# Briefing
## Initial Appraisal of a European Commission Impact Assessment

April 2017

# Respect for private life and protection of personal data in electronic communications

*Impact Assessment (SWD(2017) 3, SWD(2017) 4 (summary)) of a Commission proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).*

## Background

This note seeks to provide an initial analysis of the strengths and weaknesses of the European Commission's Impact Assessment (IA) accompanying the above proposal, submitted on 10 January 2017 and referred to Parliament's Committee on Civil Liberties, Justice and Home Affairs. The proposal aims to amend the existing legal framework on privacy in electronic communications in order to adapt it to technological novelties, as well as to make it less burdensome for businesses and clearer for EU citizens. The proposal is linked to the digital single market (DSM) strategy.

Currently, the two main legislative acts on data protection and privacy rights are either coming to a close (as is the case with the Data Protection Directive 95/46/EC, to be replaced by the General Data Protection Regulation (GDPR) as of May 2018) or under review (as is the case with the e-Privacy Directive (ePD), which was adopted in 2002 and last revised in 2009). The ePD mainly covers forms of electronic communications supplied by electronic communication services (ECS) providers, i.e. phone calls, voice and text messages.[1] Moreover, the ePD regulates storage of (and access to) 'cookies'[2] saved in users' devices. Within the current legal framework, some new services providers, which are comparable to ECS, are not subject to the ECS protection requirements. This is the case with 'over-the top' services (OTTs), i.e. services provided by other, non-telecom providers (for example, WhatsApp or Skype)[3], which do not control communications directly, but supply communication services through applications relying on the user's internet connection. Therefore, OTTs are not obliged to guarantee the

[1] According to Directive 2002/21/EC, '"electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'.

[2] According to the IA, a cookie is defined as 'information saved by the user's web browser, the software program used to visit the web. When visiting a website, the site might store cookies to recognise the user's device in the future when he comes back on the page. By keeping track of a user over time, cookies can be used to customize a user's browsing experience, or to deliver targeted ads. First-party cookies are placed by the website visited to make experience on the web more efficient. For example, they help sites remember items in the user shopping cart or his log-in name. Third-party cookies are placed by someone other than the site one is visiting (e.g. an advertising network to deliver ads to the online user) for instance in the browser of the visitor with the purpose to monitor his/her behaviour over time'.

[3] OTTs are services that allow communication which bypasses the traditional content distribution system. They take their name from the way in which communication is ensured, as it goes 'over the internet' without the need for an operator of multiple cable or direct-broadcast satellite television systems. Therefore, communication takes place between members of the application providing the service via voice, video, text and data.


Author: Vadim Kononenko with Rosario Parise
**Ex-Ante Impact Assessment Unit**
PE 598.616

same level of data protection as traditional electronic communications services as they are not covered by the ePD. The main differences between these services are presented in the table below.

The Commission included the review of the ePD in its communication of 6 May 2015 on a digital single market strategy for Europe. The reassessment of the legislation on privacy in electronic communications is part of a broader reform of the telecom framework, a set of rules on electronic communications including also the ePD.[4] In January 2017, the European Commission issued an ex-post REFIT evaluation of the ePrivacy Directive, which pointed out the shortcomings of the current legislation. The impact assessment reviewed in this initial appraisal draws on the main conclusions of the REFIT evaluation and discusses the policy options with regard to a possible reform of the EU's data protection regulation on electronic communications.

## Problem definition

The IA identifies three main problems: 1) insufficient protection of citizens' private lives in online communications; 2) lack of effective safeguards against unsolicited marketing; 3) difficulties for economic operators in interpreting legislation due to differing transposition of the ePD across Member States and unclear or obsolete legislation (IA pp.6-11).

The IA also specifies several problem drivers. It highlights in particular the lack of technological neutrality of the ePD, i.e. insufficient adaptation of the current legal framework to new technological and market developments (IA, pp. 6-11 and Annex 4); a vague and fragmented legal framework which, according to the REFIT evaluation and the IA, is created by the overlap of some provisions of the current ePD and the Data Protection Directive/GDPR; and poor and inconsistent enforcement of rules as a result of the allocation of competences to multiple enforcement authorities at Member State level, which tend to overlap.

## Objectives of the legislative proposal

The *general* objective of the proposal is 'the achievement of the original objectives[5] of the [current] Directive, taking into account new technological and market developments in the electronic communications sector' (IA, p.19).

The *specific* objectives are: '(1) ensuring effective confidentiality of the electronic communications; (2) ensuring effective protection against unsolicited commercial communication; (3) enhancing harmonization and simplifying/updating the legal framework' (IA p.20). These are in line with the three main problems identified.[6]

Furthermore, seven *operational* objectives are listed, namely to ensure that confidentiality is protected in relation to OTTs, publicly available private networks (WiFi) and Internet of Things (IoT) devices;[7] to ensure user-friendly management of online privacy settings; to enhance transparency requirement; to reduce the number of nuisance calls; to increase transparency of marketing calls; to reduce the number of authorities competent to apply ePrivacy rules in each Member State; and to reduce 'notification fatigue'. The operational objectives are discussed in relation to the preferred option (IA, p.56), as recommended by the better regulation guidelines.

## Range of options considered

The IA considers five policy options, in addition, to the *do-nothing, or baseline scenario* option. The options are briefly summarised below.

**Option 0. Do-nothing.** Under this option, the status quo would be maintained and no policy action would be undertaken.

[4] See Lorna Schrefler, 'Reforming the regulatory framework for electronic communications networks and services', implementation appraisal, EPRS, August 2016.

[5] The Directive aims to protect the privacy and regulate the processing of personal data in electronic communications field.

[6] See also section 1.3 of the IA.

[7] Also known as 'smart devices', IoT devices are physical objects that have the in-built technology allowing them to transmit and exchange data.

**Option 1. Non-legislative ('soft law') measures.** Under this option, only non-legislative measures would be taken. These would include interpretative communications and other self-regulatory, co-regulatory and awareness-raising initiatives that might help to strengthen and clarify the current legal framework. Recognising that the success of such an option would significantly depend on the extent of stakeholders' concern and willingness to participate in the Commission's initiatives, the IA does not define what specific outcomes these soft measures might produce. Moreover, considering the non-binding nature, the overall impact of this policy option is expected to be limited.

**Option 2. Limited reinforcement of privacy/confidentiality and harmonisation.** This policy option envisages some regulatory changes to the current legal framework, the main aim being to extend to OTTs the legal safeguards currently provided for ECS. According to the Commission's IA, although the extension of the scope of the ePD would address the current regulatory asymmetry between old and new technologies, it would not cover other shortcomings of the current legal framework. Furthermore, the IA report argues that a limited reinforcement of the current framework might not be sufficient to guarantee a more simple and harmonised system.

**Option 3. Measured reinforcement of privacy/confidentiality and harmonisation (preferred option).** This reinforcement would include, inter alia, a new, technology-neutral definition of electronic communications in order to fill the regulatory gap between ECS and OTTs; a stronger protection of confidentiality of terminal equipment,[8] which is currently poorly safeguarded; an opt-in consent system for unsolicited communications (currently existing only in part); and stricter controls on enforcement by national competent authorities. Moreover, this option aims at simplifying the understanding of privacy and consent rules for users, requiring data collection entities to provide clear and concise privacy alerts. Although many new safeguards are introduced by this option, it should be noted that it also provides for a more flexible system, as it repeals existing provisions on security and itemised billing. It also includes additional exceptions to confidentiality of communications by amending the existing ePD provisions on traffic data. According to the IA report, the removal of some provisions of the existing legislation under this option has the aim of simplifying the legal framework and avoiding unnecessary costs for businesses.

**Option 4. Far-reaching reinforcement of privacy/confidentiality and harmonisation.** This policy option includes all major safeguards provided in the previously considered options, and also adds stricter measures, such as a ban on consent mechanism ('cookie walls'). The IA argues that while guaranteeing major protection of confidentiality in electronic communications and reducing legal/interpretative uncertainty, this approach may be economically burdensome and inefficient in terms of compliance and opportunity costs for businesses. Administrative costs would also increase for Member State authorities, as checks on the concrete application of the ban on cookie walls is expected to be resource and time consuming.

**Option 5. Repeal of the ePD.** The repeal of the existing legislation on ePrivacy has been included in the range of policy options as advocated by some stakeholders in the ECS and OTT sectors. According to the IA, many stakeholders argued that the GDPR alone is sufficient to safeguard citizens in electronic communications. Nonetheless, according to the IA, the repeal of the ePD would be a backward step in the legislative path towards better protection of confidentiality of e-communications, being inadequate for guaranteeing the respect of Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) concerning the respect for private and family life, home and communications.

The five policy options appear to be presented in accordance with the requirements set by the Commission in its better regulation (BR) guidelines and the BR toolbox.

[8] According to Art.2(b) of Directive 1999/5/EC, 'telecommunications terminal equipment' is 'a product enabling communication or a relevant component thereof which is intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks (that is to say, telecommunications networks used wholly or partly for the provision of publicly available telecommunications services)'.

## Scope of the impact assessment

The IA considers mainly economic, social and environmental impacts of the options. The economic impacts are considered primarily in terms of compliance and opportunity costs for business. For example, with regard to the preferred option 3, the IA estimates basic compliance costs to be around €900 per website, with 3.7 million websites potentially affected in 2030 (IA, p.37). With regard to social impacts, the IA envisages significant impacts only under options 4 and 5. Under the other three options, the IA report only acknowledges the lack of relevant expected impacts without providing further explanation. This is the case with environmental impacts which are simply stated as 'not to be expected'.

One significant impact considered by the IA concerns fundamental rights, and in particular the respect for private and family life, home and communications (Article 7 of the Charter). Impacts on fundamental rights are considered for each policy option, although the sections dedicated to this specific aspect are sometimes very short (in the case of options 1, 2 and 5, for instance, impact on fundamental rights is dealt with in no more than three to four lines). In option 3, the impact seems to give contrasting outcomes depending on the various e-communication areas: while, on the one hand, this option is generally expected to enhance the confidentiality of communications, on the other, the protection may be weaker than the existing framework because in some cases it would be possible to process data without users' consent.

With regard to the comparison of the policy options, the IA sometimes seems to tend to concentrate more on the benefits and less on the drawbacks of the preferred option 3, at the expense of the remaining four policy options. For instance, in the section dedicated to the impacts of the different policy options (IA, pp.27-47), with regard to option 3, the IA report mentions some possible drawbacks in terms of major safeguards of confidentiality of communications (specific objective 1).[9] According to option 3, indeed, the regulation would provide a 'derogation to the consent rule for the processing of communication data' (IA p.35), which may undermine the full achievement of that specific objective. As stressed in the discussion on the main provisions of the policy options, the elimination of some existing provisions has been envisaged with the aim of reducing unnecessary burdens on businesses. Nonetheless, these burdens have not been thoroughly quantified in the REFIT report and limited information has been gathered.[10] Moreover, in order to limit these possible negative effects, the IA talks about 'strict safeguards, i.e. as approved by competent authorities' (IA p.35), without giving additional comments or further justifications. Considering the importance of specific objective 1, which has the main aim of guaranteeing the respect of Article 7 of the Charter, the explanation given by the IA in this regard could be seen as being too vague and perhaps simplistic.

## Subsidiarity / proportionality

The IA indicates Article 16 TFEU (right to protection of personal data) and Article 114 TFEU (approximation of law in the internal market) as legal bases for the proposed regulation. Furthermore, the protection of communication enshrined in Article 7 of the Charter, and Article 8(1) of the European Convention on the Protection of Human Rights and Fundamental Freedoms (ECHR), are also mentioned and discussed in section 2 of the IA report. With regard to subsidiarity, both the IA and the explanatory memorandum of the proposal stress the need for action at the EU level in order to ensure cohesion within the digital single market and guarantee a 'level playing field for economic operators' as well as 'equal protection of end-users at Union level'.

Proportionality is also justified by the need to extend the safeguards set by the previous legislation to new technologies (OTTs), currently not covered by the ePD. Moreover, starting from the acknowledgement of the poor and fragmented implementation of the ePD, the explanatory memorandum stresses the need for more stringent legislation (regulation). Nonetheless, it also points out that the new regulation would be flexible enough to cater for the needs of individual Member States, as the preferred option would allow for national derogations for legitimate purposes.

[9] For more details, see IA, pp.34-35.
[10] See REFIT report, p.18.

Finally, the explanatory memorandum also specifies that the proposed regulation would impose minimum regulatory burdens on stakeholders, without undermining the fundamental rights concerned. Following the criteria set by the Commission, option 3 seems to present the best combination for strengthening confidentiality whilst minimising the administrative burden for businesses. At the same time, other options (1, 2 and 5) provide for even more significant decrease of regulatory burden. Furthermore, according to the IA, the preferred option actually may have some negative impacts on human rights, even though these impacts apply in specific situations and may be mitigated by other regulatory devices.

No reasoned opinions had been submitted by national parliaments at the time of writing. The deadline for submission is 12 April 2017.

## Budgetary or public finance implications

The explanatory memorandum indicates that there are no budgetary implications for the EU. Nevertheless, the IA highlights that Member States may still incur administrative costs due to the strengthening and simplification of enforcement powers envisaged by the preferred option. These will be mainly running costs and will vary among Member States according to the enforcement mechanism which has been put in place for the ePD.[11]

## SME test / Competitiveness

An external study carried out for the Commission highlights that the share of the micro and small economic operators affected by at least some provision of the ePD is considerable: 2.5 million micro enterprises and 260 000 SMEs, out of 2.8 million businesses, are involved. The IA evaluates the impact of each of the selected options on competitiveness and SMEs in terms of real costs, opportunity costs and compliance costs. Within this context, the IA report shows a trade-off between efficiency and effectiveness of the proposed regulation: the more policy options safeguard the confidentiality of communications, the more they are costly for small and medium-sized economic operators and undermine overall competitiveness. According to the IA, this tendency seems to find an exception in option 3. Indeed, the preferred option is likely to have a specific effect on SMEs according to the type of business: ECS providers are likely to benefit from the new technology-neutral regulation, while OTT providers will probably be subject to setbacks in terms of opportunity costs. While option 5 seems to be the most suitable for SMEs in terms of economic and regulatory burdens, the IA suggests option 3 as a balanced alternative within the aforesaid trade-off (option 5 is deemed insufficient in terms of fundamental rights protection). In addition, the IA report clarifies that, despite some additional costs, the negative impact of option 3 on SMEs would be 'mitigated by the further flexibility introduced in the legal framework through brand-new exceptions and derogations' (IA p. 39).

## Simplification and other regulatory implications

As far as regulatory implications are concerned, it is important to note that the proposed regulation has the main aim of reforming the current ePD, in the form of *lex specialis,* and therefore overriding other pieces of legislation on this issue in case of conflict. In this regard, regulatory simplification is considered with particular attention in the IA as it is linked to one of the main problems (problem 3). According to the IA, the preferred option may actually lead to simplification of the existing legal framework. With particular reference to OTTs, for instance, the preferred option would simplify the current system in two respects. First, the new regulation would cover both ECS and OTTs under the same, technology neutral, definition. This option also appears to be more straightforward than option 2, which would create a level playing field between ECS and OTTs that would not be rooted on a common legal ground. Second, as things stand at the moment, OTTs are actually only disciplined by law in some Member States,[12] while in other countries this issue is not covered. The preferred option, therefore, would create a simpler transnational legal coverage of electronic communication with specific regard to OTTs.

[11] For a more detailed overview of Member State designated authorities, see Annex 11 of the IA.
[12] See, in this regard, Annex 9 of the IA.

## Quality of data, research and analysis

The Commission relied, for the preparation of its IA, on external expertise, mainly based on two studies: SMART 2013/007116 and SMART 2016/0080.[13] While the first study was aimed at analysing the impacts and enforcement of the ePD, examining also the interaction between the latter and a new data protection regulation (which eventually became the GDPR), the second study was mainly focused on the review of the ePD. SMART 2016/0080 assesses in depth the consequences and the points of strength and the weaknesses of the existing legislation, and analyses in detail the impact of every policy option envisaged by the Commission. The data collected are mainly qualitative, but the study quantifies as much as possible the effects of the policy choices on the main stakeholders and their degree of change compared to the status quo.

The overall impression is that the quality of data, research and analysis is high. The main reports on which the Commission relied, and, in particular, the most recent external study on the ePD, seem to be sound, extensive and well structured. As already mentioned, SMART 2016/0080 provides an in-depth analysis of the policy options proposed by the European Commission (over 200 pages describing the baseline scenario, the problem assessments, the relevance and coherence of each option and its impact – calculated both qualitatively and quantitatively – in many policy areas). Furthermore, the structure of the study is fairly rigorous, dedicating a considerable section to the background, broadly discussing the REFIT evaluation and presenting the methodology used to carry out the study and to collect data. Besides the specific studies, *ad hoc* consultations of expert groups have produced important insights. The Eurobarometer surveys used[14] in the IA also provide reliable data for understanding and quantifying key aspects of the IA concerning, for instance, the magnitude of the problem, stakeholders' opinions or citizens' knowledge and perceptions on ePrivacy matters.

## Stakeholder consultation

Annex 3 of the IA describes and discusses the various consultations that took place with regard to the revision of the ePD. An online public consultation was held between 12 April 2016 and 5 July 2016. The consultation collected 421 replies from citizens, civil society and consumer organisations, industry and public bodies (such as Member State data protection authorities and national regulatory authorities). Moreover, *ad hoc* consultations with EU expert groups, as well as seminars and other informal meetings, have also been organised. With regard to Member States, there is no specific mention in Annex 3 of the IA of the number of Member States consulted.

As far as the online public consultations are concerned, questions have been particularly focused on problems 1 and 2, such as direct marketing calls, tracking cookies, the need for special rules for electronic communications and the requirement to cover new communications services. Just one question has been asked on problem 3 (simplification/harmonisation of the current legal framework). This question was aimed at identifying the presence of multiple enforcing authorities in the Member States and did not mention a potential overlap between some provisions of the GDPR and the ePD.

With reference to targeted consultations, two platform groups were established: the REFIT stakeholder group and the REFIT governance group. The first asked for a harmonised approach in the implementation of the rules regarding this issue, with particular focus on cookies and tracking technologies. The second also issued some comments with regard to cookies and, more specifically, on the 'cookie provision', which it considered should be evaluated according to the specific scope of raising citizens' awareness on this topic. Furthermore, the Article 29 Data Protection Working Party, the European Data Protection Supervisor, the Consumer Protection Cooperation Network and the Body of European Regulators for Electronic Communications were also consulted by the Commission and issued specific opinions on the revision of the ePD.

[13] ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation (SMART 2013/007116) and Evaluation and Review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080)

[14] See flash Eurobarometer 443, cited above.

## Monitoring and evaluation

Overall, the IA report's suggestions on monitoring and evaluation appear to be rather vague and general. Six out of the seven indicators are not time-specific, nor are clear oversight responsibilities established at the EU level. Article 28 of the proposed regulation states that an evaluation shall be carried out every three years.

## Commission Regulatory Scrutiny Board

The Commission's Regulatory Scrutiny Board (RSB) examined a draft version of the IA report on 30 September 2016. It issued a positive opinion, with several specific recommendations to be addressed in the final version. These included further elaboration of the baseline scenario, improvement of the analysis of impacts across the options, and a clearer indication of the simplification and burden-reduction elements in the preferred option. The explanatory memorandum of the proposal points out that the final version of the IA has been modified in order to comply with the comments of the Board, with clarifications having been made regarding the scope of the legislative initiative and more details provided concerning the baseline scenario and the estimated costs and benefits of the policy options presented. Moreover, according to the explanatory memorandum, the new IA supplies a more balanced comparison of the various options. In line with the better regulation guidelines, the Commission also explains, in Annex 1 (pp.2-3) of the IA, how the recommendations of the RSB were integrated into the final version.

## Coherence between the Commission's legislative proposal and IA

The legislative proposal seems to be coherent with the recommendations expressed and the preferred option in the IA.

## Conclusions

Overall the IA report makes a good presentation of the Commission's impact assessment work for the legislative proposal. The IA draws on a vast amount of research and expertise in elaborating the policy options and linking them to the main problems. Also, the range of policy options appears comprehensive. However, a more thorough analysis of the social and fundamental rights impacts would have considerably strengthened the report. In particular, as confidentiality remains a sensitive issue in this field, the IA report could have gone into more depth on this issue, especially when comparing the options. In addition, more attention could have been dedicated to developing clearer monitoring and evaluation indicators.

---

*This note, prepared by the Ex-Ante Impact Assessment Unit for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), analyses whether the principal criteria laid down in the Commission's own better regulation guidelines, as well as additional factors identified by the Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal. It is drafted for informational and background purposes to assist the relevant parliamentary committee(s) and Members more widely in their work.*

To contact the Ex-Ante Impact Assessment Unit, please e-mail: EPRS-ImpactAssessment@ep.europa.eu

Manuscript completed in April 2017. 