Questionnaire for the Public Consultation on the Evaluation and Review Of The E-Privacy Directive (En)

Questionnaire For The Public Consultation On The Evaluation And Review Of The E-Privacy Directive

New Section

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.

(X) 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.

NB: Please select only one answer, unless stated differently.

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).

(X) Yes

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

(X) Trade association

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

(X) United Kingdom

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.

The ePrivacy Directive included different provisions and while some have been successful in meeting the ePrivacy Directive's objectives, others have not. Each of the various provisions of the Directive must be assessed independently.

In the UK the cookie rules have had detrimental effects on the user experience as regular visitors to a website are asked every time they visit the same website, if they consent to the use of cookies. This can be frustrating for consumers and detracts from the user experience.

The ePrivacy Directive for the most part relies on an opt-in consent for marketing communications. This over reliance on opt-in consent makes it incompatible with sections of the GDPR, in particular with Article 6 Nr.1 (f) and Article 6 Nr. 4.

The ePrivacy Directive was introduced after Directive 95/46 and so introduced new rules for online identifiers such as cookies, which were not covered by previous legislation. The GDPR fully includes within its scope this kind of processing, as explicitly mentioned in recital 30. Consequently, the DMA believes that there is no purpose for this provision to remain within the ePrivacy Directive.

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.

Specific provisions for confidentiality of communication, such as article 5.3, requiring consent for storing of information or gaining access to information already stored, in the terminal equipment of a subscriber has seen inconsistently interpreted, leading to difficulties of implementation. The various interpretations of a same provision has created huge uncertainty among the numerous organisations which have to implement it, as well as important implementation costs. Furthermore, the various interpretations developed at national level are in direct contradiction with the very nature of online communication, which is by definition without border. Finally, the practical implementation of the provision 5.3 has led to disruption of user online experience.

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.

The ePrivacy Directive has had a divergent implementation across the EU. Different member states have interpreted different provisions in varied ways, for example, article 5.3. The problem has been made worse by the plethora of regulator guidance around the EU. The lack of harmonisation has led to particular difficulties in an online context, where the distinction between the borders of member states and different jurisdictions is not apparent.

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.

The GDPR was created with the technological developments in the online world in mind, including data processing in the electronic communications sector. Many of the objectives of the ePrivacy Directive are met by the GDPR. For example, the GDPR contains detailed rules for the notification of personal data breaches. The review of the ePrivacy Directive should assess the provisions of the Directive which are no longer relevant and can be removed, as they are covered by the GDPR.

In the DMA's views, storage and access to a terminal's equipment, are both already covered by the rules of the GDPR, as online identifiers are clearly mentioned in the definition of personal data and recital 30 makes clear that activities related to online identifiers, such as IP addresses and cookies are included within the scope of the GDPR. Consequently, the DMA believes that this provision should be repealed from the ePrivacy Directive to ensure that the protection and flexibility developed by the GDPR fully applies to this processing.

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.

The GDPR takes a risk based approach regarding security which requires data controller and processors to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk", while taking into consideration a number of criteria, such as the cost of implementation. In this case, the DMA believes that the GDPR includes provisions on security which, while being in line with the security requirements set up by the ePrivacy Directive, goes further, by detailing some of the tools that could be used to ensure security, and by providing some guidance for assessing the appropriate level of security needed. Equally, the GDPR provides

for detailed rules on breach notification which are the result of intense negotiations with the objective of ensuring the right level of protection. In the DMA's view, the provisions on security of the ePrivacy Directive are not necessary anymore as the GDPR provides for an equivalent, or higher level of protection.

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?

(X) Yes

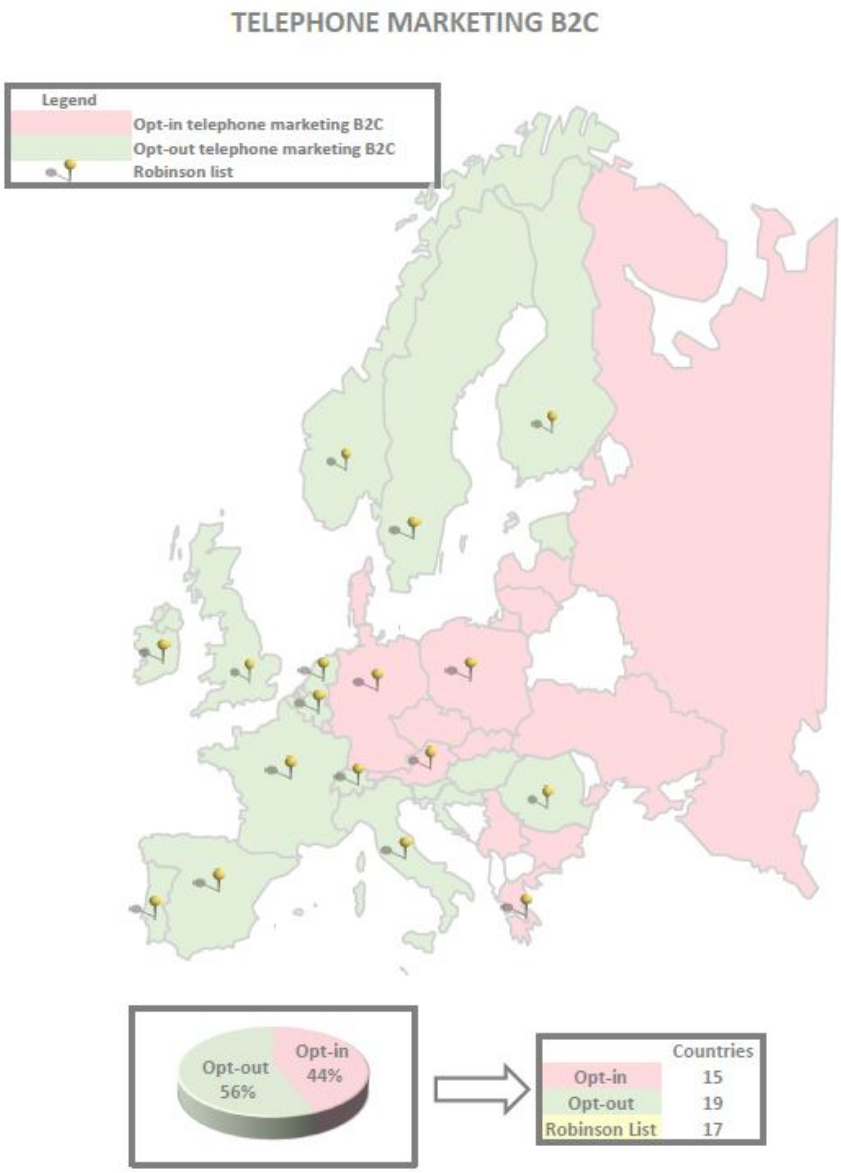
( ) No

( ) No opinion

Question 8 A: Please specify your reply if needed.

The UK operates an opt-out model, which both organisations and consumers are familiar with. The Telephone Preference Service (TPS) is a condition of the opt-out model in the UK. Consumers are able to register their phone number with the TPS and opt-out of unsolicited telemarketing. Organisations screen their data sets against the TPS data to ensure that no phone numbers registered to the TPS are called. This is an effective model of regulation as Ofcom research revealed in July 2014. Signing up to the free service reduces the number of unsolicited live marketing or sales calls consumers receive by around a third.

The DMA believes that the different national preferences should be maintained as there are different cultural expectations in different EU countries. Furthermore, telemarketing is, broadly speaking, a local issue as a result of language. Across the EU consumers expect to receive a call from a telemarketer speaking their native language restricting telemarketing to national boundaries. There are a few exceptions where different nations share languages such as, the UK and India, of German speaking nations such as, Switzerland, Germany and Austria.



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
- **(X) Moderately**
- Little
- Not at all
- Do not know

Question 10 A: Please specify your reply if needed.

The main problem is rogue companies that ignore the law to make telemarketing calls. In the UK it has been PPI and accident claims callers that have driven complaints. These companies break the law and whether the rules were opt-in or not the rogue traders would ignore them. There must be a differentiation between the legitimate telemarketers and those who flout the law. A move to opt-in consent will not, in the UK, stop rogue telemarketers, which is the source of complaints to the Information Commissioner's Office (ICO) and the TPS.

However, the information requirement set up by article 5.3, and which is also covered by the GDPR, has generated some trust, by providing more information to internet users. The Pan European Self-regulatory programme on online behavioural advertising (OBA) developed by the industry provides alternative mechanism to provide in a less intrusive way information and control to the user about OBA. Using an icon on which the individuals can click for more information and access the control tool, this programme contribute to individual's awareness about OBA.

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

- Significantly
- Moderately
- Little
- Not at all

(X) Do not know

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

No reliable available statistics for cost of implementation for one-to-one marketing in the UK.

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
(X) No
( ) No opinion

Question 12 A: Please specify your reply if needed.

The DMA believes that the GDPR is sufficient to protect consumer's fundamental right to privacy. Therefore, the provisions in the ePrivacy Directive can be seen as onerous as they are an extra layer of rules for organisations to comply with.

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
(X) No
( ) No opinion

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

(X) Other

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

The GDPR has been adopted as a regulation, with the objective of ensuring harmonisation of data protection in Europe. As already commented, the DMA believes that most of the objectives of the ePrivacy Directive are already covered and, in some cases, increased in the GDPR. The review of the ePrivacy Directive should assess the provisions of the directive which are no longer relevant as they are already fully covered in the GDPR and repeal them in order to avoid double legislation as well as the risk of divergent legislation. In many cases, individual's right to privacy is already fully protected under the GDPR, which found a delicate balance between data protection and free flow of data. The review of the ePrivacy Directive should be the occasion to remove provisions which are already covered in the GDPR, thus ensuring that harmonized rules can be applied in all sectors.

However, some provisions of the Directive should be left as they currently are, maintaining the flexibility afforded to member states while ensuring equivalent protection. In the DMA's view the flexibility given by the ePrivacy Directive to member states to decide between opt-in and opt-out

solutions for telemarketing has led to a regime that both the industry and individuals have become familiar with. While greater harmonization is important, it should not lead to the restriction of marketing practices which are commonly accepted at national level and are sufficiently protective of the individual.

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

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 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.

The DMA would like to highlight that individuals always remain free to visit a private website or not. Individuals always keep the ability to make a choice between visiting a website or another. Denying access to users who refuse to accept cookies on a specific website does not deprive individuals of this choice to visit another website. However, it ensures that individuals who do not wish to pay with money can still access content, by ensuring the sustainability of the business model of the publisher. This argument, however, should not apply to website from the public service, or providing for a public task.

Marketing and advertising directly fund publishers online and ensure the development of media pluralism, and entertainment content. As mentioned above, the demand for paid for services from the market has triggered the development of such business model, and individuals should keep the real choice of having to choose between sustainable advertising funded websites and paid for websites, without obliging websites owner to engage in providing paid for services they do not wish to develop.

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.

The DMA believes that consumers want to receive information about the collection of data taking place while online, as well as information about the opportunity to object to such collection when such data can have an impact on their privacy. Information and control are two important pillars of the GDPR. The GDPR has increased the number of information obligations to provide to the individuals, while encouraging organisations to provide such information in an easy and understandable format. The GDPR also puts a strong emphasize on the right to object, and other tools for the individuals to control his data (consent withdrawal, right to erasure, right to object to profiling). Consequently, the GDPR provides sufficient protection for the collection of personal data, regardless of the context in which it takes place, while providing the data controller with the necessary flexibility to process data.

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.

The DMA Code is an exemplary example of industry self-regulation and holds DMA members to a high and ethical direct marketing standard. The DMA Code is an aspirational agreement to which all DMA members and their business partners must adhere. It is principles based and the five principles are; put your customer first, respect privacy, be honest and fair, be diligent with data and take responsibility. The DMA Code is supported by channel specific guides that delve into the technical details of running a best practice marketing campaign. Self-regulatory models are reactive and flexible, which means they are able to respond to our ever changing and disruptive market place.

The industry has also developed guidance regarding other provisions of the ePrivacy Directive such as the so-called email soft opt-in (article 13.2) and telemarketing (article 13.3). Industry self-regulation also developed tools for individual to express their preference regarding telemarketing, with the many existing Robinson lists such as, the TPS in the UK. The recognition and active promotion of such tools is, in the DMA's view, the best way to reach greater consistency while maintaining the national level status quo which exist for article 13.3 and 13.5).

Link to DMA Code: http://dma.org.uk/the-dma-code

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.

The one-to-one marketing industry uses many different channels of communication from the most traditional such as fax and telemarketing to the most modern such as social media. Each channel is a different way to communicate and interact with customers and potential customers and each channel has its own specificities. Marketers will use different channels for different audience, different strategies and at different costs. Furthermore, from a privacy point of view, each channel is not perceived in the same way by individuals. The E-Privacy Directive requires a prior consent (opt-in) for email marketing and SMS/MMS marketing, but leaves other form of marketing, mainly telemarketing, to member states to legislate on, with either an opt out or an opt in requirement. As the assessment study writes “As they are relatively more costly for direct marketers, member states are free to choose an opt-in or opt-out consent regime. Some member states have chosen opt-in, and others opt-out.”

For further information refer to the answer to question 8A.

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

(X) Do not know

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

(X) 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

(X) 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.

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

DMA Code: http://dma.org.uk/the-dma-code

FEDMA Code of Conduct:
http://www.fedma.org/fileadmin/documents/SelfReg_Codex/FEDMACodeEN.pdf

DMA research 'Data Privacy: what the consumer really thinks' June 2015
http://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf

Zach Thornton

External Affairs Manager

Direct Marketing Association UK Ltd