Briefing
Implementation Appraisal

European Parliament

February 2017

Review of the ePrivacy Directive

Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector

This briefing is one in a series of 'Implementation Appraisals' on the operation of existing EU legislation in practice. Each briefing focuses on a specific EU law, which is likely to be amended or reviewed, as envisaged in the European Commission's annual work programme. Implementation Appraisals aim to provide a succinct overview of material publicly available on the implementation, application and effectiveness of an EU law to date – drawing on available input from the EU institutions and external organisations. They are provided to assist parliamentary committees in their consideration of the new proposals, once tabled.

EP committee responsible at time of adoption of the EU legislation: Committee on Civil Liberties, Justice and Home Affairs (LIBE).[1]
Date of adoption of original legislation in plenary: 30 May 2002.
Entry into force of original legislation: 31 July 2002 (Article 20).
Date of transposition: before 31 October 2003 (Article 17). The amendments adopted in 2009[2] had to be transposed by 25 May 2011 (Article 17 of Directive 2009/136).
Planned date for review of legislation: Article 18 of the directive requires the Commission to report to the co-legislators on its application and impacts no later than three years after the transposition date,[3] and to make the necessary proposals to amend the directive to improve its effectiveness.
Timeline for new amending legislation: The amendment of Directive 2002/58 is included in Annex 1 of the Commission Work Programme 2017 (CWP 2017). The proposal was published on 10 January 2017.

1. Background

Since the adoption of Directive 2002/58 on privacy in the electronic communications sector (ePrivacy Directive), pervasive technological, economic and social changes have tangibly influenced the way we use electronic communications and electronic communications equipment such as mobile phones and laptops. Among other things, these changes have had a direct impact on how our personal data are accessed, processed, used and ultimately protected.[4] This in turn has affected the ability of the ePrivacy Directive to

[1] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs at the time of adoption.
[2] The original text was amended in 2009 by Directive 2009/136 (Citizens' Rights Directive). Additional measures linked to the ePrivacy Directive include Commission Regulation 611/2013 on the notification of personal data breaches. For a detailed analysis of these changes and their implications, see Y. Poullet (2010) Commentary on Directive 2002/58/EC, article3, 4 and 5 - *Concise European IT law*, p. 183-199; V. Papakonstantinou and P.de Hert (2011), The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights, J. *Marshall Journal of Computer & Information Law* 29 (1).
[3] The relevant reports can be accessed here.
[4] For a definition of personal data, the issue of trust in a digital environment and key data protection challenges, see S. Monteleone Golden Eye: Who rules tomorrow's Europe?, At a glance, EPRS, April 2016. For a comprehensive overview of the impact of

achieve one of its primary objectives: ensuring that the fundamental rights to the respect of private and family life, home and communications, and to the protection of personal data (respectively Articles 7 and 8 of the Charter of Fundamental Rights of the European Union), are equally protected in an electronic communications environment.[5] The directive is part of the regulatory framework for electronic communications; as such, it applies the definition of 'electronic communications' outlined in Article 2 of Directive 2002/21 (the Framework Directive).[6] As will be explained below, this has direct implications for the current scope of ePrivacy rules and their continued ability to provide legal clarity in a fast-moving technological environment. For instance, despite the 2009 amendments to Directive 2002/58, the recent diffusion of over-the-top (OTTs) players offering to consumers various internet-based services, such as instant messaging, still leaves areas of uncertainty, as OTTs are currently not covered by the current ePrivacy provisions.[7]

Against this background, the Digital Single Market Strategy of May 2015 included a revision/upgrade of existing ePrivacy rules among its key priorities, as a way to complement and further specify the EU legislative framework on data protection. Indeed, the revision of Directive 2002/58 is also meant to ensure that future ePrivacy rules are aligned with the General Data Protection Regulation (GDPR) that will become applicable in May 2018.[8] A proposal to that effect was adopted by the European Commission on 10 January 2017. It seeks to repeal the original directive and replace it with a regulation, with the aim of achieving three main objectives through a set of targeted changes to the current text:[9] 1) the effective confidentiality of all electronic communications, thanks to more technologically neutral and future-proof legislation; 2) effective protection from unsolicited commercial communications through, among other things, a ban on anonymous marketing calls; and 3) greater harmonisation and simplification of the existing legal framework, by adopting a single set of rules for the entire EU and by eliminating redundant and outdated provisions.[10]

2. EU-level reports, evaluations and studies

e-Privacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation - Report for the European Commission

Completed in 2015, this external study[11] carried out for the European Commission focused on five central topics of the ePrivacy Directive: its geographical and material scope of application (Articles 1 to 3); the confidentiality of communications (Article 5(1)); cookies and other techniques covered in Article 5(3); traffic and location data (Articles 6 and 9), and unsolicited commercial communications (Article 13). The report sought to fulfil three objectives: assessing the state of transposition and implementation of the five elements described above;[12] establishing whether Directive 2002/58 has achieved its intended goals; and providing an

technological developments on privacy in various areas of our lives, see C. Akrivopoulou and A.Psygkas (eds.), Personal data privacy and protection in a surveillance era: technologies and practices, IGI global, 2011; and T. Payton and T. Claypoole, Privacy in the age of big data recognizing threats, defending your rights, and protecting your family, Rowman & Littlefield, 2014.

[5] Article 1 of the ePrivacy Directive refers to the 'right to privacy, with respect to the processing of personal data in the electronic communication sector'. Note that under the directive, both natural and legal users of electronic communications services are protected. Other central objectives outlined in Article 1 are to ensure the free movement of data processed in the electronic communications sector and of electronic communications terminal equipment and services within the EU internal market.

[6] For further details on the regulatory framework and ongoing debates on the opportunity of revisiting the concept of electronic communications, see L. Schrefler, Reforming the regulatory framework for electronic communications networks and services, Implementation Appraisal, EPRS, August 2016. For an in-depth analysis, see Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), July 2016; and European Data Protection Supervisor (2016), Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), Opinion 5/2016, July. The Article 29 Working Party is a platform of cooperation composed by representatives of the national data protection authorities, the Commission and the EDPS.

[7] On this point, see Commission Communication Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe of 25 May 2016, COM (2016) 288, pp. 6-7.

[8] For further details, see Review of the ePrivacy Directive - Legislative Train Schedule, Train N. 2, European Parliament.

[9] For further details, see section 6.2 of the impact assessment SWD (2017)3 accompanying the proposal.

[10] See European Commission SWD (2017) 4, p. 2.

[11] SMART 2013/0071, January 2015.

[12] A comprehensive set of country fiches on transposition and implementation in the Member States can be found in Annex 1 of the report, and in a concordance table with references to country reports.

analysis of the interaction between the ePrivacy Directive and future data protection legislation.[13]

As regards **the geographical and material scope of application** of the ePrivacy Directive, the report noted that similar services (at least from the users' perspective) are still being regulated under three separate sets of rules: the electronic communications framework (to which the ePrivacy Directive belongs); information society services legislation, and rules on audio-visual media services. As a result, Directive 2002/58 has been transposed under different legal frameworks at the national level. Indeed, in some countries it is part of the legislation on electronic communications, while in others it falls under the general data protection law or under consumer legislation. Ultimately, this may mean that the scope of application of individual provisions of the directive, in particular Article 3 on the services concerned by the legislation, differs between countries. The report also added that the scope of application of the directive itself is ambiguous, as it tends to exclude some information society services which should incontestably fall under its remit. This ambiguity has also led to the unequal treatment of services which are very similar from a functional perspective. And indeed, some Member States (e.g. Germany and Finland) have extended the directive's scope of application to additional services when transposing the text.

How do cookies work?

The ePrivacy Directive is often referred to as the 'cookies law' because of its provision on the storage of and access to information on users'' terminal equipment (Art. 5.3). This Article covers various techniques and in particular 'cookies', i.e. small pieces of data that a browser can be asked to save/store when a user visits a website. Cookies will then allow the website to recognise the device when the user visits again, and also to gain a better understanding of his/her preferences over time and use such information to target advertisements or customise the online experience. Several types of cookies exist. When they are classified by lifespan, cookies can be **session cookies** if they are erased once a user closes their browser, or **persistent cookies** if they are stored on the user's device for a certain period of time. Another important distinction concerns the domain hosting the cookies. **First-party cookies** are those placed by the visited website and essentially aim at improving efficiency and the user's experience. Instead, **third-party cookies** are those hosted by a domain that is not the same as the visited page's domain. They are used among others by advertising networks to monitor users' behaviour and better target their advertisements over time. A recent analysis by the Article 29 Working Party established that **70 % of the recorded cookies** (on average 35 per website) across nearly 500 websites **were third-party cookies** and tended to be **of the persistent type**.

The requirements on the **confidentiality of communications** outlined in Article 5(1) did not achieve the objective of harmonising national provisions across the EU. In many Member States, this aspect was already regulated prior to the adoption of the ePrivacy Directive; despite transposition, different legal traditions across the EU eventually resulted in a diversity of definitions, conditions and modalities to protect confidentiality, as well as in differing applicable exceptions – for instance as regards the monitoring of communications for law enforcement purposes or in a professional context. Potential issues were also noted as concerns the enforcement of the rights granted by the directive. This could be explained by the fact that in various Member States different authorities are responsible for implementing the ePrivacy Directive.[14] Such a situation may sometimes lead to inconsistencies and uncertainty in the application of existing rules within the same country.

According to the report, Article 5(3) on **cookies**, spyware and other techniques and the requirement to obtain **users' prior consent** 'did not entirely reach its objective'. The cookies modification introduced in the 2009 revision of the directive reportedly led to uncertainty on its application on the ground. It also required interpretation and guidance by the Article 29 Working Party,[15] for instance on the question of browser setting configurations and how consent should be given. Moreover, an excessive use of cookies by many websites seems not only to have caused irritation among users, but has also reduced the informative goal of such warning messages. Indeed, users 'bombarded' by cookies may not necessarily (take the time to) understand

[13] Note that when report SMART 2013/0071 was being drafted, the GDPR was still at the proposal stage in the ordinary legislative procedure. Hence, that particular section of the report is not covered in the present briefing.

[14] Article 15a leaves Member States free to choose which national authority/authorities is/are competent for enforcing Directive 2002/58.

[15] See above, footnote 6.

the difference between different types of situations, such as the use of third-party cookies versus cases where cookies relate to the purpose 'for which the user is navigating on the site' (first-party analytic cookies).

The report found that Article 6 of the directive (**traffic data**)[16] had been correctly transposed into national legislation. However, concerns remained in terms of enforcement. Problems were also observed for **location data** (Article 9),[17] particularly as some location-based services entailing privacy risks are not covered by the directive when they occur on a *private* network. Indeed, the directive covers services on a *public* network, because of its link with the electronic communications framework and the definition of electronic communication services therein.[18] Finally, on **unsolicited direct marketing communications**, the report concluded that Member States successfully transposed Article 13 of the directive, leading to the prohibition of automated calling and communications systems for direct marketing without prior consent. Other forms of direct marketing may still be treated differently at the national level, and in fact some countries have chosen an opt-out regime for such cases, while others favoured an opt-in approach in their legislation.

The findings of the report led to a series of recommendations on each of the five issues, as summarised in Table 1 below.

Table 1: Recommendations on selected issues

Issue	Recommendation
Scope of application	Amend Art. 3 and make it applicable to the processing of personal data 'in connection with the provision of publicly available services *in public or publicly accessible private communications networks* in the Union'.
Confidentiality	Amend Art. 5(1) and make it applicable to the 'confidentiality of communications and the related use of traffic data by means of a *public or publicly accessible private communications network'*. Clarify the scope of Art. 5(2) on 'business exceptions' to ensure uniform transposition and implementation across the EU.
Cookies & similar techniques	Reformulate existing exceptions to Art. 5(3) to increase clarity and insert additional exceptions. Include requirements for 'specific, active and prior consent in all cases where cookies or similar techniques are used for direct marketing purposes'.
Traffic & location data	Minor modifications to article 6(1) and 9(1) to ensure their applicability to all services provided through public and publicly available private communication networks, in line with the modification suggested for Art. 3 above.
Unsolicited direct marketing communications	Align Art. 13 with the modifications suggested above for Art. 3 so that the opt-in rule foreseen in Art. 13 applies to email messages transmitted via information society services. Maintain Member States' freedom of choice between opt-in & opt-out for direct marketing messages.
Links with the GDPR	Transform the ePrivacy Directive into a regulation.

Source: Author's elaboration on basis of SMART 2013/0071, pp. 7-18.

REFIT evaluation of the directive

As indicated in the Commission's inception impact assessment announcing the revision of the directive, the assessment of other elements not covered by the above report were addressed in a separate REFIT evaluation.[19] The latter was carried out in parallel with the impact assessment and both documents were published together with the proposal on 10 January 2017.

The evidence collected for the REFIT evaluation covers the EU28 and the timeframe 2009-2016.[20] In line with the Commission's Better Regulation Guidelines, the report addresses the five **evaluation criteria** of efficiency,

[16] Namely 'data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'. See glossary, Annex 14 of SWD (2017)3.

[17] This refers to 'any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service', SWD (2017)3, Annex 14.

[18] This may also lead to ambiguous situations: for instance, the report cites the case of free wi-fi in airports. Should it be considered as public or private?

[19] European Commission, SWD(2017)5. Note that the REFIT evaluation drew, among others, on two additional external studies: Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080) and ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019). The quantitative estimations provided in Deloitte (2016) are available in the impact assessment SWD (2017)3, Annex 8, accompanying the new proposal.

[20] As mentioned, 2009 is the date of the last revision of the directive. When available and relevant, the evaluation also used older data.

effectiveness, relevance, coherence and EU added value applied to five main areas of the directive: 1) the security of electronic communications; 2) the confidentiality of communications and related traffic data; 3) the confidentiality of information stored in terminal equipment; 4) the protection of users against unsolicited communications, and 5) other provisions ensuring users' privacy and the protection of subscribers' legitimate interests.[21]

In addition, the evaluation discussed **two horizontal questions** (the scope of the directive and the choice of competent authorities) that have direct implications for its effectiveness in meeting the intended goals set out by the legislator. On these two points, the REFIT evaluation concluded that basing the directive on the definition of electronic communications services resulted in **too narrow and/or outdated a scope**. In addition, the current scope was found to be ambiguous and potentially leading to **legal uncertainty**. This situation has ultimately hampered the effectiveness of the legislation. Problems were also linked to the directive's failure to designate which national law is applicable, particularly in cross-border situations; and to the allocation of enforcement competences to different authorities between, and often within, Member States.

Turning to the areas covered by the evaluation questions, the requirements on the **security of electronic communications** (Article 4) were found to be still relevant and 'an essential precondition' to meet the directive's objectives, also in light of the increasing number of security incidents affecting users' privacy. As similar provisions have been included in other legislative acts, such as the GDPR, the evaluation came to the conclusion that **some parts of the ePrivacy Directive have become redundant**. Reportedly, Article 4 has been only partially effective, despite the improvements brought by the 2009 revision of the directive. Yet, the current formulation of the article leaves areas of uncertainty, for instance as regards the type of security risks that are covered by the obligation to inform subscribers, and on the possible mitigating measures to be adopted in such cases. This has led **to varying degrees and modes of implementation** of the requirement by EU Member States. Such a result could not be attributed to failed or incomplete transposition, but rather appeared as a question of clarity of the text.

Public authorities also claimed **difficulties in enforcing the data breach notification requirement**, a finding that seems to be corroborated by the relatively low number of reported breaches in the Member States covered by one of the supporting studies.[22] In terms of coherence, the evaluation noted that the recent adoption of the GDPR and its provisions on data breach notifications (Articles 33 and 34) could lead to two different approaches if the ePrivacy Directive is not amended. As the approach introduced by the GDPR seems to be more effective, the evaluation concluded that only Article 4(2) of the ePrivacy Directive remained relevant as it is not covered by other legislative instruments. This overlap was also noted when assessing the efficiency of Article 4, which was deemed one of the more costly provisions of the directive. Finally, while the EU added value of having provisions on personal data breaches was confirmed, particularly in cross-border situations, the evaluation found once again that the relevant GDPR provisions would be sufficient.

On the **confidentiality of communications and related traffic data** (Articles 5(1), 6 and 9), the evaluation confirmed the relevance of these provisions, as they do not feature in other EU acts. This was also supported by the evaluation's conclusion on the coherence of those provisions with the rest of the EU *acquis*. However, it appeared that the directive has **not been entirely effective in ensuring confidentiality**. These results could be explained by various factors, including some issues with the wording and the implementation of Art. 5(1) and the fact that some provisions were rendered somewhat obsolete by the evolution of the electronic communications sector. In addition, diverging national approaches as regards the treatment of content and traffic data persist. Moreover, the fact that the directive does not currently apply to OTTs has undermined its actual level of protection and resulted in an 'uneven playing field' between market players. Finally, the possibility for Member States to derogate from the directive for national security reasons was exploited differently across the EU, resulting in a certain degree of fragmentation.

[21] SWD (2017) 5, section 3 and p. 22.
[22] SWD (2017) 5, p. 27-28 on Deloitte (2016) p. 68.

A lack of quantitative evidence, a problem that was noted throughout the evaluation, did not allow to draw definite conclusions on the efficiency of these articles. Views on efficiency diverged between consumers and industry representatives, as will be explained in Section 4 of this briefing. The evaluation **confirmed the EU added value** of provisions on the confidentiality of communications and related traffic data, not only because of the increasingly cross-border dimension of communications, but also because of the **benefits in terms of harmonisation of concepts and definitions** (e.g. traffic and location data) brought about by the directive.

The relevance of requirements on the **confidentiality of information stored in terminal equipment** (Article 5(3)) was supported by the evaluation, even though the Article was found to be over-inclusive as it also covers practices that are not privacy-invasive. Its EU added value remained uncontested and its coherence with the GDPR was also highlighted. Conversely, the effectiveness of the provision appeared to have been undermined by several of the reasons already mentioned elsewhere in this briefing, namely an excessive use of cookies leading to fatigue and automated consent by users, and the phenomenon of 'cookie walls': a take-it-or-leave-it approach that prevents users from accessing a website if they refuse cookies. Moreover, as with other provisions, differences in implementation and enforcement between Member States negatively impacted on effectiveness. Finally, quantitative estimates found that complying with the requirements of Article 5(3) could cost around €300 per website per year, leading to an overall EU-wide compliance cost estimate of €1.8 billion for 2015.[23] The evaluation indicated that more efficient ways to comply with the directive could be found.

On the **protection against unsolicited communications** (Article 13), the evaluation explained that the cost of such practices has decreased in recent years, thus potentially increasing the magnitude of the problem and confirming the relevance of the provision. Yet, **views differed among stakeholders on the type of protection to be provided by the directive**. On the one hand, collected evidence pointed to a partial effectiveness of Article 13, as testified by the high number of nuisance calls reported by citizens to the competent authorities in each country. On the other hand, industry representatives consulted for the evaluation and the underlying studies reported difficulties both in understanding and implementing the relevant provisions. Here again, fragmentation and legal uncertainty across the EU was also noted, due to the different implementation modalities followed by Member States. Assessing efficiency in quantitative terms proved difficult. It is important to note, however, that from the perspective of businesses, the costs generated by Article 13 are essentially opportunity costs, stemming from the loss of marketing and sales. The EU added value of the provisions was acknowledged. Finally, the evaluation found complementarities between Article 13 and the GDPR, the eCommerce Directive 2000/31 and the Consumer Rights Directive 2011/83, thus indicating a coherence between different legislative acts on this point.

Finally, **other provisions,** such as the right to receive non-itemised bills (Article 7) and the right to decide whether to be included in a public directory (Article 12), were considered relevant by citizens and civil society, while industry took the opposing view, calling for their repeal or their adaptation to technological change. The evaluation also found that overall these other provisions **had been effective in achieving their intended objectives and brought EU added value**. Assessing the efficiency of such requirements proved to be difficult, due to a lack of quantitative data. The evaluation also came to the conclusion that there is a general coherence between the provisions in question and other relevant areas of the EU *acquis*.

3. European Parliament position/MEP questions

3.1 European Parliament resolutions

European Parliament resolution of 19 January 2016 - Towards a Digital Single Market Act

In stressing the importance of complying with fundamental rights, and in particular of data protection legislation, the European Parliament called for a revision of Directive 2002/58 to 'to ensure the consistency of its provisions with the data protection package by the time the package enters into force' (May 2018). It

[23] SWD (2017)5, p. 47.

also recalled how episodes of electronic mass surveillance have eroded citizens' trust in digital services and the effective respect of their privacy, underlining once again the importance of 'strict compliance with existing data protection legislation... when processing personal data for commercial or law enforcement purposes'. Parliament recalled that citizens' and businesses' trust in the digital environment is a cornerstone for future innovation and growth, and for establishing a competitive digital single market.

In its follow-up to the resolution, the European Commission confirmed that it had already started the review process of the ePrivacy Directive. It also indicated its initial intention of adopting a proposal by the end of 2016. In terms of content, the Commission stated that it would also take into account the importance of encryption as a means to protect users' privacy and security in electronic communications as emphasised in Parliament's resolution.

3.2 Written questions by Members of the European Parliament

Written question by Morten Messerschmidt (ECR, Denmark), 15 April 2016

In referring to Article 5(3) of the ePrivacy Directive on prior informed consent for storage of or access to information stored on a user's terminal equipment, the Member noted that it would be time to assess whether the legislation has met its intended objective and if it is proportionate in terms of burdens for users. On the one hand, users are irritated by constant requests to authorize 'cookies'; on the other hand, approval is often given without a complete awareness of the consequences, and thus does not increase security. He therefore wanted to know whether the European Commission would be prepared to remove this specific provision which appears to create more burdens than benefits.

Answer given by Günther Oettinger on behalf of the Commission, 14 June 2016

The Commissioner recalled that consent is not necessary for 'technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'. He also noted that it is often possible to give consent only once for a given website or for users to set a preferred approach on their browser. However, he also recalled that the Article 29 Working Party found that many websites still use unnecessary cookies, often with the primary purpose of tracking users and building profiles of their lives/habits. He indicated that these questions were being explored in the public consultation and evaluation supporting a revision of Directive 2002/58.

Written question by Santiago Fisas Ayxelà (EPP, Spain), 27 April 2016

Some websites increasingly prevent users who have installed pop-up blockers on their computers from accessing content. The Member noted that the actual mechanisms to prevent such access to content may be contrary to Article 5(3) of the ePrivacy Directive, as they do not require users' express consent.[24] He thus wanted to know how the Commission was planning to guarantee users' privacy when those practices are at stake, and enquired about the possibility of finding a balance between the protection of users and the 'viability of websites from an advertising point of view'.

Answer given by Günther Oettinger on behalf of the Commission, 8 July 2016

The Commissioner explained that the technology used by websites to identify the presence of pop-up blockers determines whether Article 5(3) of Directive 2002/58 applies to a given situation. He also recalled that the supervision and enforcement of existing legislation is in the hands of national supervisory authorities and courts, including the assessment of whether the directive's provision apply to pop-up blockers detection mechanisms used by websites. He also indicated that the recently adopted General Data Protection Regulation is expected to further boost user's trust in digital services. Finally, he noted that the performance of the ePrivacy Directive was being evaluated in terms of efficiency and effectiveness, including the assessment of its costs and benefits.

Written question by Kathleen Van Brempt (S&D, Belgium), 13 April 2015

A report commissioned by the Belgian Privacy Commission found that Facebook recorded the internet use of

[24] Note that concerns over the obligation to accept cookies to access a website, and more broadly on access to personal (including traffic and location) information, were also expressed in some of the questions received by the European Parliament's Citizens Enquiries Unit (AskEP) in the last two years.

individuals who did not use its services and did not even visit the social media website. This practice occurred without their knowledge or consent. Hence, the Member wanted to know whether the European Commission was aware of 'the use of long-term, identifying cookies to track non-registered users' and whether this contravened the ePrivacy Directive. She also asked which actions the Commission was planning in order to counter the unlawful tracking of users and ensure awareness of third-party tracking among internet users.

Answer given by Günther Oettinger on behalf of the Commission, 7 July 2015

The Commissioner confirmed the Commission's awareness of the practice cited by the Member and recalled that uses of cookies to track users should be in line with the national measures implementing the ePrivacy Directive, and in particular the 2009 revision of Article 5(3) on users' informed consent. He also recalled that the competence to enforce those rules falls under the remit of the Member States. Competent national authorities, with their investigation powers, are thus the appropriate venue for affected users to share their concerns. Finally, he noted that the Commission supported industry's efforts in increasing awareness among users of their rights under Directive 2002/58 through systems such as Do Not Track (DNT) or the use of dialogue boxes providing information on cookies and various mechanisms to seek consent.

4. European Commission public consultations

Eurobarometer survey on ePrivacy

At the request of the European Commission, nearly 27 000 EU citizens were contacted for a survey on the protection of their privacy during the summer of 2016.[25] The survey questions revolved around the following issues: citizens' use of communications technologies; the importance they attribute to the protection of privacy online and to the secrecy of their communications; the type of steps citizens undertake to protect their privacy online; knowledge of existing legislation; and attitudes to unsolicited communications by email or through marketing calls.

The survey showed that over 70 % of the interviewed citizens call and send text messages through mobile phones on a daily or almost daily basis, and browse the internet (60 %) and use emails (46 %) with the same frequency. Use of instant messaging over the internet on a weekly basis was reported by half of the respondents. Only 8 % reported a daily use of the Internet for phone and video calls.[26]

As regards citizens' familiarity with existing legal provisions on ePrivacy, the majority (67 %) appeared to be aware of the fact that personal information, such as photos and call history, stored on their devices can only be accessed with their consent, and 58 % of respondents were also aware of the rules on the storage of information (such as cookies) on their devices without permission. It is worth noting that awareness on this second point exhibited higher levels of variation between Member States than the previous question. Conversely, only 37 % knew that instant messaging and online voice conversation are not systematically confidential, and as many as 58 % erroneously believed that these communications can never be accessed without their permission. While answers provided to this question showed geographic differences in awareness, socio-demographic analysis did not appear to have had an influence on the level of respondents' knowledge.

The survey results also showed widespread support for the confidentiality of personal information, emails and instant messaging and indicated that 65 % of respondents took active steps to increase privacy, such as changing privacy settings on their devices and avoiding certain websites so as not to be monitored.[27] These active steps were more widespread among respondents aged 15-39 and among those with the highest education levels. Nearly 70 % fully supported the view that default settings on browsers 'should stop ...information from being shared', and another 65 % were fully in favour of calls and messages encryption so

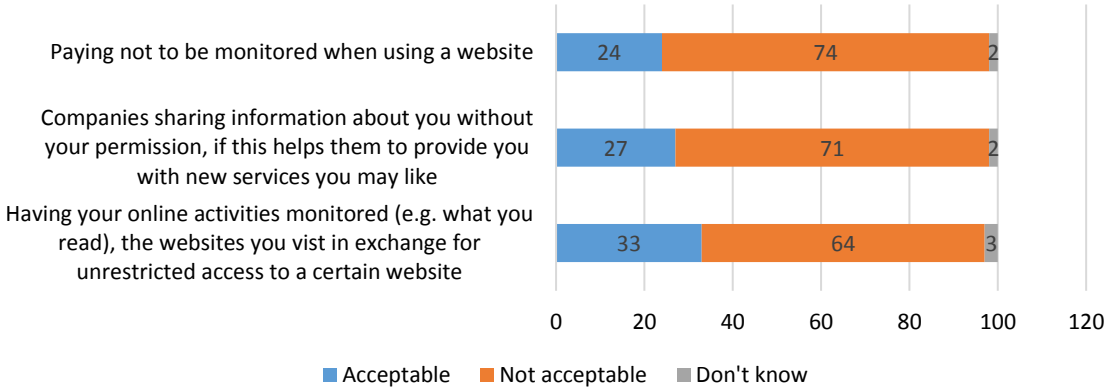
[25] Flash Eurobarometer 443, July 2016.

[26] For the distribution of survey answers per Member State, age category and level of education, as well as data on the use of social networks, fixed phone lines, etc., see Eurobarometer 443, pp. 8-21.

[27] In all Member States, only a minority of respondents reported using specific software to prevent seeing online adverts or to prevent their online activities from being tracked, Eurobarometer 443, pp. 39-40.

that communications are accessible only to the intended recipient. Opinions varied on the preferred frequency of requests by websites to access users' information. Finally, 60 % of respondents indicated that they received too high a number of unsolicited commercial calls and supported the option that this type of calls should always display a specific type of prefix. Support for this option was higher the longer respondents were in education. The survey also sought feedback on the acceptability of a series of scenarios, as illustrated in the figure below. Support for the last two options varied between Member States and was lower the older the respondents.

Figure 1: To what extent do you find each of the following things acceptable (% EU)?



Source: Author's elaboration on Flash Eurobarometer 443 (July 2016), p. 55.

Open public consultation

Between April and July 2016, the European Commission held an open public consultation covering both the evaluation and the intended review of the ePrivacy Directive.[28]

The first part of the **consultation questionnaire** was linked to the REFIT evaluation of the directive and asked about effectiveness in meeting its three main objectives; potential problems in understanding and applying a selection of provisions; and the perceived impact of allocating the competence for the directive to different authorities within the Member States. The questionnaire also covered the directive's relevance, particularly as regards the opportunity of having a specific set of rules on ePrivacy in addition to those contained in other pieces of legislation. It also explored coherence with specific articles in other EU acts and the directive's EU added value. As explained above in the section on the REFIT evaluation, the consultation also aimed at gathering qualitative and quantitative evidence on the costs and benefits of the directive to assess its efficiency. The second half of the questionnaire took a more forward looking perspective, asking about the priorities that any future instrument covering privacy and data protection issues in electronic communications should set; the desirability of replacing the directive with a regulation and of broadening its scope. It also explored stakeholders' views on various approaches to strengthen the security and confidentiality of communications, and to improve users' experience with cookies; on existing exemptions to consent for processing traffic and location data; and on opt-in versus opt-out regimes for unsolicited marketing communications. It concluded with a series of questions on fragmented implementation and inconsistent enforcement.

The consultation received **421 responses** from various categories of stakeholders including citizens (39 %), industry representatives (44 %), public authorities (10 %) and civil society and consumer associations (8 %). In terms of geographical distribution, 26 % of responses came from Germany, followed by the United Kingdom (14 %), Belgium (10 %) and France (7 %). It is fair to say that the responses received[29] could be

[28] In parallel, the Commission conducted additional consultation activities through the REFIT Platform, the Article 29 Working Party, the Consumer Protection Cooperation Network, and two workshops with stakeholders. The results of these activities are reported in SWD (2017) 3, Annex 3.

[29] All contributions, divided per type of respondent can be accessed here.

roughly divided among three groups (citizens, consumer and civil society organisations; industry; and public authorities)[30] holding rather opposing views on the main themes of the consultation. It is worth adding, however, that **these categories are not as uniform as they may initially appear**: for instance, industry stakeholders include both traditional telecommunications operators and OTTs, which hold different positions on key elements of the directive, such as its scope.

As many of the consultation findings were fed directly into the REFIT evaluation described above, this section will focus only on a set of selected issues tackled by the consultation. Starting with the **five criteria covered by the evaluation**, the vast majority of citizens, consumer and civil society organisations did not deem the current version of the directive to be effective in ensuring a full protection of privacy and confidentiality of communications; they cited its limited scope of application and the lack of real choice when it comes to cookies as some of the reasons for reaching this conclusion. On the industry side, electronic communications services players sided with citizens on this point, while 57 % of industry respondents found the directive to be effective. Public authorities also held similar, more favourable opinions.

Citizens and civil society representatives widely confirmed the relevance of having specific rules in the electronic communications sector to achieve privacy and confidentiality objectives. 90 % of public authorities also took this position. Conversely, industry respondents did not see the benefits of having sector-specific regulation, as many of the requirements of the ePrivacy Directive could be covered by the GDPR or other legislative frameworks.[31] Feedback from citizens and civil society was relatively limited on the directive's coherence with other legislative instruments. Industry instead reported a higher level of coherence between the ePrivacy Directive and the GDPR, the Framework Directive on electronic communications and the Directive on security of network and information systems (NIS Directive). Public authorities also responded along these lines. As mentioned above, obtaining quantitative information to assess the directive's efficiency proved to be difficult. While on the one hand, many industry respondents indicated that compliance costs generated by the directive were significant (62 %) or moderate (21 %) and generally disproportionate; citizens, consumers and civil society representatives (57 %) found them to be proportionate to its goals, as did public authorities (73 %). However, there was a general agreement among citizens and industry players on the fact that the directive and the national provisions implementing it had failed to increase users' trust. Public authorities had a slightly more positive view on this point. Finally, nearly 87 % of citizens, consumer and civil society representatives confirmed the EU added value of the directive; 65 % of public authorities held the same view, while 50 % of industry representatives, with a peak of 60 % among electronic communications providers, disagreed with this statement.

As regards the **forthcoming revision of the directive**, once again views were split between stakeholders. While a detailed analysis would fall outside the scope of this briefing note, comparing (see Table 2 below) how different options for reviewing the current text were ranked by the three categories of respondents is rather telling and worth reporting. The percentage of respondents favouring each option is indicated in brackets.[32]

Concerning the future form of a revised instrument, replacing the current directive with a regulation was supported by citizens, consumers and the civil society (66 %) and by 67 % of public authorities that responded to the consultation. Industry representatives were more in favour of other options, including a repeal of Directive 2002/58 and relying on other pieces of legislation, such as the GDPR.

Finally, there was widespread agreement among citizens, civil society and industry on **streamlining the existing governance structure** and attributing the responsibility for enforcing the directive to a single entity,

[30] This classification is also followed by the European Commission in its full report on the consultation.
[31] Note that some industry respondents, however, believed that some specific rules remained necessary for direct marketing and directories. Full consultation report, p.5.
[32] A more detailed analysis of the various positions summarised here can be found in pages 9-18 of the full consultation report.

with a preference for national data protection authorities. Only 39 % of public authorities agreed with this statement, while 50 % were against this option.[33]

Table 2: ranking of top priorities for revision per main group of respondent

Citizens, consumers & civil society	Industry	Public authorities
Amend rules on confidentiality of communications & terminal equipment (69 %)	Provisions no longer needed (56 %)	Broaden scope to cover OTTs (72 %)
Broaden scope to cover OTTs (63 %)	Broaden scope to cover OTTs (29 %)	Amend rules on unsolicited commercial communications (59 %)
Amend rules on governance (62 %)	Amend rules on unsolicited commercial communications (23 %)	Amend rules on confidentiality (52 %)
Amend rules on unsolicited commercial communications (58 %)	Amend rules on governance (23 %)	Amend provisions on security (41 %)
Amend provisions on security (56 %)	Amend rules on confidentiality of communications & terminal equipment (20 %)	Amend provisions on governance (41 %)
Provisions no longer needed (4 %)	Amend provisions on security (17 %)	Other options (7 %)

Source: Author's elaboration on consultation report, p. 9

5. European Economic and Social Committee

A recently completed study on the ethics of big data[34] undertaken for the European Economic and Social Committee (EESC) addressed the delicate question of how to find a balance between fundamental rights, such as privacy and confidentiality, and the growing economic opportunities offered by big data. The study led to the identification of **five balancing actions** that could be translated into policy. While the recommended actions are closely linked to the GDPR, actions one, two and five could also have clear implications for the areas currently covered by the ePrivacy Directive.

In particular, the first action identified was the creation of an EU Privacy Management Platform: a central EU hub/portal enabling natural persons to control how their personal data are being used. The second action envisaged setting up an Ethical Data Management Protocol in the form of a European certification system that would help identify virtuous market players in the field of data protection. The fifth action touched on digital education to foster a deeper understanding of big data and their implications for individuals. All five actions were submitted to stakeholder consultation, partly to investigate their feasibility. While some suggestions, including the creation of a central hub/portal, were deemed premature or inappropriate in the current context, actions to invest in education and awareness-raising, and the development of a European certification system for companies, received the support of various stakeholders.

6. Conclusions

The technological, economic and social landscape has significantly changed since the adoption of Directive 2002/58 on privacy in electronic communications. In spite of targeted amendments adopted in 2009, the current text of the directive does not entirely reflect recent evolutions in the sector and in consumers' habits. Some of the most notable changes in this respect include the entry of new types of players on the market and the widespread usage of internet-based services, such as instant messaging, with a potential impact on the effectiveness of existing ePrivacy rules. In addition, the adoption of the General Data Protection

[33]Note that these answers hide differences in the rationale for supporting a certain choice and that 21 % of total respondents were in favour of other options not presented above. The latter included repealing the Directive; other respondents instead expressed the concern that concentrating enforcement in the hands of data protection authorities might lead to less attention for 'non privacy values'.

[34] Evodevo srl (2017), The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in EU policy context, study for the EESC. The study will be published in early February on the Committee's website.

Regulation in 2016 has altered the legislative framework on data protection, possibly calling into question the relevance and continued coherence of the ePrivacy Directive with the new legislation.

Evidence collected to evaluate the effectiveness, efficiency, coherence, relevance and EU added value of Directive 2002/58, as well as the feedback gathered by the European Commission through targeted workshops, an online public consultation and a Eurobarometer survey, have confirmed the existence of various challenges. These were also raised during a dedicated conference organised by the European Parliament in 2015.[35] In particular, some of the key provisions of the directive have not been fully effective in delivering the intended levels of confidentiality and protection envisaged by the legislator. This is the case of Article 5(3), for instance, on cookies and other techniques to store and access information on users' equipment, a point that was raised on various occasions also by the Members of the European Parliament. Moreover, it appears that some parts of Directive 2002/58 have become technologically obsolete or that better legal approaches have been adopted in the meantime. Finally, an analysis of the implementation of EU ePrivacy rules in the Member States pointed to various degrees of legal fragmentation, the coexistence of different levels of protection across the EU, and a complex governance structure with responsibilities for implementation and enforcement allocated to different types of authorities, at times even within the same country. Overall, this has contributed to a lack of legal certainty and clarity, and the absence of a level playing field across Europe. On the other hand, the EU added value and the overall relevance of having dedicated provisions protecting privacy and ensuring the practical application of Article 7 of the Charter of Fundamental Rights of the European Union, was repeatedly confirmed. Indeed, a modernisation of the current rules is a central component of the EU's digital single market strategy, and is expected to restore and increase citizens' and businesses' trust in the digital environment.

On 10 January 2017, the European Commission adopted a proposal to repeal Directive 2002/58 and replace it with a regulation to address several of the issues outlined above, to simplify existing rules and to make them future-proof. The co-legislators will now have the task of finding a balance between the various conflicting positions and expectations that have emerged throughout the process leading to the directive's review.

7. Other sources of reference

Carey, P. (2015), Data protection: a practical guide to UK and EU law, Oxford University Press.

Davies, R., Regulating electronic communications: A level playing field for telecoms and OTTs?, Briefing, EPRS, 31 August 2015.

Leith, P. (2015), Privacy in the Information Society - The library of essays on law and privacy, Volume II, Aldershot, Ashgate Publishing Group.

Luzak, J. (2013), 'Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies' 21 European Review of Private Law, Issue 1, pp. 221–245.

REFIT Platform, Opinion on the submission by the Danish Business Forum on the E-Privacy directive and the current rules related to 'cookies', 27-28 June 2016.

To contact the Policy Cycle Unit, please e-mail: EPRS-PolicyCycle@ep.europa.eu

Manuscript completed in January 2017. Brussels © European Union, 2017.

www.europarl.europa.eu/thinktank (Internet) – www.epthinktank.eu (blog) – www.eprs.sso.ep.parl.union.eu (Intranet)

[35] Protecting online privacy by enhancing IT security and strengthening EU IT capabilities, High-level conference co-organised by the European Parliament's LIBE Committee and the STOA Panel together with the Luxembourg Presidency, 8 December 2015.