance regarding cookies and similar technologies in the context of the implementation of the GDPR. The guidance should be clear, reflect the years of experience with the cookies banner and allow for creative solutions and innovation so that companies can ensure the objective of Article 5(3), namely transparency and control, in consumer friendly ways.

Self-regulation and co-regulation balances the protection and empowerment of users with fast-moving technologies. These solutions are also promoted by the GDPR. There seems to be no evidence to change this approach already (e.g. by mandating standards development activities). A new ePrivacy instrument is not required in order to promote this approach.

It is also worth recalling that the GDPR specifically puts forward rules on data protection by design and by default (Article 25). The GDPR also contains detailed rules on profiling. These provisions have been clearly proposed and drafted with the online industry in mind. Therefore, it seems counter-intuitive for the Commission to propose new rules on top of something that hasn't even been implemented yet.

Question 25: The e-Privacy Directive contains specific privacy protections for the processing of traffic and location data in order to ensure confidentiality of the related communications. In particular, they must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication or consent to users should be asked in order to use them for added value services (e.g. route guidance, traffic information, weather forecasts and tourist information). Under the existing exemptions, the processing of traffic data is still permitted for a limited time if necessary e.g. for billing purposes. See background document for more details.

Do you consider that the exemptions to consent for processing traffic and location data should be amended? You can choose more than one option. In particular, the exceptions:

- [ ] should be broadened to include the use of such data for statistical purposes, with appropriate safeguards
- [ ] should be broadened to include the use of such data for public purposes (e.g. research, traffic control, etc.), with appropriate safeguards
- [ ] should allow the data to be used for other purposes only if the data is fully anonymised
- [ ] should not be broadened
- [x] the provision on traffic and location data should be deleted

Question 25 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

The provisions on traffic and location data in the ePD should be deleted to avoid any confusion and/or inconsistencies with the GDPR. Location data is explicitly included in the definition of personal data and traffic data is personal data if it allows identifying an individual. Adequate protections for traffic data are available in the GDPR, and to the extent tighter restrictions are applicable under the ePD, these are not justified by the risks presented. In relation to the possible extension of the ePD to non-traditional communication services, it is not always clear how the requirement for only persons acting under the authority of the communications provider to process the data would apply. For location data, given processing of such data is generally held to a higher standard than other processing under the GDPR, we do not believe that additional provisions need to be maintained under the ePD.

II. 3. NON-ITEMISED BILLS, CONTROL OVER CALL LINE IDENTIFICATION, AUTOMATIC CALL FORWARDING AND SUBSCRIBERS DIRECTORY

The e-Privacy Directive provides for the right of subscribers to receive non-itemised bills. The e-Privacy Directive also gives callers the right to prevent the presentation of the calling-line identification if they wish so to guarantee their anonymity. Furthermore, subscribers have the possibility to stop automatic call forwarding by a third party to their terminals. Finally, subscribers must be given the opportunity to determine whether their personal data is included in a public directory (printed, electronic or obtainable through directory inquiry services). See background document for more details (see Section III.5).

Question 26: Give us your views on the following aspects:

	This provision continues being relevant and should be kept	This provision should be amended	This provision should be deleted	Other
Non-itemised bills	○	○	◉	○
Presentation and restriction of calling and connected line identification	○	○	◉	○
Automatic call forwarding	○	○	◉	○
Subscriber directories	○	○	◉	○

Question 26 A: Please specify, if needed.

Text of 1 to 1500 characters will be accepted

These provisions do not relate to privacy or data protection, but rather to commercial practices and consumer protection. Imposing these obligations under a set of privacy and data protection rules such as the ePD creates confusion for the users as to where their rights under EU data protection law start and end. Therefore, to the extent that these provisions are still justified and needed, they should be moved to other more relevant legislative instruments, like the Telecoms Package or consumer legislation.

In any case, they are not relevant for new communication services. In relation to itemised billing, it is often not on a per communication/per session basis for new communication services, making this provision redundant. Moreover, in the B2B context, it is unlikely to make sense in any case for the individual user/employee to determine billing presentation as opposed to the business entity. For caller ID suppression, given how many different kinds of communications services users have available to them, they should be allowed to choose whether they want ones that support anonymous calling or not. It is also not evident how this would apply to non-voice services. For call forwarding, the right seems obscure in a world where you are likely to forward calls to your own mobile device. As regards subscriber directories, these are now decentralised and build in privacy in different ways.

II.4. UNSOLICITED COMMERCIAL COMMUNICATIONS

The e-Privacy Directive requires prior consent to send commercial communications through electronic mail (which includes SMS), fax and automatic calling machines without human interaction). However, companies which have acquired an end-user's email in the context of a sale of products or services can send direct marketing by email to advertise their own similar products or services, provided that the end-user is given the possibility to object (often referred to as '**opt-out**'). Member States can decide whether to require opt in or opt out for marketing calls (with human interaction). Furthermore, the protection against all types of commercial communications also benefits to legal persons but the e-Privacy Directive leaves it to Member States to decide whether they are protected by an opt-in or opt-out regime. See background document (see Section III.6) for more details.

Question 27: Do you think that the Member States should retain the possibility to choose between a prior consent (opt-in) and a right to object (opt-out) regime for:

	Yes	No	Do not know
Direct marketing telephone calls (with human interaction) directed toward individual citizens	○	◉	○
Direct marketing communications to legal persons, (automatic calling machines, fax, e-mail and telephone calls with human interactions)	○	◉	○

Question 28: If you answered "no" to one or more of the options in the previous question, please tell us which system should apply in your view?

	consent (opt-in)	right to object (opt-out)	do not know
Regime for direct marketing communications by telephone calls with human interaction	○	◉	○
Regime of protection of legal persons	○	◉	○

Question 28 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

The numerous initiatives for opt-out lists for direct marketing calls at national level show that users trust the opt-out mechanism and are using it in practice. This is also the solution that the GDPR applies when subjecting direct marketing to robust right to object rules.

II.4. FRAGMENTED IMPLEMENTATION AND INCONSISTENT ENFORCEMENT

Some provisions of the e-Privacy Directive may be formulated in too broad and general terms. As a consequence, key provisions and concepts may have been implemented and transposed differently by Member States. Moreover, while the Data Protection Directive entrusts the enforcement of its provisions to data protection supervisory authorities, the e-Privacy Directive leaves it up to Member States to designate a competent authority, or where relevant other national bodies. This has led to a fragmented situation in the Union. Some Member States have allocated competence to data protection supervisory authorities (DPAs), whereas others to the telecom national regulatory authorities (NRAs) and others to yet another type of bodies, such as consumer authorities. See section III. 7 of background document for more details.

Question 29: Do you consider that there is a need to allocate the enforcement to a single authority?

- (●) Yes
- ( ) No
- ( ) Do not know

Question 30: If yes, which authority would be the most appropriate one?

- (●) National data protection authority
- ( ) National (telecom) regulatory authority
- ( ) National Consumer protection authority
- ( ) Other

Question 30 A: If 'Other', please specify.

Text of 1 to 1500 characters will be accepted

```
Rules on privacy and data protection should be enforced by national data
protection authorities to avoid overlap and confusion.
```

Question 31: Should the future consistency mechanism created by the GDPR apply in cross-border matters covered by the future e-Privacy instrument?

- (●) Yes
- ( ) No
- ( ) Do not know

Question 32: Do you think that a new e-Privacy instrument should include specific fines and remedies for breaches of the relevant provisions of the new e-Privacy legal instrument, e.g. breaches of confidentiality of communications?

- ( ) Yes
- (●) No
- ( ) Do not know

Question 33: These questions aim to provide a comprehensive consultation on the functioning and review of the e-Privacy Directive. Please indicate if there are other issues that should be considered. Also please share any quantitative data reports or studies to support your views.

Text of 1 to 3000 characters will be accepted

Please upload any quantitative data reports or studies to support your views.

Background Documents

document de rfrence (/eusurvey/files/c6df1ba2-dd8d-4833-829d-5d777561d8c6)

Contact

Regine.MENZIES@ec.europa.eu