Contribution ID: 004d9d5c-ce01-42e2-99f8-46783875c84a
Date: 05/07/2016 17:49:51

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-1739884.

* **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.

57305017757-64

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

Center for Democracy and Technology (CDT)

Question III: Please enter your organisation's address:

1401 K Street NW, Suite 200, Washington, DC 20005

Question IV: Please enter your organisation's website:

www.cdt.org

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

Jens-Henrik Jeppesen, Director European Affairs

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

+32 477 18 32 85

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

jjeppesen@cdt.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

* Question IX A: Please specify:

USA

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

CDT has not done research on the functioning of the e-Privacy Directive. We are aware of the European Commission's report: "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation". https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data. This report concludes among other things that: "... at the moment of the adoption of this provision in 2002, all Member States had already long since introduced legislation protecting the confidentiality of private communications. The transposition of Art. 5.1 did not have a harmonizing effect on these existing national legal provisions. The legal protection of confidentiality of communications in the Member States remains therefore diverse".

The question of how effective the Directive has been in achieving its objectives is of course distinct from the question of whether those objectives were the right ones at the time, and what should be the objectives of a possible future legislative instrument.

Looking ahead, the following questions will be key: Which provisions of the EPD continue to be essential, given technological, market and legislative developments? To what extent are these provisions covered in the GDPR or other pieces of legislation? If they these provisions are not covered in other instruments, how should they then be brought about?

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

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

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

The question is whether operation of electronic communications infrastructure is an activity that requires a distinct regulatory framework. The answer is yes. ECS run on physical infrastructures of strategic importance to society. As is the case with other utilities policy makers have a legitimate interest and responsibility in making sure that ECS perform to the benefit of society and the economy as a whole.

Whether separate rules on data protection are justified is another matter. As the Commission has noted, there has been significant convergence and substitution between traditional PSTN-based ECS and Internet-based voice and messaging services. From both from the user and the provider perspective, it is desirable that similar services are subject to similar rules. One question to consider is whether there are data protection/privacy issues specific to the provision of Internet Access Services or operation of ECS networks.

A new legislative should be targeted at problems that are not covered effectively in other EU legislation. A compelling argument for proposing a new instrument to replace the E-Privacy Directive is the fact that the GDPR is not based on Article 7 of the Charter of Fundamental Rights of the EU on the right to privacy and confidentiality of communications. EU Member States are bound by Article 8 of the European Convention on Human Rights, but in the absence of EU legislation, there is arguably a risk of fragmented implementation.

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

It seems to us that the Framework Directive, the General Data Protection Regulation and the future NIS Directive include obligations that are consistent with those in the the EPD.

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

We do not have particular insights to offer on this question. It appears that the types of marketing mentioned in Article 13.1 are no longer particularly relevant for today's market place. Online advertising has changed significantly since the adoption of the Directive, and further dramatic shifts can be expected as technology evolves.

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

```
Answering this question requires data on (1) whether there are different
levels of trust in ECS in different Member States and (2) whether such
differences, if they exist, are due to different implementation of the EPD,
or other factors. We do not have such data.
```

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

```
CDT does not have data on this question.
```

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

CDT does not have data on this question.

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
- [x] 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
- [ ] 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

The answer to this question is not straightforward. A Regulation should in principle, due to its direct applicability, ensure a higher level of harmonisation. However, it can reasonably be expected that, for this reason, Member States will work to secure more and broader exceptions to a Regulation. The language of a Regulation will probably be crafted to ensure a certain level of flexibility, which will then leave broader scope to regulatory authorities to interpret it. An example is the Telecommunications Single Market Regulation (2015/2120). The regulation includes fairly short provisions on non-discrimination of traffic in Internet Access Services and instructs regulatory authorities to develop detailed implementing guidelines.

That said, the most appropriate choice of instrument is probably a Regulation. The fact that GDPR is a Regulation suggests that any complementary instrument should also be a Regulation. In terms of substance, a new instrument should be conducive to the provision of a wide range of communications services, built on different business models and using different technologies. It should be flexible enough and technology neutral enough to enable innovation and development of new types of services, with different pricing models, levels of quality, and other attributes. Such an instrument should be focused narrowly on those topics not covered by existing regulation, notably the GDPR.

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 18: If you answered "yes" or "in part" to the previous question, please specify which e-Privacy principles & obligations should apply to so called OTTs (multiple replies possible):

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
Security obligations	○	○	◉	○	○
Confidentiality of communications (prior consent to intercept electronic communications)	○	◉	○	○	○
Traffic and location data (prior consent to process)	○	○	◉	○	○
Unsolicited marketing communications (i.e. should Article 13 apply to messages sent via OTT services?)	○	○	◉	○	○

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

Application of strong, state-of-the-art encryption technology is essential to secure and reliable communications, and to protect the data being communicated. It is of great concern that some Member States consider legislation that may inhibit the deployment of end-to-end encryption. Communications providers and users should be free to use the best available security solutions.

In considering the need for a new instrument, it is essential to ensure that it would not result in limitations on the freedom of communications providers or users to apply encryption to their communications and data. It is possible that a new instrument could be used to safeguard this freedom.

There is currently significant uncertainty about the conditions under which law enforcement authorities are able to intercept, access and decrypt communications and data (and compel providers to assist in obtaining it). A legislative instrument could possibly be used to ensure that access by law enforcement agencies to data is subject to the safeguards that have established in EU law and by the Court of Justice of the EU, and in the European Convention on Human Rights.

On 20 May 2016, Europol and ENISA issued a joint statement on encryption and privacy, in which they among other things noted the need for "...more explicit and ideally aligned regulation of the lawful online use of privacy-invasive investigative tools and the conditions under which they can be applied".

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

Both measures seem disproportionate in their interference in the freedom of a service provider to develop its business model. Their practical impact might be to shut down successful services that consumers appreciate and stop European businesses from getting off the ground. But, service providers should be required to provide clear and understandable guidance about their behavioural advertising practices, in order that users can make informed choices.

At the same time, the greater the market power of the service provider in question, the stronger the argument for regulatory interference in its business practices. If the provider of a service that is all but indispensable for consumers enjoys such market power that no alternative provider exists, the case for intervention is strengthened.

There may be a case for specific obligations on providers of Internet Access Services on this issue, depending on specific market conditions. There may also be a case for obligations on public sector services in order that citizens are not be required to accept identifiers in order to access public sector information or services.

Tracking practices will need ongoing attention from regulators, and far better transparency of behavioural advertising practices is needed. There are many legitimate reasons for people to resist tracking, and if this preference limits their ability to communicate and seek information, it raises both privacy and free expression issues.

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):

- [x] 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

What is important for the user is transparency into the sharing and use of data and an ability to make informed choices on that basis. This applies to personal data in any context. The consent mechanisms can be different depending on the technology used and other factors. It seems that the framework provided by the GDPR covers the examples listed above.

Rapid advancement in tracking technology has highlighted the need for consumer protection in this area. While consumers likely understand first-party tracking, in which the service provider saves information in order to enhance user experience, third party tracking remains less understood. Third party tracking is also more pervasive. Moreover, other less visible forms of tracking like browser fingerprinting, which uses the unique preferences each user sets for their browser as an identifier, should be disfavoured precisely because consumers cannot avoid such practices. Using an individual's preferences against them without notice, consent, or opt-in clearly obviates the consent model.

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
- ☑ Others

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Any e-Privacy instrument should be as technology neutral as possible. Technology is advancing fast, and it is likely that the use cases we are thinking about today will not be relevant in a few years' time. The best scenario is one in which service providers deliver clear and unambiguous information about their use of data. On that basis, users can choose whether and to what extent to engage with these services. There is no reason why consent rules and requirements for notices should be different for a communications service provider than for any other business (data processor or controller under the GDPR). An example: Consider a retail store that uses behavioural advertising. In one scenario, it uses the in-store WIFI to track customers' smartphones (or other wearable devices) to understand their movements in the shop and their interests and preferences. In another scenario it uses video surveillance and facial recognition tools to do the same. Both scenarios are clearly privacy-invasive and should be subject to clear consent. Consent rules are provided in the GDPR, and there seems no compelling reason why they should not cover both scenarios. In both cases, the customer should be fully informed about the data collection and processing that goes on. It would make sense for self-regulation and/or DPAs /the EDPB to develop the consent mechanisms that would work for these scenarios. It is unlikely that legislation is the right approach, given rapid technology development.

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:

- [x] should be broadened to include the use of such data for statistical purposes, with appropriate safeguards
- [x] 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
- [ ] 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

With rapidly evolving technology, and new digital services being deployed, it is likely that more processing of personal data will involve electronic transmission of that data. That makes it essential that a new instrument replacing the EPD does not duplicate GDPR provisions.

Many types of location and traffic data will no doubt be considered as personal data under the GDPR. Traffic and location data that are in isolation anonymous may in combination be considered personal data, depending on whether and how easily they allow an individual to be identified. The boundary between personal and anonymous data is likely to shift depending on context, and data protection authorities will need to evaluate different scenarios on an ongoing basis. Overall, there would seem to be a strong case for deferring to the GDPR on traffic and location data. This could create a more flexible and innovation-friendly regime, and would be preferable to broadening the legacy EPD provisions to a potentially broad set of services.

There does not seem to be a need to carry over the concept of value-added services to a new instrument. Different bundles of services can be envisaged, including ones in which a communications service is provided as an additional feature to another service. For example, a travel agent may offer a chat service as part of its business. A connected car will transmit data over an electronic communications network, but transport is the main service being offered.

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

```
CDT does not have views on the utility and practical value of these
provisions.
```

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

CDT does not have views on these questions.

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

One of the main objectives of the GDPR is to ensure consistent application of rules across the EU, and to provide for mechanisms to deal with cross-border disputes. DPAs deal with personal data across all sectors, both private and public, and there does not seem to be any reason they should not be responsible for communications services.

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

Overall, CDT would list the following priorities for the EPD review.

- The Review should maintain robust protection of the confidentiality of communications.
- It should not result in duplicative and possibly inconsistent provisions in different pieces of legislation, notably the GDRP. More and more processing of personal data involves transmission of that data over communications networks. Where at all possible, deference should be given to the GDPR.
- It should result in as harmonised a framework as possible. This would be to the benefit of service providers and users alike.
- It should result in a regime is conducive to the provision of a broad range of communications services, built on different business models and using different technologies. It should be flexible enough and technology neutral enough to enable innovation and development of new types of services, with different pricing models, levels of quality, and other attributes.
- It should not result in less stringent rules for law enforcement agencies seeking access personal data or private communications, and it should not limit the freedom of users and providers to use state-of-the-art encryption solutions.

There are advantages and drawbacks to proposing a new instrument. Many areas covered by EPD are covered by GDPR and other legislation. A compelling argument for a new instrument would be that whereas the EPD is based on Art 7 of the Charter of Fundamental Rights, GDPR is based on Art. 8. A new instrument should focus narrowly on addressing identified 'gaps' in protection, rather than import concepts from the EPD into the GDPR framework. If such gaps can be dealt with under GDPR (e.g. through delegated acts) this should be considered. In that sense, 'widening the scope' of the EPD does not seem desirable. But ensuring a consistent level of protection regardless of the underlying technology, is. Personal data processed in the context of communications should be subject to the same protection as any other data. It is likely that more and more processing of personal data will involve electronic transmission of that data, in one form or another. This makes the scope for duplication and/or inconsistency between GDPR and a new instrument very considerable. Also, the balance expressed in GDPR reflects several years of negotiation. From a data protection standpoint it would be important to ensure that proposing a new instrument does not result in a weakening of the standards set by GDPR.

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