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.

71149477682-53

*

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

Access Now

Question III: Please enter your organisation's address:

20 Rue Belliard
1040 Brussels
Belgium

Question IV: Please enter your organisation's website:

https://www.accessnow.org/

*

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

Estelle Massé

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

*

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

estelle@accessnow.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

Since its adoption in 2002, the e-Privacy Directive has not achieved its objectives, partially due to fragmented implementation, weak enforcement and its failure to anticipate the rapid development of technology. At the time of its adoption, the legislators did not adequately capture the impact that smartphone applications, online tracking, javascript, social media services, or behavioural advertising would have on internet users' right to privacy and confidentiality of communications. The Directive's market oriented objectives on the free movement of data and equipment were somewhat successful, as reflected by the development of Big Data and Internet of Things products and services in the last decade. However, these activities and their impacts on users' privacy need to be further addressed in the review process to ensure trust and confidence of users in those products.

In the spirit of the recently concluded EU Data Protection Reform, the current e-Privacy rules need to be modernised and upgraded to fit to today's reality for the protection of privacy and confidentiality of communications. Furthermore, the differences in the implementation of the rules by each Member State results in unequal protections and safeguards for users across the EU as well as complexity for cross-border businesses. Given these challenges, and for sake of consistency with the recently adopted General Data Protection Regulation (GDPR), the future e-Privacy framework should be a Regulation.

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

The differences in implementation and enforcement across the EU have caused difficulties for users in understanding how their personal information is used by online actors and providers of electronic communications services. According to the 2015 EuroBarometer, more than half of the respondents reported concerns about mobile services or applications providers recording their everyday activities. These concerns highlight the need for robust and clear safeguards for the protection of users' data and confidentiality, which will lead to increased trust in services.

While data breach notification is covered by the GDPR, other issues remain to be tackled. The e-Privacy review should specifically ensure protection of traffic and locations data and the principles of data minimisation, purpose limitation, and data protection by design defined under the GDPR. Overall, the future e-Privacy legislation should promote the development, spread, and use of technologies that protect the confidentiality of communications - both content and metadata - and safeguard user anonymity. To that end, the legislators should refrain from establishing specific technical standards or requirements as those could hinder security and create vulnerabilities that negatively impact users' rights and ultimately undermine the objective of the e-Privacy.

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

The e-Privacy Regulation will seek to protect user privacy by complementing and particularising the GDPR. The GDPR does not specifically cover the right to private life enshrined in Article 7 of the EU Charter of Fundamental Rights, and specific protections will have to be articulated in the future revised e-Privacy. Enforcement of the future e-Privacy legislation should be assigned to the data protection authorities (DPA), who have expertise in this area, and not to telecoms regulators, as is currently often the case. This will also facilitate uniformity across sectors, as DPAs are already tasked with enforcing the GDPR.

While implementation of a single set of rules agreed under a Regulation will facilitate harmonised enforcement and help users seek redress of privacy violations, further safeguards for an efficient right to remedy must also be put in place. Specifically, the future e-Privacy legislation should apply the "cooperation and consistency" enforcement mechanism agreed upon under the GDPR and include similar administrative fines. In addition, to improve users' access to remedy the e-Privacy should clearly authorise consumers and non-for-profit organisations to represent a user or a group of users in claims in front of supervisory authorities. To ensure meaningful access to remedy, the legislation should also make clear that participation in administrative enforcement mechanisms do not preclude or prevent users from seeking judicial remedy.

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

As lex specialis, the e-Privacy must maintain and upgrade rules on confidentiality of electronic communications, traffic and data location, unsolicited communications, and itemised billing. New rules on tracking and mandatory transparency reporting should also be introduced and implemented (see attached report). Alignment with the GDPR will be crucial to avoid conflict of laws, uncertainty for users' rights, and administrative burden for the industry. To that end, the issue of data breach notification is sufficiently covered under the GDPR and need not be re-addressed under e-Privacy. Furthermore, all definitions of core concepts, such as consent, data minimisation or purpose limitation, agreed under the GDPR should be incorporated into the future e-Privacy legislation.

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

The referenced legal instruments establish security obligations and requirements that broadly correspond to the objectives of the e-Privacy Directive. To avoid duplication, administrative burden and uncertainty, the security obligations set under the e-Privacy Directive should re-assessed against those instruments. While the requirement set under the Telecoms Framework and the Radio Equipment Directive appear to complement each other, the Network and Information Security Directive specifically refers to the security requirements set under the GDPR. We encourage the legislators to follow the same approach in the e-Privacy review and reflect the provisions established by 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

A harmonised approach toward opt-in requirement for telemarketing calls must be included in the future e-Privacy legislation. Telemarketing calls are highly intrusive, and the process through which marketing companies obtain user information is opaque and outside of user control. Requesting prior consent will ensure user empowerment and control over his or her personal information. For the sake of consistency, the definition of consent should be the one agreed under the GDPR, which requires that a user decision is affirmative, express, and informed.

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

The 2015 EuroBarometer indicated that two-thirds of respondents to the survey are concerned about not having control over the information they provide online. Respondents are particularly concerned about the recording of everyday activities via providers of mobile phone networks or applications, the recording of everyday activities on the Internet, and the tracking of their behaviour via payment cards. While those concerns have increased since the last 2010 survey, only 37% of the respondents are aware of the existence of data protection authorities and even those respondents broadly do not know how to seek assistance and redress.

The findings of the 2015 EuroBarometer highlights the need for stronger rules in protecting user privacy, anonymity and confidentiality of communications in the future e-Privacy legislation, while strengthening users' access to remedy for violations of these protections. With its "cooperation and consistency" enforcement mechanism, the GDPR provides a robust basis of harmonised enforcement and takes important steps for easier access to remedy for users. While the enforcement mechanism agreed under the GDPR should be reflected in the future e-Privacy legislation, it should also include an additional provision clearly authorising consumers and non-for-profit organisations to represent a user or a group of users on claims in front of supervisory authorities.

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

Member States have taken advantage of the current uncertainty under EU law to enact data retention mandates, which have a deleterious impact on human rights, the environment, and the digital economy. The retention of vast amount of data requires massive storage capacity, cooling systems, security protections and more. While the costs of data retention have been demonstrated and highlighted in the EU Commission impact assessment on the Data Retention Directive (DRD), the necessity and proportionality of data protections measures remains to be proven. In Joined Cases C-293/12 and C-594/12, the EU Court has highlighted the severe impact on the right to privacy of this highly intrusive scheme. Article 15 of the e-Privacy Directive should be removed in the review process in order to remedy these problems.

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

Any compliance costs associated with the privacy and security obligations of the e-Privacy Directive are at least mitigated by the benefits produced by the same privacy and security obligations in regard to increased user trust and networks' protection. These compliance and related administrative costs can be further mitigated by changing the nature of the e-Privacy instrument from a Directive to a Regulation, free of national exceptions or derogations.

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:

- [x] 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
- [x] Amending the provisions on unsolicited communications
- [x] Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)
- [x] 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

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

Legislation, and in particular the upcoming e-Privacy legislation, should ensure the right of individuals to secure their communications. Legislators should not erode the security of devices or applications by either introducing a legal requirement for vulnerabilities or backdoors into products or service or by pressuring companies to keep and allow law enforcement access to data, or have disproportionate access to the encryption keys to private data. There are no known methods to provide for a secure “magic key” or other form of exceptional access. Any vulnerabilities or backdoors can be used for both good and bad. Any attempt to undermine the development or use of encryption or other tools and technologies protecting the confidentiality of communication would also undermine the fundamental right to privacy as well as the integrity of communications and systems, and therefore stands at odds with the objective of the e-Privacy.

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

On the first question: Under Article 16 of the EU Charter of Fundamental Rights, companies enjoy the freedom to conduct a business and should therefore not be "required to make paying services available." However, even services offered free of charge in the EU have the duty and obligation to comply and respect Article 7 and 8 of the EU Charter, guaranteeing fundamental rights to privacy and data protection, as well as with relevant legislation such as the GDPR and the future e-Privacy legislation. Therefore, if companies seek to implement behavioural advertising or other types of intrusive measures, they must, at minimum, comply with data protection rules.

On the second question: Access to a service should not be dependent on user's agreement to vague, opaque, and abusive terms of service or intrusive tracking. This concept is intrinsically contrary to the principles of informed and freely given consent. Users should have a right to access and use websites and other online services without being monitored or disproportionately tracked.

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
- [x] 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
- [x] 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

The current rules under the e-Privacy Directive fail to distinguish between different types of online tracking. Cookies, for example, can be used to facilitate the mere functioning of websites, for analytics, for advertising, or for cross-website tracking, as well as other reasons. There are different types of cookies, including first-party or third-party hosted, and their impact on privacy varies extensively. Most of these distinctions are not made transparent to users. The obligations and requirements link to the use of tracking technologies established in the e-Privacy Directive should be reworked to distinguish between different forms of tracking. The more privacy-invasive the tracking, the stricter the user protections should be. Specifically, users should be informed about the most invasive types of tracking such as identifiers placed and/or collected by a third party information society service for online behavioural advertising purposes and identifiers collected or placed by an information society service for frequency capping, the use of which by telecoms providers has increased exponentially over the past years (see report linked at the end of this consultation).

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):**

- [x] 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
- [x] Mandate European Standards Organisations to produce standards (e.g. Do Not Track; Do not Store/Collect)
- [x] 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

Data protection by default and by design, as well as the development of technical standards, such as Do Not Track, as legal standards, have been included in the GDPR and should be reflected in the future e-Privacy legislation. Further specification on the particular use of these technical standards within the context of e-Privacy could be included in the revised framework to provide certainty. Finally, introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent, would be a welcome development to strengthen user’s right to privacy.

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
- ☐ 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 e-Privacy Directive establishes that traffic and location data must be erased or made anonymous once it is no longer needed for the purpose of the transmission of a communication, unless the user has consented to the use of this data for “value added services”. There are further exemptions that allow the processing of non-anonymised data without consent for a limited period of time and if “necessary,” such as for billing purposes.

While this data can be valuable for public purposes, and research in particular, user consent for these specific uses should be requested to ensure individual control over his or her personal information. Furthermore, rules and safeguard on supposedly “anonymised” data should be strengthened. Recent studies from Open Rights Group on the use of anonymised traffic and location data in the UK have shown that in many cases personal attributes such as names were replaced by a code which still enable identification of the users.

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

The future e-Privacy framework should maintain and improve the provision on non-itemised bills. Non-itemised bills are particularly relevant to ensure users' privacy at the workplace or when several users share a same bill.

The current provisions should be revised and tightened to ensure that they do not lead to unintended consequences, such as unreasonable retention period for detailed user web history logs by companies on the ground that users might challenge data charges. Transparency provisions on billing and monthly consumptions should be developed to reduce this risk and clear rules preventing the retention of log in or communication transmission information by companies should be in place.

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

User opt-in consent guarantees individual's retain control over his or her personal information. As provided for in the GDPR, consent should be informed and freely given. Not only it is the fundamental right of users to have their personal information protected, which means that this information should be used on the basis of their consent as established by Article 8.2 of the EU Charter of Fundamental Rights, but it is also what users want, according to the result of the 2015 EuroBarometer: 67% of users indicated concern about not having complete control over the information they provide online.

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

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

Thank you very much for the opportunity to provide inputs though this consultation.
To support our submission please find attached, a joint letter signed by more than 100 organisations and companies encouraging lawmakers to ensure safety and security of users, companies, and governments by strengthening the integrity of communications and systems. In doing so, governments should reject laws, policies, or other mandates or practices, including secret agreements with companies, that limit access to or undermine encryption and other secure communications tools and technologies.

We would also like to share with you our work on transparency reporting. Transparency reporting is one of the strongest ways for technology companies to disclose threats to user privacy and free expression. Such reports educate the public about enforcement of company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, network disruptions, content removal, and a host of other practices impacting our fundamental rights. Please find attached our Transparency Reporting Index, a resource that contributes to important efforts tracking how well companies across the globe are meeting their responsibility to respect human rights in the digital age.

Finally, please find here our global report, “The Rise of Mobile Tracking Headers”: https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf In October 2014, Access Now launched AmIBeingTracked.com to enable mobile broadband users from around the world to determine whether their service provider was using “supercookies” — special tracking headers that the carriers inject beyond the control of the user. Since its launch in October 2014, more than 330,000 people used the tool, and the results showed significant, secret, global deployment of supercookies. We have conducted tests in 10 countries, two of which are EU member states, Spain and the Netherlands. We found that at least two carriers in those EU countries used supercookies, without notifying affected users. We also found that the use of the “Do not track” tools in web browsers did not block or prevent the tracking headers injected by the telecoms operators.

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

6fd087b4-41dd-4be1-82c9-e67069799127/Global_Letter_-_Encryption_-_Access_Now.pdf
6fb5d530-e93d-4427-80a7-1e7ae49038b8/Transparency-Reporting-Index_-_Access_Now.csv

Background Documents

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

Contact

Regine.MENZIES@ec.europa.eu