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.

30988577529-37

*

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

GSMA

Question III: Please enter your organisation's address:

Park View, 4th Floor, Chaussée d'Etterbeek 180, 1040, Brussels, Belgium

Question IV: Please enter your organisation's website:

www.gsma.com

*

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

Laszlo Toth

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

+32479559087

*

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

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

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

I. REFIT EVALUATION OF THE E-PRIVACY DIRECTIVE

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

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

I.1. EFFECTIVENESS OF THE E-PRIVACY DIRECTIVE

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

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

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

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

Text of 1 to 1500 characters will be accepted

The objective of an equal protection is no longer achieved, since the ePD has not kept pace with an increasingly dynamic digital market. The ePD's current scope does not reflect the converging area of electronic telecommunications where functionally equivalent services are not subject to the same regulatory constraints. Accordingly the ePD is neither technology-agnostic nor provider-agnostic.This has led to the problem that users cannot rely on consistent protection standards across the digital market even when using comparable services. While all electronic communications providers are subject to the current Data Protection Directive, which will soon be replaced by the General Data Protection Regulation (GDPR), traditional telecommunication providers are subject to both the Data Protection Directive/GDPR and additional rules on the protection of personal data, such as rules on location and traffic data.Consequently, the objective of the ePD (see recital 4), an "equal level of protection of personal data and privacy, regardless of the technologies used" has not been achieved.Furthermore, despite having set out some basic principles like confidentiality of communications in a harmonised approach, the ePD was implemented by each Member State with different specific rules which cumulatively have the effect of undermining harmonisation.

-- Response continued under 2A

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

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

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

Text of 1 to 1500 characters will be accepted

Question 1 A continued: One cause for variation between Member States is that the rules are enforced by different types of enforcement authorities which can give rise to different regulatory approaches. Another area of variation, particularly to do with confidentiality of communications, is that Member States have laid down very different conditions in which the content of communications can be lawfully accessed.

Question 2 A: The ePrivacy Directive addresses a number of areas that are substantively different from one another and was implemented differently in each Member State. This has led to a fragmentation of the regulatory landscape across the EU which is burdensome for telecommunications providers and confusing for consumers.
Telecommunications providers specifically encounter problems in regard to the notification of personal data breaches due to inconsistencies between the obligations under Directive 95/46 EC and the obligations set out in Directive 2002/58 EC specified by Regulation 611/2013. While a data breach subject to Directive 2002/58 EC has to be notified within 24 hours in accordance with Art. 2 of Regulation 611/2013, there is no general obligation on businesses to notify data breaches either to DPAs or to the affected data subjects under Directive 95/46 EC. In the meantime, several Member States have passed their own data breach notification duties and the GDPR will soon introduce a 72 hour notification period.
-- Response continued under 4 A

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

Question 2 A continued: The existence of more than one data breach notification regime leads to complexity for telecom operators who are forced to decide which regime they should notify incidents under or to notify under both. As there are no objective reasons to maintain such differences, Art. 4 of the ePD and Regulation 611/2013 should be entirely substituted by the corresponding articles of the GDPR.
Additionally the divided interpretation and implementation of article 6 has led to many questions and concerns. In some Member States traffic data is only permitted to be processed for transmission of communication and for billing purposes. For example processing for fraud prevention would not be allowed even with consent.

Question 4 A:
While shared competences between authorities might seem justified in light of the different nature of some of the provisions of the ePD, it carries with it the inherent risk of ineffective enforcement, e.g. due to conflicting decision making by different authority bodies on the same case.

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

Please see response in the pdf document uploaded with this online form.

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 security obligations of the e-Privacy Directive are at least partially 'consistent' with the other security obligations listed, but they are not 'coherent'. Providers of electronic communications services would be subject to numerous security duties to keep electronic communications secure, so the e-Privacy security duty is redundant and makes little sense. Specifically in comparison to the overarching and horizontally applying provisions of GDPR (which go beyond the requirements of the ePD by introducing safeguards such as encryption and pseudonymisation), it is justified to delete the sector specific provision in the ePD. Art. 32 GDPR already foresees almost identical security obligations in relation to the same scope, the protection of privacy when processing personal data. A dual notification regime of 24 and 72 hours respectively would lead to an unjustified and overly complex situation for telecom providers, stakeholders, authorities and consumers alike.

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

```
Rules regarding opt-in or opt-out from direct marketing communications should
be dealt with horizontally under the Unfair Commercial Practices Directive
and/or GDPR.
```

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

As a consequence of the current outdated EU telecommunications framework, users cannot rely on consistent protection standards across the digital market even when using comparable services. This is especially the case for the provisions of the ePD that only apply sector specific to classic telecoms and thus ignore the converging area of telecommunications, where functionally equivalent services are not subject to the same regulatory constraints. The ePD – in contrast to the GDPR, which applies horizontally – has thus done little to raise users trust in the protection of their data. In consequence, similar services from a functional perspective are still subject to different legal regimes depending on whether they fall under the outdated (technical) categorization of an electronic communications service or not. Due to this asymmetry and non-consistent approach, it is difficult for users to understand which privacy provisions are applicable to the services offered. With the application of the GDPR, a more consistent and horizontal approach will be taken, which leads to a level playing field and thus contributes to raise users trust. Any additional sector specific regulation would thus jeopardize this new harmonized approach towards data privacy.

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

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

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

Text of 1 to 1500 characters will be accepted

It is difficult to quantify the additional costs directly related to the measures included in a single legal instrument as data protection related implementation stems from different legal sources. Although precise costs are not available, it is well recognized that the costs of compliance with multiple and overlapping regulatory paradigms places a financial burden on service providers. By making it far more difficult for ISPs to do what edge providers such as Over-the-Top service providers and Operating System developers do —use non-sensitive customer data to engage in socially productive first and third-party marketing—the rules would reduce the profitability of broadband services, exert upward pressure on broadband prices, and depress incentives for broadband deployment. Thus, it is critical for the ePD to align with the GDPR in a way that facilitates the efficient growth of the DSM ecosystem to achieve the economic and social benefits that DSM can bring to consumers.

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

The costs of compliance are not proportionate in so far as the rules do not achieve the goal of ensuring confidentiality of communication to all consumers. As it is applied only to telco providers and not to other players supplying similar services, the consumer is not protected in an equal measure and telco operators have been put at a competitive disadvantage compared to other players offering similar services. This is even more unreasonable when considering the convergence and bundling of different services that allow communication.
The review should make sure that rules are proportionate, necessary and fit for purpose for the services of today and tomorrow. The answer here may lie in best practice or GDPR guidance, not more law.

I.5. EU ADDED VALUE OF THE ERIVACY DIRECTIVE

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

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

- ○ Yes
- ◉ No
- ○ No opinion

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

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

II. REVISING THE E-PRIVACY DIRECTIVE: LOOKING AHEAD

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

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

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

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

- ( ) Yes
- ( ) No
- (•) Other

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

Text of 1 to 1500 characters will be accepted

A harmonised approach across the EU is preferable and will help to establish a 'Digital Single Market'. The review should focus on GDPR which is a directly applicable instrument. Sector-specific legislation like the ePD is therefore not the right tool to tackle privacy related issues in a harmonised and technology neutral approach towards all industries. Only in the unexpected case that provisions are still deemed relevant and necessary to be implemented in a specific ePrivacy instrument, should such rules be provided in the form of a Regulation and apply to all market players. This would guarantee a more harmonized approach at Member State level as well as coherence with the GDPR.

II.1. REVIEW OF THE SCOPE

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

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

- (●) Yes
- ( ) In part
- ( ) Do not know
- ( ) Not at all

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

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

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

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

II.2. ENSURING SECURITY AND CONFIDENTIALITY OF COMMUNICATIONS

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

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

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

- ○ Yes
- ◉ No
- ○ Do not know

Question 20 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Encryption and other security measures are very important tools to protect the confidentiality of communications, but they are only tools. Prescriptive rules focused on particular technologies or sectors risk failing to keep pace with rapid technological and societal change. Mandating specific security tools as legal rights risks prematurely dating any new legislation. Instead, laws should be principles-based and as regards the security of electronic communications, organisations are already subject to comprehensive and adequate security obligations that can be enforced by regulatory authorities.

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

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
- ☑ Others

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

There is no need for a specific ePD instrument. Key factors to facilitate users' ability to consent without disrupting the Internet experience are inter alia requiring manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings as well as to mandate European Standards Organisations to produce standards and the support of self-co regulation. These instruments are already covered by the GDPR. According to Article 25 GDPR, the future manufacturers of terminal equipment including operating systems and browsers will be obliged to meet principles of data protection by design and by default. While this is the case for manufactures producing both terminal equipment and operation systems, manufactures who only produce operation systems nevertheless have to take care that the respective terminal equipment produced by third parties enables them to meet the obligations set out by the GDPR.
Furthermore regarding the setting of standards and the self-co regulation the GDPR provides the possibility to draw up codes of conducts for the purpose of specifying the application of the regulation as well as to establish certification mechanisms in order e.g. to demonstrate compliance with obligations of data protection by design and by default.

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

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

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

Question 25 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

In the GSMA's opinion, risks to consumers from use of traffic and location data can be adequately dealt with under the GDPR and do not need to be addressed in a separate and sector specific piece of legislation. The GDPR horizontally provides for a significantly higher level of protection for the processing of personal data than the former Directive. It equips consumers with improved rights and imposes upon controllers and processors to carefully evaluate the risks for individuals when processing personal data (see the new impact assessment obligations in GDPR), including for other purposes (see newly introduced compatibility criteria for further processing), while considerably increasing user privacy through the introduction of safeguards like pseudonymisation and encryption. The stricter requirements for the processing of traffic and location data are therefore not anymore justified and should consequently be deleted.

To the extent that that traffic and location data are regulated outside of GDPR (whether in relation to legal persons or natural persons), the exemptions to consent should be extended to the legal grounds provided by the GDPR (Art. 6) when processing personal data, including the possibility of pseudonymisation for further processing. It should further be taken into account that the processing of traffic and location data can help protecting communications from the threat of malware and viruses.

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

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

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

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

Question 26 A: Please specify, if needed.

Text of 1 to 1500 characters will be accepted

These provisions refer more to consumer protection principles than to privacy principles. The first three items can be offered to subscribers on commercial basis to if demanded and the fourth may no longer be needed. If they are deemed important enough to deserve protection in law, GSMA would propose that these be moved to to the currently updated new framework covering communications a broader range of services.

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

```
Rules regarding opt-in or opt-out from direct marketing communications should
be dealt with horizontally under the Unfair Commercial Practices Directive
and/or GDPR.
```

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

In our view each element of the ePD is either already covered or should be dealt with elsewhere in horizontal legislation. The competent authority would therefore be determined by where the rule is addressed, for example, under data protection, telecom or consumer protection legislation.
The enforcement mechanism of the ePD has led to a fragmented approach and a considerable level of confusion and uncertainty both for providers and citizens alike. While shared competences might seem justified in light of the different nature of some of the provisions of the ePD, it implies risks of ineffective enforcement, e.g. due to conflicting decision making by different authority bodies on the same case. To avoid overlapping rules with the GDPR, which already provides a proper enforcement mechanism, additional sector specific legislation is no longer justified.
If, and only if, a separate legal privacy instrument would still be considered necessary, then a more harmonized and less intrusive approach should be taken, by having solely one competent body as the responsible authority in place. This would avoid divergent decisions and foster a more consistent and harmonized enforcement of ePD rules.

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

[GENERAL] The ePrivacy Directive should be repealed, because the rules should either be: covered in the Telecom Framework (e,g: confidentiality of communications, definitiions), dealt with in consumer protection rules (e.g: calling line identification, itemised billing, automatic call forwarding, inclusion in directory) or redundant because they are already covered elsewhere, in particular, in the GDPR.

- Security is already comprehensively and adequately covered in GDPR, Framework Directive, Radio Equipment Directive and NIS. Additional requirements are therefore not necessary.
- Data breach notification is covered by GDPR.
- GDPR would also cover lawful use of location and traffic data which is increasingly important for innovation and growth in the context of the Digital Single Market

[QUESTION 19 – Types of Network] All types of network listed whether public, private, closed or non-commercial WIFI) should apply a level of security that is appropriate to the circumstances. A general standard such as provided in the GDPR is effective as it forces organisations to consider the risks, but allows them to decide precisely which measures are appropriate to protect the communications and data.

[QUESTION 21 – Security] Security is already comprehensively and adequately covered in GDPR, Framework Directive, Radio Equipment Directive and NIS. Additional requirements are therefore not necessary. It should be noted that even without explicit duties in law, there exists for organisations an inherent commercial and/or reputational imperative to keep their customers communications and data safe.

[QUESTION 32 – Fines] In our view each element of the ePD is either already covered or should be dealt with elsewhere in horizontal legislation. The competent authority and their corresponding powers would therefore be determined by where the rule is addressed, for example, under data protection, telecom or consumer protection legislation. If there is a successor piece of legislation to the ePD the aim should be to apply a sanction regime that is proportionate to the risks implied by the remaining content of such future instrument. It would therefore not be appropriate to allow the equivalent provisions of the GDPR to apply.

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

facbbd36-cfdc-4a9a-aa8d-c9a6532f789c/GSMA_Full_response_to_Question_6A.pdf

Background Documents

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

Contact

Regine.MENZIES@ec.europa.eu