European Commission

SYNOPSIS REPORT OF THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE EPRIVACY DIRECTIVE

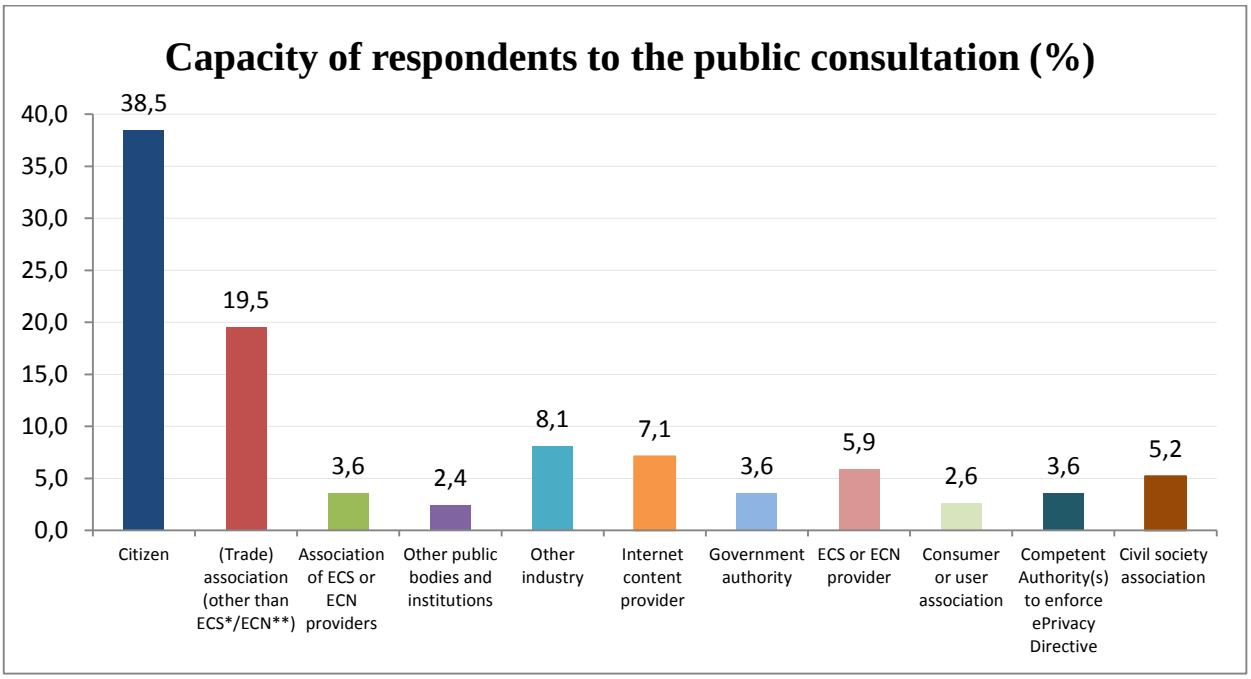
Digital Single Market

SYNOPSIS REPORT OF THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE EPRIVACY DIRECTIVE

The public consultation on the review of the ePrivacy Directive[1] ran from 12 April to 5 July 2016. The questions gathered input on: (1) the evaluation of the ePrivacy Directive; (2) the possible solutions for its revision. The results of the consultation will feed into the REFIT Evaluation (Regulatory Fitness and Performance Programme) and Impact Assessment Staff Working Documents in preparation of a legislative proposal.

OVERVIEW OF RESPONDENTS

The consultation received **421** replies from stakeholders in all Member States and outside the EU. The largest number came from Germany (25.9%), UK (14.3%), Belgium (10%) and France (7.1%). The Commission received **162** replies from citizens; **186** contributions from industry actors such as electronic communications, network providers, Internet content providers, trade associations and others; **40** replies from public authorities including competent authorities which enforce the ePrivacy Directive at national level; **33** contributions from consumer and civil society associations.



This report categorises the responses into the following groups:

- **Citizens, consumer and civil society organisations**: citizens' answers were compared to those of civil society and consumer associations. As their positions did not differ, these categories are grouped together and referred to as "citizens, consumer and civil society organisations";
- **Public authorities**: government authorities, competent authorities enforcing the ePrivacy Directive, other public bodies and institutions;

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

- **Industry**: trade associations of electronic communication service ("**ECS**") or electronic communication network ("**ECN**") providers, ECS or ECN providers; trade association other than ECS/ECN, Internet content providers e.g. publishers, providers of digital platforms and service aggregators, broadcasters, advertisers, ad network providers, other industry. The position of ECS/ECN was compared to the other industries'. The report indicates where the positions differ.

As questions were optional, the percentages in the report refer to the amount of respondent per group that answered the particular question.

The contributions of stakeholders who consented to publication are available online.

This analysis does not represent the official position of the Commission and its services, and does not bind the Commission in any way.

I. REFIT EVALUATION OF THE EPRIVACY DIRECTIVE

I.1. EFFECTIVENESS OF THE EPRIVACY DIRECTIVE

The first part of the questionnaire sought to assess whether the objectives of the ePrivacy Directive have been achieved.

The majority of citizens, consumer and civil society organisations (76.2%) do not think that the ePrivacy Directive has achieved the objective of ensuring full protection of privacy and confidentiality of communications across the EU, or has done so to a small extent. 58.3% of the ECN/ECS industry agrees with this statement while the industry at large (57.4%) thinks this objective has been achieved to a significant or moderate extent.

The most frequently cited reasons for this assessment are the following:

- The ePrivacy Directive has a limited scope of application since most of its rules do not apply to over-the-top services ("**OTTs**")[2];
- The principle of confidentiality should be included in an overarching, horizontal legal instrument instead of a sector specific one;
- Some of the rules allow for divergent national interpretation;
- The rule on cookies does not result in adequate protection for consumers: consumers are not offered a real choice to accept cookies and some new tracking applications are not captured;
- The ePrivacy Directive has been enforced in a fragmented manner.

Both categories of citizens, consumers and civil society organisations and industry are internally divided on the question whether the objectives of ensuring the free movement of personal data, equipment and services in the EU have been achieved.

42.3% of citizens, consumers and civil society organisations believe the objective has been achieved for the free movement of personal data. 36.3% do not believe that (or only to a little extent); the other respondents have no opinion (21.4%). The proportions are relatively similar on the free movement of equipment with 45.3% stating that the objective has been met and 30.9% disagreeing.

[2] E.g. Voice over IP, instant messaging, web mail services.

48.7% of industry representatives said that the objectives have been met for the free movement of personal data, while 37% disagree. For the free movement of equipment and services, 41.6% responded that the objective has been met while 26.2% disagree. On the question on the free movement of equipment around one third responded that they did not know.

The most frequently quoted reasons relate to differences in implementation (especially on cookies), hence high compliance costs, unfair competition between those subject to the rules and those that are not and divergent enforcement at national level.

Public authorities are more positive. The majority assesses that the Directive has significantly or moderately achieved its objectives in all areas: 74% for confidentiality, 68% for free movement of data; 62.5% for free movement of equipment and services.

I.1.1. MOST PROBLEMATIC RULES

- **Citizens, consumer and civil society organisations** report that most difficulties stem from the application/understanding of the rules on:
    - unsolicited commercial communications (unclear application to non ECS, unclear mix of opt-in and opt-out system, 'spam continues');
    - confidentiality of electronic communications (unclear scope, OTT services are not covered, general distrust);
    - traffic and location data (unclear application of rules when data is both location and traffic data, scope only covers ECS whereas data is generated by apps and services which are not ECS);
    - notification of data breaches (ePrivacy Directive and General Data Protection Regulation ("**GDPR**")[3] are not aligned, different competent authorities).

- **Industry** reports most difficulties with the rules on:
    - confidentiality of communications (unclear scope of application; rules on cookies cause a disrupted Internet experience for users and are costly for businesses due to divergent interpretations throughout the Member States);
    - traffic and location data (overlap with the GDPR; even with consent of users, ECN/ECS industry cannot extract value from this type of data in the same way as operators not subject to the rules of the ePrivacy Directive; the rules hinder innovation and cause fragmented national implementation);
    - unsolicited commercial communications (fragmented situation at national level).

- More specifically, **ECS/ECN providers** report most difficulties with the rules on:

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

- traffic and location data (overlap with the GDPR, call for same rules as applicable to OTTs, rules are too strict and hamper new business models);
- notification of data breaches (inconsistent rules with the GDPR, lack of uniform interpretation across the EU);
- and confidentiality of communications (scope of application).

- **Public authorities** report most difficulties with the rules on

  - processing of location and traffic data (unclear definitions, overlaps between both types of data);
  - unsolicited commercial communications (definition of direct marketing is controversial, unclear relationship with Electronic Commerce Directive).

I.1.2. DIFFICULTIES LINKED TO DIFFERENT ENFORCEMENT AUTHORITIES

Citizens, consumer and civil society organisations and industry agree that divergent interpretation of the rules is due to Member States giving enforcement powers to several authorities. However, a relevant percentage of public authorities hold different views.

The majority of citizens, consumer and civil society organisations believe that the significantly or moderately divergent interpretation of the rules in the EU (64.4%) and non-effective enforcement (61.9%) is due to some Member States allocating enforcement powers to several authorities. Of those that have reported significant and moderate problems, the main source of confusion is for citizens, the providers themselves, followed by the competent authorities.

Industry also believes that the allocation of enforcement powers to several authorities has caused divergent interpretation (65.4%) but is more divided on the effectiveness of enforcement, with 41.3% believing that this has significantly or moderately caused non-effective enforcement. Industry notes that companies are the main party affected by the situation, followed by citizens and the authorities. A larger majority of ECN/ECS believes that attribution of enforcement powers to several authorities has caused divergent interpretation (83%) and non-effective enforcement (63.8%).

Public authorities are more optimistic: 36.3% believe that the allocation of enforcement powers to several authorities has caused divergent interpretations, 47.8% consider that it has caused non-effective enforcement to a significant or moderate extent. This category believes that it is a source of confusion mostly for citizens, followed by industry.

I.2. RELEVANCE OF THE ePRIVACY DIRECTIVE

Given the recent adoption of the GDPR, the questions sought to assess the relevance of the objectives of the ePrivacy Directive and its articles, taking into account technological, social and legal developments.

I.2.1. PERTINENCE OF EU SECTOR SPECIFIC RULES

The majority of citizens, consumer and civil society organisations (90.3%) see an added-value in having rules on EU-level to ensure the right to privacy and confidentiality in the electronic communications sector.

61% favour EU rules to ensure the free movement of personal data in the electronic communications sector and 62.8% see the need to ensure the free movement of equipment and services.

A majority of citizens, consumer and civil society organisations consider it relevant to have specific rules for the electronic communications sector on confidentiality (83.4%), traffic and location data (73%), unsolicited commercial communications (78%) and notification of personal data breaches (72.8%). For directories (54.4%) and calling line identification (55.5%), a smaller majority supports the need for special rules. The respondents were more divided on the need for special rules on itemised billing, (47.3% support it, while 31.3% have no opinion and 21.4% do not support it) and automatic call forwarding (48.4% support it, while 31.9% have no opinion and 19.8% do not support the need).

Citizens, consumer and civil society organisations believe that the rules are needed because they protect the personal data of consumers and they believe they should be in control of the data they communicate to the public. If taken out, the rules should be included in the revised Universal Service Directive.

90% of public authorities agree that having rules on EU-level in the electronic communications sector are needed to ensure privacy and confidentiality.

72.4% believe that they are needed to ensure free movement of data; 67.8% see a need to ensure the free movement of services and equipment.

Public authorities believe that specific rules for the electronic communication sector are needed on confidentiality (88.9%) and on traffic and location data (92.3%). By a majority, public authorities support special rules for the electronic communications sector in all areas of the consultation (specified above).

A majority of industry does not see the benefit of EU sector-specific rules. 63.4% replied that EU rules are not needed to ensure the protection of privacy and confidentiality, 64.6% said that rules are not needed to ensure the free movement of data and 58.3% do not see the need for rules to ensure the free movement of services and equipment. This is echoed by the ECS/ECN providers who by a larger majority do not believe that rules are necessary (72-86%).

The area that industry quotes as not requiring special rules for the electronic communications sector is the notification of personal data breaches (78.1%), followed by the rules on traffic and location data (66.2%), confidentiality (63.4%), and on unsolicited commercial communications (63.1%).

A few industry respondents argue however that rules on direct marketing and directories should be maintained in the ePrivacy Directive and that specific rules are needed for the ECS/ECN sector because it collects data inherently more sensitive than the data OTT services collect.

The ECS/ECN industry argues that special rules are not needed because some are covered by the GDPR and all actors are collecting and processing similar personal data. Inconsistent regulation of the same services leads to discrimination between types of businesses and this is also confusing for consumers, they argue. The rules that the GDPR does not cover could be covered by consumer protection legislation or by the telecom package.

I.3. COHERENCE OF THE ePRIVACY DIRECTIVE

This section aimed to assess whether the existing rules are coherent with one another and with other legal instruments.

I.3.1. COHERENCE WITH OTHER EU INSTRUMENTS

On the coherence of the ePrivacy Directive with other instruments on security (i.e. Framework Directive, GDPR, Radio Equipment Directive and Network and Information Security (NIS) Directive) **around one third of citizens, consumer and civil society organisations reported that they did not know**. Among those that had an opinion, most reported that the provisions are significantly or moderately coherent with each other.

Industry in general reported that the strongest level of coherence is with the GDPR (65.5% reported significant or moderate levels of coherence), followed by the Framework Directive (51%) and the NIS Directive (50%). On the Radio Equipment Directive, most industry respondents were unaware of its coherence; 24.6% reported significant/moderate coherence.

ECS/ECN providers report general coherence with the Framework Directive and the NIS Directive (60% for both) but less with the GDPR (40%). Many respondents reported that they did not know about coherence with the Radio Equipment Directive.

Public authorities reported general coherence except on the Radio Equipment Directive for which they also did not know.

I.3.2. TELEMARKETING

Citizens, consumer and civil society organisations and public authorities think that the freedom left to Member States to decide on opt-in or opt-out for telemarketing is not coherent.

On telemarketing calls, a majority of citizens and civil society (61.5%) report that it is not coherent to allow Member States to make telemarketing calls subject either to prior consent or to a right to object, while Article 13.1 requires opt-in consent for email, fax, and automatic calling machines.

41.4% of industry say this is coherent while the rest find it is not (31.8%) or have no opinion (26.8%).

A majority of public authorities also report that this is not coherent (61.5%); around 30% report that this is coherent, the rest have no opinion.

I.3.3. MARKETING MESSAGES VIA SOCIAL MEDIA

Citizens, consumer and civil society organisations and public authorities want an opt-in rule for marketing messages sent via social media, while industry wants an opt-out system.

On the legal uncertainty regarding the legal treatment of messages sent through social media, a majority of citizens, consumers and civil society organisations (82.4%) and public authorities (74.1%) would like an opt-in system for marketing messages sent through social media (like for email) and they are largely against applying the opt-out system of Article 13.3.

Industry largely prefers the opt-out system (71%).

I.4. EFFICIENCY OF THE EPRIVACY DIRECTIVE

This part sought to assess the costs and benefits of the ePrivacy Directive, including for citizens at large.

I.4.1. USERS' TRUST

A majority citizens, consumer and civil society organisations (61.1%) do not believe that the national provisions implementing the ePrivacy Directive have raised the level of trust in the protection of their data when using electronic communications services (or has only done so to a slight extent). **50% of responses from industry also point to this finding, while 44% of public authorities report that there has been a significant/moderate increase in the level of trust** (most of the other respondents in this category do not have an opinion).

I.4.2. ADDITIONAL COSTS FOR BUSINESSES

In terms of the cost of compliance for businesses, 43.5% of citizens, consumer and civil society organisations respond that they do not know and 24.9% say that the cost is little. Some state that the costs are excessive for SMEs and start-ups. A regulation would be cheaper to comply with than a Directive, they believe.

Industry replies that the costs are significant (62.3%) or moderate (20.8%), while public authorities do not know (56.5%) or respond that they are moderate (17.4%).

Precise costs are not provided by ECS/ECN and do not appear in their accounting systems. The ECS/ECN industry argues that the ePrivacy Directive has prevented them from offering new services launched by actors not subject to the rules (opportunity costs), due to an uneven playing field under the current legal framework.

Some report that the costs are disproportionate for SMEs, that the fragmentation at national level raises costs, technical and legal advice costs and costs to check Robinson registers are significant, litigation procedures for Article 5.3 and Article 13.3 are lengthy and disproportionate. Another SME points that the overall costs are relatively small for complying with cookie rules, no more than the annual hosting cost of a website. A few have expressed concerns regarding the excessive costs of compliance for SMEs and start-ups. They argue that large "fixed cost" of compliance should not become a barrier for new businesses.

Public authorities do not appear to have much information. They say that the costs are indirect and that there are legal setbacks.

I.4.3. PROPORTIONALITY OF COSTS

A majority of citizens, consumer and civil society organisations (57.1%) find that the cost of compliance is proportional to the objectives of the ePrivacy Directive. Most consumers believe that the price of compliance is justified in order to reach the objectives of confidentiality of the ePrivacy Directive.

A majority of industry players (65.3%) report disproportionate compliance costs to meet the objectives. 22% of industry players did not have an opinion and 12.7% agreed to the cost of compliance.

ECS/ECN providers argue that compliance costs are creating a clear competitive disadvantage as compared to OTTs, which are not in the scope of the directive.

Some of them demand a level playing field with OTTs. They argue that the current approach is creating legal uncertainty and an asymmetry of data protection/privacy law, as consumers are not protected in the same way when they use functionally equivalent communication services, e.g. Internet based service providers. According to them, a highly competitive market such as ECS/ECN can provide effective solutions without regulation.

Moreover, some entities have expressed the concern that personal data protection rules are already fully covered by the GDPR and that the answer to this issue lies in best practice of GDPR guidance and not in more law.

Finally, some of these ECS/ECN operators insist that a competitive disadvantage creates significant loss of competitiveness and business opportunities for the concerned organisations, with a negative impact on innovation and on the time needed to market new services. Moreover, investments that would have been made in the absence of sector-specific regulation are delayed or discarded.

Most public authorities (72.7%) believe that the costs of compliance are in line with the objectives pursued.

Some have highlighted the right to privacy as one of the most important rights guaranteed by the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. In order to protect it, actors involved in data collection and manipulation must accept the cost of compliance.

I.5. EU ADDED-VALUE OF THE EPRIVACY DIRECTIVE

This section seeks to assess the EU added-value of the ePrivacy Directive in order to evaluate whether EU action is needed for this specific sector.

A majority of citizens, consumer and civil society organisations (86.7%) believe that national measures would have been necessary if the ePrivacy Directive had not existed. 65% of public authorities agree but 50.4% of industry (60% of ECN/ECS) disagree.

A majority of citizens, consumer and civil society organisations think that the ePrivacy Directive has had clear added-value for increasing/harmonising the confidentiality of communications (55.4%) and the free flow of personal data (54.4%). Less than half (47.4%) believe this is the case for the free movement of services and equipment. Public authorities believe there is added-value for the 3 areas (respectively, 91.6%, 80% and 56%).

Industry at large is more critical. Only 40.1% believe that the Directive has had added-value for the confidentiality of communications, 34% for free flow of personal data and 39.6% for the free movement of services and equipment. ECN/ECS providers are more critical: 20.2% believe that the Directive has had added-value on the confidentiality of communications, 17.6% for free flow of personal data and 11.7% for the free movement of services and equipment.

II. REVISING THE EPRIVACY DIRECTIVE: LOOKING AHEAD

This section covers forward-looking questions to assess the possible solutions in case there is a need to revise the ePrivacy Directive.

PRIORITIES FOR REVISION

- Citizens, consumer and civil society organisations believe that the priorities (with the option to select several) of any future instrument should be the following (in the most frequently quoted order):

    - Amend the provisions on confidentiality of communications and of terminal equipment (68.5%);
    - Widen the scope of the provisions to cover OTTs (62.9%);
    - Amend the rules on governance (61.8%);
    - Amend the provisions on unsolicited commercial communications (57.9%);
    - Amend the provisions on security (55.6%);
    - None of the provisions are needed any longer (3.9%);
    - Others (11.8%).

- For industry, top priorities should be:

    - None of the provisions are needed any longer (55.6%);
    - Widen the scope to cover OTTs (28.8%);
    - Amend the rules on unsolicited commercial communications (22.9%);
    - Amend the provisions on governance (22.9%);
    - Amend the provisions on unsolicited commercial communications (22.9%);
    - Amend the provisions on confidentiality of communications and of terminal equipment (19.6%);
    - Amend the provisions on security (17%);
    - Others (12.4%).

    The position of ECN/ECS is broadly in line with this.

- For public authorities, top priorities should be to:

    - Widen the scope to OTTs (72.4%);
    - Amend the rules on unsolicited commercial communications (58.6%);
    - Amend the rules on confidentiality (51.7%);
    - Amend the provisions on security (41.4%);
    - Amend the provisions on governance (41.4%);
    - Other (6.9%).

CHOICE OF LEGAL INSTRUMENT

A very clear majority of citizens, consumer- and civil society organisations (66.3%) and of public authorities (66.7%) believe that a regulation would be a better instrument than a Directive.

47% of industry representatives suggest other options. 24.1% are against the idea of a regulation, while 28.9% are in favour of a regulation. Among the ECS/ECN, 67.7% favour other options, while only 15% are in favour of a regulation.

When referring to the other options, industry often states that the ePrivacy Directive should be repealed and not replaced, the GDPR is sufficient. According to this category of stakeholders, consumer related questions are thought to be better covered under consumer protection instruments.

II.1. REVIEW OF THE SCOPE

II.1.1. EXTENSION OF SCOPE TO OTTs

Citizens, consumers and civil society organisations think that the rules should be broadened to cover OTTs (76%), a few believe it should in part (8.4%) while a few think that it should not be broadened (5.6%). They would like the rules on security, confidentiality, traffic and location data and on unsolicited marketing communications to be extended to messages sent via OTT services by close to 100% support. **Public authorities are aligned with the opinion that the rules should be extended but in slightly different proportions (62.1% in favour**, 31% in part, none answered not at all). Those in favour also support with close to 100% that all the rules mentioned should be extended.

Industry is more divided as 41.6% do not want the scope to be broadened while 36.2% do and 7.4% believe it should in part. Of the respondents that said that the rules should be broadened entirely or in part, 98.4% said so for the rules on confidentiality, 95.1% for the security obligations, 85.2% said so for the rules on security and traffic and location data and 72.1% for the rules on unsolicited commercial communications.

45% of the ECS/ECN industry answered that the scope should be broadened to OTTs, while 15% said no. The rest said in part (7.5%) or did not know (12.5%).

II.1.2. TYPE OF NETWORKS TO BE COVERED

A majority of citizens, consumer and civil society organisations believe that the rules on security (58.2%), confidentiality (64.7%) and on traffic and location data (58.2%) should apply to all networks: public, private and closed. A smaller proportion (20-24%) advocates that these rules should apply to Wi-Fi internet access provided to customers or the public such as in airports, hospitals etc. ("**non-commercial Wi-Fi**"), while a smaller proportion (11-20%) opts for the current situation i.e. that they should only apply in relation to publicly available networks.

Industry is equally divided between advocating that the rules on security should apply to all networks on the one hand (48.6%) and to only publicly available networks on the other (48.6%). On the confidentiality of communications, slightly over half (51.4%) think that the rules should apply only to publicly available networks, and the other half to all networks. As for the rules on traffic and location data, significantly more (57.7%) believe that the rules should only apply to publicly available networks. A few respondents say that non-commercial Wi-Fi should be covered (2-2.5%, depending on the area i.e. security, confidentiality and the rules on traffic and location data).

The ECS/ECN industry (slightly over 70%) favours the rules applying to all networks.

Public authorities are more divided as on applying the rules on security, an equal number (37.5%) opt for all networks and non-commercial Wi-Fi, slightly less (25%) for publicly available networks. On the confidentiality of communications, slightly more opt for all networks (44%). With regard to the applicability of the rules on traffic and location data, more opt for application to non-commercial Wi-Fi (44%).

II.2. ENSURING SECURITY AND CONFIDENTIALITY OF COMMUNICATIONS

II.2.1. SECURITY

A majority of citizens, consumer and civil society organisations (87.2%) believe that legislation should ensure the right for individuals to protect their communications, e.g. by securing Wi-Fi connections or by using encryption apps.

Public authorities agree (72%) with user empowerment measures.

Industry is divided between those that agree (41.5%), those that do not (31.1%) or that do not know (27.4%). The ECS/ECN industry is also divided between those that agree (30%) and that do not (37.5%). Many in this category did not answer (17.5%) or did not know (15%).

Those from industry (at large) that disagree highlight that legislation is not needed, that user solutions can be developed by industry and it is in their interest to do so. Some also explain that when traffic is encrypted, operators cannot detect malware and viruses and cooperate with law enforcement and detection of illegal and harmful content. Others point that the obligation to secure communications is covered in other instruments such as the GDPR and the NIS Directive.

The consultation document put forward the following policy options to improve security:

- 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 communications 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.

A majority of citizens, consumer and civil society organisations support the options for additional policy measures to improve the security requirements in all the areas suggested by the Commission and each option received support with largely the same proportions: development of minimum security or privacy standards for networks and services (86%), followed by Internet of Things (79.8%), network components (74.8%) and software used in combination with the provision of a communication service (73.7%).

Industry is much less receptive to these additional policy measures on security. The development of minimum security or privacy standards for networks and services received support from 29% of industry, followed by the Internet of Things (28.8%), network components (23.6%) and software used in combination with the provision of a communication service (20.5%).

Public authorities are broadly in favour except for the idea to extend security to cover software used in combination with communications services, where only 46.2%

think that this will significantly or moderately improve the situation. The development of minimum security or privacy standards for networks and services received most support (80.7%), followed by extending the security requirements to include all network components (65.3%) and Internet-of-Things devices (61.5%).

II.2.2. COOKIES

The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated criticism that citizens do not have choice. The Commission asked in the consultation whether:

- Information society services should be required to make available paying service (without behavioural advertising) as an alternative to the services paid by users' personal information (**option 1**);
- 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 (**option 2**).

Citizens, consumer and civil society organisations support option 1 (55.5%) less than option 2 (76.6%), while public authorities do not agree with option 1 (55%) but agree with option 2 (70%). Industry disagrees or strongly disagrees with option 1 (78.7%) and option 2 (75.8%).

Those in favour of a paying service argue that this would enable users to enjoy an online experience without intrusion into their personal lives. Those against the pay option say this would be discriminatory between those who can afford to pay and those who cannot, that this is not commercially possible for many online companies and would be contrary to the fundamental right to conduct a business.

Those in favour of the solutions whereby online service providers should not be allowed to prevent access to the service argue that a pay option should be available. Those against the option argue that the law should not impose a certain business model. Online behavioural advertisement, enabled through the use of cookies, is a way to ensure sustainability.

The consultation asked for which options among the following (with several options available), consumers should be asked for their consent before personal data and other information is processed when stored on their smart devices:

- Identifiers placed/collected by a third party information society service (not the one you are visiting) for online behavioural advertising purpose (‘third party cookies’);
- Identifiers placed/collected by an information society service which the consumer is 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 the consumer is visiting whose purpose is to support user experience, such as language preference cookies;
- 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 identifiers.

Citizens, consumer and civil society organisations replied most often (96.5%) that they want to be asked to consent before third party cookies are used. 69.4% said they want to be asked before cookies are used for frequency capping, 62.3% for website analytics and 60% before identifiers are used by information society services to detect fraud.

Although the other stakeholders did not have to answer these questions, some did. Industry mostly refers to others solutions (62%) and says that consent should be sought for use of third party cookies (36.7%). The other options received between 11.4% and 19% of support by industry.

Public authorities believe that consent should be sought for third party cookies (85%), for frequency capping (55%). The least support was for consent to be given when the data is immediately anonymised (15%).

On the solutions proposed to the cookie consent issue, citizens, consumer and civil society organisations supported some options (respondents could select multiple answers):

- Introducing provisions to prevent specific behaviours, irrespective of users' consent (86.7%);
- Imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated, preventing operators from collecting and storing data (81.2%);
- Mandating EU standards organisations to produce do-not-track or do-not-collect/store types of standards (74%);
- Adopting legislation e.g. delegated acts on defining how to express user preferences regarding whether they want to be tracked (60.2%);
- Supporting self/co-regulation (34.8%);
- Other (9.4%).

This contrasts with the solutions preferred by industry:

- Supporting self/co-regulation (58.3%);
- Other (36.8%);
- Imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated, preventing operators from collecting and storing data (18.4%);
- Introducing provisions to prevent specific behaviours, irrespective of users' consent (16%);
- Mandating EU standards organisations to produce do-not-track or do-not-collect/store types of standards (14.1%);
- Adopting legislation e.g. delegated acts on defining how to express user preferences regarding whether they want to be tracked (9.8%).

The most common solution industry put forward was to repeal the ePrivacy Directive and refer to the rules of the GDPR. They believe that horizontal rules are needed, technology-neutral and future-proof. Some also argued in favour of an opt-out approach.

The options most **public authorities preferred were the introduction of rules prohibiting specific abusive behaviour (70.4%) and placing obligations on manufacturers (63%).**

II.2.3. TRAFFIC AND LOCATION DATA

The ePrivacy 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. Furthermore, consent of users should be asked in order to use them for value-added services e.g. 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. Under the current regime, traffic data cannot be processed for any other purpose than those mentioned.

On the question if the exemptions to consent for processing traffic and location data should be amended (possibility to choose several options), **citizens, consumer and civil society organisations' preference was not broadening the rules (49.1%)** but they accept that the use of this type of data should be allowed for other purposes if it is fully anonymised (45.1%). A proportion considers that the provisions should be broadened to include the use of such data for public purposes (27.4%) or statistics (20%) provided certain guarantees are included (the argument being that this is the case already in practice). They argue that traffic and location data provide a detailed picture of individuals' habits and that this type of data should only be processed with their prior consent. Some would also like the principles of data minimisation and purpose limitation to be included in sector-specific legislation. They also flag the difficulty of ensuring full harmonisation.

Industry considers that the provisions on the processing of location and traffic data should be removed (63.2%). A substantial proportion considers that the provisions should be broadened to include the use of this data for statistical purposes (with the required safeguards) (36.1%), and/or to include the use of this data for public purposes (with required safeguards) (31.6%). Some consider that the data should be allowed to be used for other purposes if fully anonymised (25.6%) and a few (6.8%) do not want the use to be broadened.

Industry appears in favour of removing the provisions to achieve a level playing field, and argues that the GDPR provides enough safeguards. In the event that special rules still exist, the possibilities to process traffic and location data should be extended and aligned with the GDPR especially on the possibility of pseudonymisation. Some traffic and location data will not fall under the scope of personal data and this data should not be made subject to processing restrictions as this could limit the EU's ability to build a data-driven digital economy.

Public authorities favour in roughly an equal manner the solutions proposed (27.3% - 42.4%) except the option to delete the provisions on traffic and location data (6%). 36.4% is not in favour of broadening the rules. They highlight the importance of being able to use data from new sources for statistical purposes. Some also highlight that the definition of traffic data should not refer to subscriber billing.

II.3. Non-itemised billing, calling line identification, automatic call forwarding, directories

The ePrivacy Directive provides for the right of subscribers to receive non-itemised bills. It also gives callers the right to prevent the presentation of the calling line identification ("CLI") if they wish to guarantee their anonymity. Subscribers have the possibility to stop automatic call-forwarding by a third party to their terminals. Finally, subscribers must be able to determine whether their personal data is included in a public directory.

Citizens, consumers, civil society and public authorities generally believe that the provisions on non-itemised billing (74.8%) calling line identification, 76.3% automatic call-forwarding (65.2%) and directories (74%) should be kept and are still relevant.

Consumer organisations and civil society believe that the rules are needed because they protect the personal data of consumers who should be in control of the data they communicate to the public. If repealed, the rules should be included in the revised Universal Service Directive.

Citizens argue that they want their say in directories, automatic forwarding should cover other types of communications, but some also argue that CLI masking should be banned.

Industry replied that they would like the rules on non-itemised billing (57.2%) calling line identification (55.7%), automatic call-forwarding (55.3%) and directories (55.4%) to be scrapped. The ECS/ECN industry favours that view by a larger proportion (around 75%).

The ECS/ECN industry argues that the rules should either be removed completely or moved from the ePrivacy Directive to other horizontal consumer protection instruments, elsewhere in the ECS/ECNs framework or in the citizens' rights Directive. Where relevant, these rights should be extended to all communications services, but it is not clear how this applies to non-voice services. The argument is made that the rules should not apply to business users. The obsolete nature of printed directories was also brought up and that it is no longer included in the scope of universal service obligations in most Member States. They also argue that the development of search engines and online services have changed the ability to search for professional services. CLI is appealing to customers but the rules should be amended to cater for cross-border communications and to cover new VoIP technologies. The GDPR provides sufficient safeguards.

Internet companies and other industries either see no need for these rules to be extended to OTTs or consider that they should be included elsewhere. Some respondents do not want commercial companies to be allowed to withhold their calling and connected line identification number because this is generally used for direct marketing calls. Many argue that the rules are not needed or are obsolete.

There are dissenting views on the possibility for subscribers to have their data listed and to have data bases with accurate information. Provisions on non-itemised billing may be needed to protect the privacy of sensitive communications such as helplines. These are valuable consumer rights according to the advertising industry.

Public authorities (84%) favour maintaining the rules on non-itemised billing, CLI (72%), call-forwarding (79.1%) and directories (60%).

Some note that the rules on CLI should be amended to prevent withholding CLI for sales and marketing purposes to avoid 'spoofing'; that the rules in general should be modernised for the digital age. More studies are needed to see if end users have used the possibility to have non-itemised billing and restrictions on CLI. If this is not widely used, the rules should be repealed.

II.4. UNSOLICITED COMMERCIAL COMMUNICATIONS

The ePrivacy Directive requires prior consent to send commercial communications through electronic mail (including SMS), fax and automatic calling machines without human interaction. However, companies which have acquired an end-user's email as a result of a sale of products/services can do direct marketing by email to advertise similar products or services, provided that the end-user is given the possibility to object (**opt-out**). Member States can decide whether to require opt-in or opt-out for marketing calls with human interaction. The protection against all types of commercial communications also benefits legal persons but the ePrivacy Directive leaves it to Member States to decide whether they are protected by an opt-in or opt-out regime.

Citizens, consumers and civil society organisations believe that Member States should not be able to choose between an opt-in or an opt-out system for direct marketing calls with human interaction directed at individual citizens (72.3%) or for direct marketing to legal entities (67.7%). **Member States should apply the opt-in solution** for marketing calls to citizens (88.2%) and for legal entities (74.8%).

Consumers and civil society believe that the opt-in system is a better option for all types of communications. They find that opt-out regimes do not function adequately, despite the fact that they have existed for a number of years.

Public authorities agree that they should not be able to choose between an opt-in or opt-out for marketing calls sent to individuals (73.3%) and legal entities (65.5%). They favour opt-in for calls to individuals (86.9%) but opinions are nearly equally divided between the opt-in and the opt-out for marketing messages to legal entities.

Of public authorities that commented, most argued in favour of an opt-in system, because it is simpler to understand. The others either recommend an opt-out system or do not have an opinion but stress the need for flexibility or coherence with the GDPR.

Industry is aligned on their preference that Member States should not be given the choice (52%). It diverges with the other two categories in so far as industry would prefer an opt-out system for marketing calls made to individuals (73.5%) and to legal entities (77.3%).

The ECS/ECN industry argues that sector-specific legislation needs to be abolished, rules need to be aligned with the GDPR which includes rules on direct marketing (right to object). Those should be clarified in guidelines from the European Data Protection Board (EDPB). If maintained, these rules should either be in the GDPR or in the Unfair Commercial Practices Directive. The system should be harmonised but kept flexible. The fact that opt-out lists exist at national level shows that users trust and rely on them. There could be more harmonisation on the existing codes of practice and opt-out models.

Many marketing companies and other companies argue that this is not sector-specific legislation and that rules should either be in the GDPR or in the Unfair Commercial Practices Directive. They argue for a single opt-out regime for all types of

communication channels, and that this would also help SMEs. Other tools to protect against direct marketing exist: smartphone settings blocking push notifications and/or calls from callers identified as nuisance, some email platforms automatically filter commercial communications into a secondary space.

II.5. FRAGMENTED IMPLEMENTATION AND INCONSISTENT ENFORCEMENT

Some provisions of the ePrivacy Directive may be formulated in too general terms. Consequently, Member States may have implemented key provisions differently. The result is a fragmented situation. While the Data Protection Directive entrusts its enforcement to data protection supervisory authorities, the ePrivacy Directive leaves it to Member States to designate a competent authority or other national bodies. The result is a fragmented situation. Some Member States have allocated competence to data protection supervisory authorities, whereas others to the ECS/ECN national regulatory authorities, others to yet another type of body such as consumer authorities. See section III. 7 of the background document.

II.5.1. AUTHORITIES IN CHARGE

A majority of citizens and consumer and civil society organisations consider that enforcement of the ePrivacy Directive should be allocated to a single authority (69.3%). 18.2% do not favour that solution, the rest do not know.

Of those that favour a single authority, consumers and citizens think that the national data protection authority would be most appropriate (67.2%) while 20.4% would prefer the national consumer protection authority to be in charge.

Industry is in line with the position of citizens and consumers in roughly the same proportion. They think that the national data protection authority would be best suited but the proportion is not as high (51.7% for the industry at large, 30% for the ECS/ECN) as many prefer other options (38.8%).

Public authorities are less convinced as only 38.5% agree while 50% disagree, and the rest do not know. Of those that agree with a single authority, they think that the best authority would be the national data protection authority (53.3%) while 26.7% would prefer the national ECS/ECN authority to be in charge.

21.3% of the total respondents answered 'other'. Close to all of them (94.7%) commented and their options and arguments vary. Some would like the DPA at EU level to be competent (EDPB or an EU agency), that the sector-specific rules should be repealed altogether, or placed in other instruments, consumer protection rules should be moved to consumer protection acquis and enforced by consumer protection authorities, ENISA is also mentioned for the security aspects, one mentions the use of the consistency mechanism.

Those that support giving responsibility to telecom NRAs argue that they have a deeper understanding of the ECS market. If everything is given to the DPAs, the non-privacy values could be forgotten or given less priority.

Of those that say that the DPA should be responsible, some stress that this should only be the case for privacy-related issues, and that the other issues should be covered in other instruments. There is strong emphasis on harmonised guidance. Some also call for the independence, powers and funding of national DPAs to be strengthened.

II.5.2. CONSISTENCY MECHANISM

A majority of citizens, consumer and civil society organisations believe that the consistency mechanism created by the GDPR should apply to cross-border matters covered by the ePrivacy instrument (71.9%). Slightly over 60% (55.5% of ECS/ECN) of industry agree, while public authorities appear more divided: 37.5% have not provided an answer, 27.5% agree and 17.5% disagree.

II.5.3. SANCTIONS

On the question of sanctions, 82.9% of citizens, consumer and civil society organisations believe that the future instrument should include specific fines and remedies. 68.5% of industry disagrees, while exactly half of public authorities agree and one third disagrees. The rest do not know.