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.

174457719063-67

*

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

Mozilla

Question III: Please enter your organisation's address:

51 Rue du Trone, 1050 Ixelles, Belgium

Question IV: Please enter your organisation's website:

https://www.mozilla.org/

*

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

Raegan MacDonald

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

*

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

raegan@mozilla.com

*

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 VIII C: Please specify if your company is an SME (<250 staff) or micro-enterprise (<10 staff):

See for the definition of SME and micro-enterprise EU recommendation 2003/361

- ○ SME
- ○ Micro-enterprise
- ◉ None of the above

*

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:

```
Mozilla is a global non-profit organisation with a primary registration as a
public benefit organisation in the 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

We've answered "little" to the first question for the following reasons: First, the choice of instrument -- a Directive -- means that there are 28 different implementations of this directive, which fragments the protection of communications within the EU. For technology companies hoping to do business across the EU, this provides compliance difficulty and risk.Secondly, some aspects of the directive have been implemented in a way that does not necessarily enhance user control and privacy. While consent is generally good for user control and the preservation of privacy, there is a stark difference between the spirit of the directive and the implementation. For example, the implementation of Article 5(3) has resulted in "notification fatigue", where users are prompted to "agree" to cookies without context around what cookies they may be using (e.g. first party cookies required for functionality vs. third party add ons the user may not want or need). The EPD has been an important instrument to advance national legislation fostering the privacy, security, and confidentiality of communications. However, since its adoption and revision, a number of legal instruments have been put in place which contribute to many of the same objectives.A review of the EPD could improve the challenges outlined above, but first, a consistency exercise should be carried out, to ensure that there are not conflicting obligations for companies among existing directives and regulations (e.g. GDPR, NIS).

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

We answered "no opinion" on prompt 3 as Mozilla does not collect this information. The last 5 elements in the chart are outside of the scope of our activities and data practices. On 2nd prompt, we've experienced and witnessed significant problems in understanding and applying Art5(3) of the EPD. This has achieved neither user trust and greater privacy nor legal certainty for online businesses. There is a need to update and harmonise the way in which the rules are interpreted, particularly on exemptions to Art5(3). Firstly, the different interpretations for when storing and gaining access to information is permitted under Art5(3) has created confusion and logical inconsistencies with the GDPR. Secondly, in many cases, the implementation of this provision has resulted in "notification fatigue" for users which has the adverse and unintended effect of undermining trust and control, rather than fostering it. Consent on its own is meaningless if it doesn't include (a) clear information to the user that empowers them to make informed decisions, and (b) the ability to indicate their preference such as what information and under which circumstances it may be used.Providing users with effective means to control their online presence have proven in many cases more effective than consent notices required by EPD.For Mozilla they are addressed at a technical level through various browser-based tools, like Tracking Protection in Firefox, content and cookie controls, or third-party add-ons.

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

As we have explained in questions 1A and 2A, some provisions of the EPD (and Article 5(3) in particular) have generated confusion on behalf of users and businesses which regrettably undermine the spirit of the EPD.
Assigning enforcement to different authorities magnifies the inherent divergence of a Directive as a vehicle. Businesses and enforcement authorities – whether DPAs or NRAs – in practice, have different interpretations of the law. The age of the EPD worsens the circumstances further – it was drafted over a decade ago, and in the intervening years (including since its last review in 2009), the landscape for online service has evolved immensely. It is difficult to know today which new services apply to the EPD's sometimes prescriptive rules. Furthermore, the data protection directive (95/46/EC) and the EPD also differ, making it difficult to understand which framework to follow (e.g. for data breach notification obligations), and whether a particular product or service would mean a business is an Information Society Service (ISS) or a data controller.

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

We answered “no” regarding data breaches as this is addressed in great detail in the GDPR. We emphasise that before the EPD review process is taken any further, a comprehensive consistency exercise should be undertaken to ensure that there remain no further conflicting provisions, which make it difficult for companies to interpret. Furthermore, a clear application and interpretation on behalf of enforcement authorities would also be necessary to create harmonisation and legal certainty for electronic privacy in the EU.
We answered “yes” to the next two questions, as there is value in further ensuring the protection of the confidentiality of communications and on the collection of traffic and location data. This is particularly relevant as mobile technology increases, and more and more devices become connected to the internet. Rules of the road that provide a baseline level of protection of user privacy and the increasing amount of data that can be collected, shared, and stored via the internet of things are demonstrably useful. However we underline that the current obligations, if reviewed, should be carefully crafted to avoid the current pitfalls with implementation. These issues, such as the implementation of Article 5(3) have been made clear in questions 1A and 2A.

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

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

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

National provisions implementing the e-Privacy Directive have contributed little to raising users' trust. Some provisions of the EPD have been implemented in a way that have not resulted in the advancement of user control, trust and transparency. The application of Art5 in particular has led to a situation whereby users are prompted to click through notices before accessing a service or visiting a website. Studies have shown that more alerts and notices to a user does not increase, but can significantly undermine, trust for the service or website. For e.g. see this survey on data breach notification fatigue: http://bit.ly/29t8kUx. Also, it is questionable whether or not consent can be achieved if the user is not also given the opportunity to make a choice (see our answer to Q1A&2A). The GDPR addresses this issue, and we strongly recommend looking to this instrument to ensure consistency if a review of the EPD is found to be necessary.From the perspective of businesses,varied implementations in MS also resulted in various, at times conflicting interpretations of EPD that ultimately stood in the way of consistent enforcement and application of the rules.See this sheet which highlights the significant variances in implementations of only a handful of member states: http://bit.ly/29qhPWU.These factors have contributed to an environment of legal and consumer uncertainty on the spirit, application, and enforcement of EPD, which undermines, rather than fosters, trust online.

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

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

I.5. EU ADDED VALUE OF THE ERIVACY DIRECTIVE

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

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

- ○ Yes
- ○ No
- ◉ No opinion

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

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

II. REVISING THE E-PRIVACY DIRECTIVE: LOOKING AHEAD

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

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

- ☐ Widening the scope of its provisions to over-the-top service providers (OTTs)
- ☐ Amending the provisions on security
- ☑ Amending the provisions on confidentiality of communications and of the terminal equipment
- ☐ Amending the provisions on unsolicited communications
- ☑ Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)
- ☑ Others
- ☐ 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 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

Article 7 of the Charter of Fundamental Rights establishes the right of individuals to secure their communications. This right is further specified in member state law and European case law. The Mozilla Manifesto states, “privacy and security should be treated as fundamental and not optional”. Thus we believe that companies like Mozilla must be able to build the best security for their users that they can provide,to ensure the continuation of trusted communications systems which are key to fostering trust in the internet economy. While we recognise the importance of law enforcement and of protecting public interests in accordance with legal process, there are many ways in which law enforcement can succeed in achieving its goals which do not include weakening encryption or otherwise compromising end-to-end encryption services. As we have made clear on several occasions, including the Apple vs. FBI dispute and the UK’s Investigatory Powers Bill, it is not possible to weaken the security of our products for law enforcement to use against “only the bad guys” (http://ti.me/29eKutu & http://bit.ly/29tdkIW).Creating gaps in security impacts everybody, increasing the risk of malicious hacking and identity theft. We thus strongly caution against the expansion or reinforcement of Art15(1), which could prevent companies from providing some forms of encryption services (such as true end-to-end encryption).

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

We develop & advocate for products, policies and practices that respect users and create trusted online environments and experiences. While supporting the spirit of its intention, we don't agree that mandating a particular technological approach would be to the benefit of the online ecosystem; and may actually have adverse affects undermining, and not improving, user privacy and choice.Enforcing technical solutions via policy approaches goes against the principle of technology neutrality in Art14 of the EPD and related instruments, such as the NIS. In order for legislation to be future proof, especially in the online economy, provisions establishing technological neutrality are key. In the event the EPD is reviewed, this baseline principle should remain in tact.Furthermore, mandating a particular business model, approach, or technical standard is generally not the best way to protect the privacy of users.Providing meaningful means to control their online presence can in many cases prove more effective.Our users are empowered at a technical level through a variety of means including various browser-based tools, such as Firefox's Tracking Protection (which blocks third party trackers by default when in private browsing mode); content & cookie controls; & add-ons developed by third parties. It is central to our mission to provide users with choice, transparency,& control over the way their data is used-based in a technical mechanism that's not dependent on interpretation.

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

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

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

Question 23 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

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

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

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

We encourage all stakeholders to not only comply with, but go beyond, what may be required by law to provide secure and privacy friendly products and services to users. The GDPR already enshrines the concepts of privacy by design and by default, which provides sufficient incentives for companies to consider privacy and data protection; baking it in by default instead of tacking it on as an afterthought.As explained in Qs 1A & 2A, relating to Mozilla’s challenges with complying with the EPD and providing secure and lean data services, we are concerned that further technological specification or more regulation in this area might hinder, and not foster, the development and widespread adoption of more privacy and security focused products and services.Secondly, for those users who are especially privacy conscious, many of these issues can be and are addressed at a technical level through various browser-based tools, such as Firefox’s Tracking Protection, content and cookie controls, or add-ons developed by third parties.Ultimately, there is sufficient technical development and rapid change in the ecosystem such that additional regulation might limit, rather than foster, increased innovation around privacy and security positive tools. For e.g., we believe that tools have had a greater impact in giving users choice around things like third party cookies than the EPD. Additionally, top-down regulation often forces particular business models rather than experimentation & innovation.

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

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

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

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

Due to the restrictive character limits of this online survey, please find attached our full answers to the public consultation. We encourage the Commission to consider this document as our primary filing. We remain at your disposal for any further information or questions.

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

28c9d412-3653-4d63-8319-78369e9b1e06/Mozilla_Submission_E-Privacy_Survey.docx

Background Documents

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

Contact

Regine.MENZIES@ec.europa.eu