Contribution ID: 75f8eabb-f06d-4e80-bbcf-824a1e711ebc
Date: 05/07/2016 23:29:37

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

Fields marked with * are mandatory.

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

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

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

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

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

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

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

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

[1] http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884.

* **PRIVACY STATEMENT**

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

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

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

Specific privacy statement e-Privacy

Specific_20privacy_20statement_ePrivacy.pdf

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

Background document

05_2004_20Background_20document.pdf

GENERAL INFORMATION

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

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

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

685809321315-95

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

IT-Political Association of Denmark

Question III: Please enter your organisation's address:

Question IV: Please enter your organisation's website:

https://www.itpol.dk

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

Jesper Lund

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

+4529727719

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

jesper@itpol.dk

* 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

In general, the e-Privacy Directive (ePD) has managed to protect the confidentiality of communications for traditional providers of public communication services, that is telephone and internet service providers. European citizens are fortunately not coerced into accepting private surveillance of their communication or profiling of their social graph (contacts) when they sign up for an internet access service or a mobile telephony subscription (with a few exceptions, such as Phorm in the UK, where an ISP spied in its customers internet traffic). However, increasingly the communication is moving to other providers ("OTT"), where this protection is not legally ensured, and where citizens may indeed be coerced into accepting surveillance or tracking in order to communicate with their friends. It is unacceptable that the fundamental right to privacy for Europeans depends on whether a text message is delivered via e.g. SMS (legally protected) or some social media service (where users are often coerced into giving consent for processing that goes beyond what is strictly necessary to deliver the message from sender to recipient). Moreover, the cookie provisions of Article 5(3), which were strengthened in 2009 to further protect citizens against commercial surveillance, have largely failed their objective. The content industry has adopted "privacy" policies, where consent is essentially coerced based on information about the purpose of the cookies that is often completely inaccurate.

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

IT-Political Association of Denmark (hereafter: IT-Pol Denmark) has worked on a case, where call detail records used for itemised billing were stored for more than 10 years. After a complaint to the national regulator, some of the data was deleted, and the mobile provider changed its policies. However, the national regulator (the Danish Business Administration) did not issue specific guidance on how long call records can be stored, only that it cannot be 10 years. So it is currently unclear whether the data can be stored for 5 years (the retention period in the Danish law on bookkeeping information), 3 years (the statutory limit on simple financial claims in Denmark), or a shorter period corresponding to when the charge for a specific phone call can no longer be disputed in practice. There is a need for more specific rules than the current article 6(2) of the ePD to protect the privacy of citizens since, at least in Denmark, call records can be stored for up to five years under the Danish transposition of the current directive. Discussions with digital rights organisations in other EU MS have revealed similar problems of lack of clarity for storage periods for call detail records (for itemised billing).

See http://history.edri.org/edrigram/number11.9/danish-phone-company-keeps-data-10-years

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

In some MS, provisions relating to privacy and data protection under the ePD are enforced by regulators which do not have proper expertise and focus in this area, for example the telecom regulator. This is the case in Denmark.

The cookie provisions are not properly enforced in Denmark. IT-Pol Denmark has been told that the regulator has tacitly accepted that only some information about cookies should be given to users (essentially the 2002 version of the ePD), but not that prior consent should be required before storing or gaining access to information in users' terminal equipment.

Location tracking based on WiFI MAC addresses is a new area which some MS have recognised falls under Article 5(3) of the ePD. But there have been divergent interpretations of the rules in the EU. In Sweden and the Netherlands, the regulator (the DPA) has decided that citizens cannot be geotracked based on the WiFi MAC address without prior consent. This case is interesting because prior consent (at least explicit consent) is impossible to obtain in practice for WiFi tracking. The Danish regulator, on the other hand, has ruled that tracking without consent is allowed in some situations (see EDRi-gram article below), but this decision really raises more questions than it answers, and creates legal uncertainty. Most likely, WiFi-based location tracking is used in many places throughout the EU because it is impossible to detect.

See https://edri.org/wifi-tracking-eprivacy-directive-denmark/

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

Specific rules on confidentiality of electronic communications are important because citizens' fundamental right to privacy and data protection (articles 7+8 in the CFR) cannot be fully protected by the principles of the GDPR. Predominantly, the GDPR, like the current Data Protection Directive 95/46, relies on consent as the legal basis for processing. In the context of electronic communication, the personal data and the content of the electronic communication refer to at least two persons, namely the parties in the communication. If a citizen is giving his/her email provider consent to scan the contents of the email communication, part of that consent is really given on behalf of others (should which not be allowed). Sometimes it is even mentioned in privacy policies that the data subject should get consent from the other parties in the communication, which is completely meaningless and only serves as pure liability shifting.

Secondly, the ePD ensures that extra services for traffic data and location data, which are not needed to deliver the communication, are treated as value-added services, which means that the user can refuse consent to these services without losing access to the communication service. For communication services like Facebook, the user is faced with a "take it or leave it" choice. In order to communicate with their friends on Facebook, citizens must accept surveillance and tracking, none of which is necessary for delivering the communication service.

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 ePD deals with a subset of services where the need for technical solutions, rather than consent to processing, is more urgent than in the GDPR in general, and where technical solutions that enforce privacy without the need for consent in the first place are easier to implement (genuine "privacy by design" solutions that do not rely on "big data" post-anonymisation of personal data).

There are also cases within the scope of the ePD where consent to processing in a GDPR-sense cannot realistically be obtained. An example is geolocation tracking based on WiFi MAC addresses, which is used in many smart city projects for legitimate public policy reasons (traffic planning, for example) and (often much less visibly) in commercial applications, such as in-store tracking of retail customers.

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

There is no awareness in Denmark that the objective of the ePD is to protect the privacy of citizens when using electronic communication networks.

The implementation and enforcement of the cookie provisions have clearly failed to raise users' trust in the protection of their personal data (online behavioral data). The cookie provision have raised user awareness of tracking on the internet, but the implementation of the rules makes users completely powerless because they can rarely object to the tracking and surveillance. So users have their privacy violated as much as before the 2009 revision of the ePD, perhaps with greater knowledge of this happening, and on top of that they are frustrated by cookie popups and consent statements that are often written in a way that makes it impossible to understand them.

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

We have answered "no opinion" mainly because we have no knowledge of the actual costs. However, confidentiality of communication is a fundamental right for European citizens, and protecting that right should not be limited to situations where it can be done at sufficiently low cost.

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 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

We answered "do not know" because we do not fully understand the question. Individuals currently have the right to secure their WiFi, use encryption and select passwords of their choice. Technologies for all of these things exist, often via free software that everybody can use, and there is no ban on encryption or unguessable passwords. If question 20A is intended to be about law enforcement needs and limitations of the right to privacy (which is not absolute, of course), further information is needed before we can answer the question. We can say, however, that we are opposed to mandatory encryption backdoors. Citizens should be free to use encryption and companies should be free to offer communication services based on end-to-end encryption, in both cases without backdoor requirements. This may, in certain situations, affect legitimate law enforcement needs, but if a communication service is based on properly implemented end-to-end encryption, there is no technical way to interfere with the right to privacy only for some citizens in a targeted way. A mandatory (or voluntary for that matter) encryption backdoor will endanger the confidentiality of communications for every user/citizen, not just those citizens where the right to privacy may legitimately be restricted because there is a valid suspicion of criminality.

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

It is very rare for citizens to have real choice whether to allow cookies /tracking or not. If citizens want to ensure their fundamental right to privacy, they really have to stop using the internet. The most technically proficient may be able to ensure their privacy through technical means, such as ad/tracker blocking. But privacy should not be a right limited to the 1% most technically proficient citizens, and having disconnection from the internet as the only alternative to accepting surveillance and tracking is utterly unacceptable.

For public-sector websites, the policy choice is very easy. Tracking should simply not be allowed, and denying citizens access if they do not accept tracking is unacceptable.

For private information society services, we recognise that tracking (or rather the advertising that is supported through tracking) is viewed as essential for securing revenues in many cases. Mandating that every information society service implements a subscription model as an alternative to "paying with behavioural data" would be excessive, but currently it does not seem that competition alone can ensure sufficient privacy-friendly services for European citizens. A reasonably compromise would be to impose this subscription mandate on larger services with many users, for example large communication services and online news services that are essential to exercising other fundamental rights (freedom of expression, freedom of information, and media pluralism).

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

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

Our choices (not wanting to be asked about consent) are based on the following assumptions and interpretations of the questions:
* Website analytics is either done by the information society service locally on its own web server, or via a clear data processing agreement with a data processor as 3rd party (not some hybrid like Google Analytics, where it is totally unclear whether Google is processor or controller for the analytics data collected)
* Immediately anonymised must specifically rule out that two website visits can be linked technically. Something like pseudonymisation, which would allow for linkability, is not sufficient.

Whether the cookie is first party or third party is not sufficient to determine whether a third party is involved in the processing and potential tracking. Google Analytics, one of the most privacy invasive tracking methods on the internet, is based on first-party cookies. These are not technically accessible by Google servers because of the same-origin policy enforced by web browsers, but websites using Google Analytics contain scripts which accesses the cookies and submits the contents to Google via webbug elements, where the cookie information is appended as URL parameters. Google Analytics is not the only tracking service to use this strategy with first-party cookies

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

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

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Requiring manufacturers of terminal equipment to design privacy protection into their products is a good idea. However, it should not be used to put the sole responsibility on avoiding tracking on the citizens. This is more or less the de facto situation today, where it is next to impossible to legally deny consent to tracking with cookies. The technically most proficient citizens turn to technical solutions like the ones listed above, but this is a cat-and-mouse game with the information society service industry that employs clever people to constantly develop new methods of tracking, for example device fingerprinting instead of cookies.

Blocking third party cookies and blocking tracking script in the client device (e.g. web browser) is a really good idea, but it's simply not enough. Most recently we have seen information society services that check (often without information and asking for consent) whether their tracking is blocked by the user and, if so, refuses access to the service.

The legal framework to ensure privacy and confidentiality of communication must do more than simply shift the burden to citizens and manufacturers of terminal equipment.

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

Important clarification to our answer for the third option: Our definition of "fully anonymised" assumes that two location measurements for the same user (citizen) cannot technically be linked under no circumstances, that is genuine privacy by design. If anonymisation is defined as post-anonymisation in a traditional "big data" sense after the citizen has been tracked for some period, we do NOT support broadening the exemptions. Post-anonymisation in big data projects involve processing personal data and tracking until some point where the data is anonymised. This creates substantial risks for citizens if data are somehow leaked before anonymisation is done, and often there are serious questions about whether the anonymisation is effective (AOL search data leak, for example).

The clear advantage of NOT broadening the exemptions is that service providers will be forced to develop other technological solutions for location data. The only place, where two location measurements can be linked for some purpose and then anonymised, is in the terminal equipment of the end-user. This simply cannot be done credibly on a central server. For example, rather than having smart city projects that track citizens for traffic planning purposes and then "promise" to anonymise the location data, the EU should promote technical solutions where the traffic measurements (e.g. time to travel from A to B) are made in the users' devices and is anonymised there before being submitted to a server.

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

Opt-out puts the burden of stopping the marketing communication on citizens. Often they will continue to receive and then delete the marketing communication because exercising the opt-out takes too much time, and sometimes it's not obvious what to do. This is simply not reasonable. Senders of direct marketing communication should ensure prior consent and face sanctions if prior consent it not obtained before sending out marketing communication.

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

Data Protection Authorities have the expertise in protecting privacy and data protection and recognising these as fundamental rights of citizens under the Charter.

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

- (●) Yes
- ( ) No
- ( ) Do not know

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

- (●) Yes
- ( ) No
- ( ) Do not know

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

Text of 1 to 3000 characters will be accepted

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

Background Documents

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

Contact

Regine.MENZIES@ec.europa.eu