EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 3 final

PART 1/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

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)

{COM(2017) 10 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

Table of Contents

1. WHAT IS THE PROBLEM AND WHY IS IT A PROBLEM? 4

1.1. Policy Context 4

1.2. Findings of the REFIT evaluation 5

1.3. What are the problems that may require action? 6

1.3.1. **Problem 1:** Citizens' private life when communicating online is not sufficiently and effectively protected 6

1.3.2. **Problem 2:** Citizens are not effectively protected against unsolicited marketing 9

1.3.3. **Problem 3**: Businesses face obstacles created by fragmented legislation and differing legal interpretations across MS as well as unclear and outdated provisions 10

1.4. Problem drivers 11

1.5. Who is affected by the problem and to what extent? 12

1.6. Baseline scenario: how would the problem evolve? 15

2. WHY SHOULD THE EU ACT? 18

3. WHAT SHOULD BE ACHIEVED? 19

3.1. General objectives 19

3.2. Specific objectives 20

4. WHAT ARE THE VARIOUS OPTIONS TO ACHIEVE THE OBJECTIVES? 20

4.1. Option 0: Do-nothing. 20

4.2. Option 1: Non-legislative ("soft law") measures. 21

4.3. Option 2: Limited reinforcement of privacy/confidentiality and harmonisation 22

4.4. Option 3: Measured reinforcement of privacy/confidentiality and harmonisation 23

4.5. Option 4: Far reaching reinforcement of privacy/confidentiality and harmonisation 25

4.6. Option 5: Repeal of the ePD 26

5. WHAT ARE THE IMPACTS OF THE DIFFERENT POLICY OPTIONS AND WHO WILL BE AFFECTED? 27

5.1. Baseline scenario: no policy change 27

5.2. Option 1: Non-legislative ("soft law") measures 27

5.3. Option 2: Limited reinforcement of privacy and harmonisation 30

5.4. Option 3: Measured reinforcement of privacy/confidentiality and harmonisation 34

5.5. Option 4: Far-reaching reinforcement of privacy/confidentiality and harmonisation 42

5.6. Option 5: Repeal of the ePD 44

6. HOW DO THE OPTIONS COMPARE? 47

6.1. Comparison of options 47

6.1.1. Effectiveness 47

6.1.2. Efficiency 48

6.1.3. Coherence 49

6.2. Outcome of the comparison 50

6.2.1. REFIT Dimension of the preferred option: simplification and administrative burden reduction 51

6.3. Choice of legal instrument 54

7. **MONITORING AND EVALUATION** 56

1. WHAT IS THE PROBLEM AND WHY IS IT A PROBLEM?

1.1. Policy Context

The digital economy has been a major driver of growth in the past two decades, and is expected to grow seven times faster than the overall EU GDP in coming years[1]. Information and Communications Technology (ICT) has therefore become the foundation of all modern innovative economic systems.

In the Communication on the Digital Single Market Strategy ("**DSM Communication**")[2], the Commission recognised that the DSM must be built on reliable, trustworthy, high speed, affordable networks and services that safeguard consumers' fundamental rights to privacy and personal data protection while also encouraging innovation.

The **ePrivacy Directive** ("**ePD**")[3] aims at ensuring the protection of privacy and confidentiality in the electronic communications sector and at ensuring the free flow of related personal data and electronic communication equipment and services in the EU. The ePD particularises and complements Directive 95/46/EC on the protection of personal data ("**Directive 95/46**")[4] in relation to the processing of personal data in the electronic communications sector.

The ePD is particularly relevant for electronic communication service providers ("**ECS**") as well as for many companies with a website storing information or accessing information already stored in users' terminal equipment (such as for example "cookies"[5]). A description of the legal and socio economic context of the ePD is provided in **Annex 4**, to which this report refers for essential background information and a better understanding of the present document.

The **reform of the data protection legal framework**, initiated in 2012, is a cornerstone of the digital single market. In April 2016, the European Parliament and the Council adopted the General Data Protection Regulation ("**GDPR**")[6]. Morever, the Commission committed to **review**, once the new EU rules on data protection would be adopted, the **ePD** with a focus on ensuring a high level of protection for data subjects and a level playing field for all market players. The review must ensure consistency with the GDPR.

As a part of the DSM Strategy, the Commission has also undertaken a **review of the electronic communications legal framework** ("**Telecom Framework**")[7]. The ePD has traditionally been part of the Telecom Framework from which it derives essential elements such as some of its key definitions. The review of the ePD should, among others, ensure consistency with the Telecom Framework. The ePD is also closely

[1] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/FI3P%20Fact%20Sheet.pdf
[2] COM(2015) 192, p. 9.
[3] Directive 2002/58/EC, as modified by Directive 2009/136, OJ L 201, 31.07.2002, p. 37.
[4] L 281 , 23/11/1995 P. 0031 – 0050.
[5] A cookie is 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.
[6] Regulation (EU) 2016/679, OJ L 119, 4.5.2016, p. 1–87.
[7] The review aims, among others, to establish a strong, competitive and dynamic telecoms sector which is capable to carry out the necessary investments, to exploit innovations such as Cloud computing, Big Data tools or the Internet of Things.

connected with the Radio Equipment Directive ("**RED**")[8], which lays down detailed rules relating to the marketing of terminal equipment in the EU including an essential requirement for this equipment to incorporate privacy safeguards.

The objectives, scope, main content of the ePD and its relationship with other pieces of legislation such as the GDPR, the Telecom Framework and the RED are set out in **Annex 4**.

1.2. Findings of the REFIT evaluation

The REFIT evaluation has shown that the general and specific objectives of the ePD still remain **relevant** today[9]. **Some rules have become less pertinent** and possibly **outdated** in the light of technological and market developments and changes in the legal framework. This is, for example, the case of the rules on security, which are entirely mirrored in the GDPR, and **itemised billing**, given that they have become obsolete in light of technological and market developments.

By contrast, the REFIT evaluation has emphasised that **several of the ePD rules have shortcomings**. The following specific flaws were highlighted:

- The effectiveness of **confidentiality of communications rules** has been mainly hampered by the incapacity of the rules to anticipate technological changes. Services which are functionally equivalent to ECS[10], such as the so-called over-the top ("**OTT**") services[11], are not subject to the same rules. Therefore, the level of protection varies according to the communication technique utilised.
- As regards the rule on **confidentiality of terminal equipment**[12], which applies to **cookies**, the REFIT evaluation found that consent given online suffers from a number of shortcomings: citizens do not have time to read long and complex privacy statements and find it difficult to understand what consent implies. Moreover, the rule is at the same time over-inclusive, as it also applies to non-intrusive practices (e.g. first party analytics), and under-inclusive, as it does not address new tracking techniques (e.g. device fingerprinting).
- The effectiveness of the rules on **unsolicited communications** has been questioned. The results of the Eurobarometer survey[13] and the sheer number of complaints received by national authorities from MS nationals are strong evidence of a problem in this area.

[8] Directive 2014/53/EC, OJ L 153, 22.5.2014, p. 62–106.

[9] See Commission Staff Working Document, *Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC* ("**REFIT SWD**").

[10] An electronic communication service (ECS) is defined by the current telecom regulatory framework as 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 excludes 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. Under the interpretation offered by the European Court of Justice (ECJ, 7 November 2013, C-518/11 – *UPC Netherland BV*; ECJ 30 April 2014, C-475/12 – *UPC/Nemzeti Média*), ECS cover communication services of providers that bear the responsibility for the conveyance of signals over the underlying electronic communication network vis-à-vis end-users. Being responsible implies that the service provider must have a certain degree of control over the conveyance of signals. Operators of traditional electronic communications services usually also own and run (parts of) the underlying network, which consequently puts them into a "controlling" position.

[11] An over-the-top (OTT) service is essentially a software application that allows communications to be exchanged by and among the members of the application, in the form of voice, text or data communications. OTT providers do not control the transmission of the messages, but rely on end-users' internet connections for the messages to be relayed.

[12] Article 5(3).

[13] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

- **Diverging implementation/interpretations and inconsistent enforcement** of several key provisions also emerged as common issues. This is, at least in part, linked with the current system of enforcement, where MS are free to choose which authorities are competent. This has given rise to a complex situation, with several authorities competent in the same MS. The situation aggravated by the fact that the instrument under consideration is a directive, and not a regulation.

The REFIT evaluation highlighted that most of the costs incurred as a result of the obligations imposed by the ePD in 2002 had been offset or were very difficult to quantify. The REFIT focussed on costs incurred by operators relate to the **cookie consent provision**. A Commission external study estimated that the overall costs of the ePD for businesses operating in the EU through a website using cookies (i.e. around 50% of the total) in the period 2002-2015 has approximately been of EUR 1,861.7 million per year[14]. Overall, the **efficiency** of this rule has been questioned by a number of stakeholders. They complain against the current coverage of this provision. Moreover, some stakeholders complain that cookie banners interfere with users Internet experience by asking repeatedly for consent.

1.3. What are the problems that may require action?

Building on the findings of the REFIT analysis, three main problems have been identified. The first two problems address citizens' protection issues (*effectiveness of the existing rules*), while the third mostly addresses *efficiency* concerns related to limited harmonisation and complexity of the rules.

*1.3.1. **Problem 1:** Citizens' private life when communicating online is not sufficiently and effectively protected*

The confidentiality provision applies only to a portion of today's electronic communications. While it covers the traditional voice and text communications services and Internet access provided by traditional telecommunications companies (the "**ECSs**"), it does not apply to an increasingly relevant and popular portion of software-based online communications (the "**OTTs**")[15]. While, therefore, electronic communications carried by the ECSs can only be processed with the consent of the users, communications carried by means of the so called over-the-top providers can be processed on the basis of the various legal grounds provided by the GDPR, including the necessity for performing a contract and controller's legitimate interest.

The Court of Justice has recognised on various occasions the utmost importance of ensuring effective confidentiality of electronic communications, for example in the *Digital Rights Ireland* case[16], which has led to the invalidation of the Data Retention Directive 2006/24/EC. Article 7 of the Charter provides that everyone has the right to respect for his or her private and family life, home and **communications**. Given the broad and general formulation of the protection afforded to communications under the

[14] Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector* (SMART 2016/0080).
[15] See C-518/1, C-475/12, cited above. See also Commission external study prepared by Ecorys-TNO Study on *Future trends and business models in communication services*, Final Report (SMART 2013/0019). The study concludes that end users regard OTT voice and text services as substitute for voice and SMS services offered by telecom operators. See also CERRE, *Market Definition, Market Power and Regulatory Interaction in Electronic Communications Market*, October 2014, http://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf.
[16] Joined Cases C-293/12 and C-594/12.

Charter provision a different protection of users' fundamental rights on the basis of the technology used is not justified.

Box 1: *OTT and ECS*

Over the past few years, new online players have emerged offering communication services which many users perceive as comparable to traditional electronic communications services such as voice telephony and SMS. These so-called OTTs provide their services in the form of applications running over the internet access service (hence "over-the-top) and are in general not subject to the current EU telecom rules[17].

Traditional electronic communications services, however, clearly fall under the scope of the EU Regulatory Framework, since they incontestably fulfil the definition of "Electronic Communication Services" (ECS), a legal term contained in the Framework Directive (Art. 2(c)).

Under the interpretation offered by the European Court of Justice, ECS covers communication services of providers that bear the responsibility for the conveyance of signals over the underlying electronic communication network vis-à-vis end-users[18]. Being responsible implies that the service provider must have a certain degree of control over the conveyance of signals. Operators of traditional electronic communications services usually also own and run (parts of) the underlying network, which consequently puts them into a "controlling" position.

Conversely, providers of OTT communications services usually do not own or operate any network infrastructure and cannot in principle fully control the signal in the same way, as this is carried over the internet access service on a 'best-effort' basis (unless they negotiate a managed service with network operators)[19].

A very recent Eurobarometer survey[20] shows that in 11 MS, individuals use these services **daily or almost daily**, with particularly high levels in Spain (70%), The Netherlands (61%), Italy (57%) and Germany (51%). At the same time, individuals attach great importance to the confidentiality of information sent or received through these new channels[21]. The public consultation showed that an overwhelming majority of citizens, civil society and public bodies finds that **OTTs should provide the same level of protection when they provide communication services as ECS providers**, while approximately a third of the industry respondents (including ECSs and OTTs) agree with this statement[22]. National data protection authorities[23], BEREC[24] and the EDPS[25] also advocated for **an extension of the scope of the ePD** to OTTs. The International Working Group on Data Protection in Telecommunications reached similar views[26]. This is also the predominant view of citizens according to a recent Eurobarometer survey (92%)[27].

[17] Popular OTTs include Skype, Gmail, WhatsApp, Facebook Messenger, Viber, Telegram, Facetime.
[18] Case C-475/12, cited above, par. 43.
[19] Some of such OTT communications services make use of telephone numbers and can for this reason be considered to fall under the framework, but the point is contested and *de facto* the rules of the framework have not been applied to them. See ERG Common Position on VoIP adopted in December 2007.
[20] SMART 2016/0079, cited above.
[21] SMART 2016/0079, cited above.
[22] Question 17 of the Public Consultation.
[23] Article 29 Working Party, Opinion 03/2016 on the *Evaluation and review of the ePrivacy Directive 2002/58/EC*, WP 240.
[24] BEREC Response to the EC questionnaire on the ePrivacy Directive: http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive
[25] EDPS opinion 5/2016, on the *Review of the ePrivacy Directive* (2002/58/EC), 22.07.2016.
[26] International Working Group on Data Protection in Telecommunications (Berlin Group), Working Paper: *Update on Privacy and Security Issues in Internet Telephony (VoIP) and Related Communication Technologies*, 59th meeting, 24-25 April 2016, Oslo (Norway). In spite of the above, the Eurobarometer survey revealed only a minority (37%) of individuals know that it is false that instant messaging and online voice conversations are confidential and nobody can access them without their permission (SMART 2016/079). This is confirmed by another (less recent) survey showing that data subjects and consumers are not aware of the differences and inconsistencies in data protection standards

Box 2: confidentiality of communications and personal data protection

There are some fundamental differences between the levels of confidentiality of communications guaranteed by the ePD and the data protection legislation:

- *First*, current and future data protection rules allow the processing of personal data under a variety of legal grounds other than consent, including contract, legal obligation, vital interest, public interest and legitimate (private) interest of the data controller;
- *Second*, the ePD rules allow the processing of traffic and location data only if these data have been anonymised or with the consent of the user, to the extent and for the duration necessary for the provision of a value-added service (i.e. consent plus specific purpose limitation); otherwise, in principle, traffic data have to be immediately deleted;
- *Third*, the data protection rules are not engaged if the communications do not contain personal data, e.g. this could be the case for example of an exchange of a technical file by email between two functional or non-personal accounts;
- *Fourth*, data protection rules do not protect, as a rule, the confidentiality of information relating only to legal persons, for instance information such as business secrets or trade negotiations.

In the absence of coverage of OTTs by the ePrivacy rules, they fall under the data protection rules: these differences lead to an inconsistent level of protection between substantially similar services and to a lack of level playing field between competing service providers.

Moreover, the public consultation (including the Eurobarometer) has revealed that citizens are significantly concerned with the confidentiality of their online activities (e.g. Internet browsing). This point is closely related to the widespread usage of **online tracking tools**, such as cookies and location tracking devices which monitor websites visited, timing of the visits, interaction with others, etc.[28] According to a survey, 69% of consumers say that it is not acceptable for service providers to use personal data (e.g. based on cookies) for commercial use[29].

Cookies are widely used today for a variety of technical or commercial purposes, such as online behavioural advertising ("**OBA**") [30]. In the OBA ecosystem, a particular form of "tracking cookies" or other tracking techniques are used in order to profile the user and serve him/her with targeted advertising. When using online services, individuals are associated with technical (online) identifiers which are set by websites or emitted by their devices, applications, tools and protocols[31] and leave traces of their activity at each server they communicate with[32]. **Annex 6** provides the technical explanation of the OBA market.

---

between traditional voice and SMS services on the one hand and OTT voice and messaging services on the other hand; see ComRes, *Digital consumer Survey*, September 2015, https://www.etno.eu/datas/publications/studies/ComRes_ETNO_Final%20Report_LATEST%20FOR%20PUBLICATION.pdf.

[27] SMART 2016/079.

[28] See, e.g., the survey conducted by the Norwegian DPA, *Personal data in exchange for free services: an unhappy relationship?*, https://www.datatilsynet.no/globalassets/global/english/privacy-trends-2016.pdf.

[29] ComRes, *Digital consumer Survey*, cited above.

[30] OBA is an online advertising technique aiming to provide adverts messages to users tailored to their preferences and needs, as determined on the basis of the tracking and profiling of their online activities.

[31] Such as IP or MAC addresses, cookie identifiers, IMEIs and others.

[32] A cookie sweep carried out by the Article 29 Data Protection Working Party (WP29) has shown that the largest majority of websites controlled used third party tracking cookies, that the information provided to users was not sufficient and that cookies have a very long or permanent duration: http://ec.europa.eu/justice/data-protection/article-29/press-material/press release/art29_press_material/2015/20150217__wp29_press_release_on_cookie_sweep_.pdf.

The REFIT evaluation revealed that users are very often not aware that they are being tracked or they have few alternatives to accepting[33]. Cookie policies are often complex, long or unclear. While cookies are probably the most common form of online identifiers used for OBA purposes, it should be noted that they are being replaced or combined today with even more invasive forms of tracking of communications, such as **device fingerprinting**[34]. The main difference between cookies and device fingerprinting is that the latter practice is not visible to users, as it leaves no trace in the device.

The REFIT evaluation identified Wi-Fi tracking as another gap in the protection guaranteed by the ePD. When a Wi-Fi enabled device is switched on, it continually broadcasts unique identifiers called MAC (Media Access Control) addresses. **Wi-Fi (and in a comparable way Bluetooth) tracking** may be used to count people, to track and observe their movements within the area covered by the network, such as airports or shopping malls. This includes the trajectories they follow as well as the time they spend at certain locations[35]. Furthermore, it is not clear in all MS whether the current ePD protects in principle the confidentiality of electronic communications over Wi-Fi networks that are publicly accessible (such as in airports, department stores, etc.). Similarly, it remains unclear to which extent the **electronic communications** of the **Internet of Things**[36] ("**IoT**") is covered by the ePD[37].

*1.3.2. **Problem 2:** Citizens are not effectively protected against unsolicited marketing*

There is evidence showing that the current rules on unsolicited advertising applying to **telephone marketing** have not effectively protected citizens. The Eurobarometer on e-Privacy has shown that a significant majority of responding citizens (61%) believe that they receive too many unsolicited calls offering them goods or services[38]. The percentages of citizens receiving too many communications are particularly high in three large MS, such as UK, Italy and France where it is on average around 75%.

---

[33] Acquisti-Taylor-Wagman point out that consumers' ability to make informed decisions about their privacy is hindered, because most of the time they are in a position of imperfect information regarding when their data is collected, with what purposes, and with what consequences: Acquisti A., Taylor C., Wagman L., *The Economics of Privacy*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411, p. 1. See also survey conducted by the Norwegian DPA, cited above; Kreiken F., Bits of Freedom, *Transparent Consumers*, https://www.edri.org/files/transparent-consumers-bits-of-freedom.pdf.

[34] A **device fingerprint** or machine fingerprint or browser fingerprint is information collected about a remote computing device for the purpose of its identification. Fingerprints can be used to fully or partially identify individual users or devices even when cookies are turned off. It is based on the combination of different sets of information about the user's device, which is isolation are not per se sufficient to identify a machine, but that combined together achieve the degree of entropy necessary that become unique and therefore identifying. According to the WP29, device fingerprinting presents serious data protection concerns for individuals. For example, a number of online services have proposed device fingerprinting as an alternative to HTTP cookies for the purpose of providing analytics or for tracking without the need for consent under Article 5(3) (Opinion 9/2014 on *The application of Directive 2002/58/EC to device fingerprinting*: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf).

[35] See, e.g., Information Commissioner's Office, *Wi-Fi location analytics*, February 2016: https://ico.org.uk/media/for-organisations/documents/1560691/wi-fi-location-analytics-guidance.pdf; Rice S., *Be wary of public Wi-Fi* (ICO Blog), September 2015, https://iconewsblog.wordpress.com/2015/09/25/be-wary-of-public-wi-fi/; Korolov M., IEEE group recommends random MAC addresses for Wi-Fi security, http://www.csoonline.com/article/2945044/cyber-attacks-espionage/ieee-groups-recommends-random-mac-addresses-for-wi-fi-security.html; Hill S., *How Dangerous is Public Wi-Fi? We Ask an Expert*, http://arstechnica.com/tech-policy/2016/06/advertiser-that-tracked-100-million-phone-users-without-consent-pays-950000/.

[36] Based on existing communications technologies like the Internet, the IoT represents the next step towards digitisation where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment (Commission SWD(2016) 110/2 *Advancing the Internet of Things in Europe*, p. 6).

[37] See the findings of the REFIT SWD.

[38] SMART 2016/079.

Available statistics show that the number of nuisance calls in the EU is very high. UK authorities estimate, for example, that each year UK consumers receive around 4.8 billion nuisance calls: 1.7 billion live sales calls, 1.5 billion silent calls, 940 million recorded sales messages, and 200 million abandoned calls[39]. Another recent survey conducted over a selected number of countries around the world showed that the number of people registering to do-not-call lists is constantly increasing[40].

The statistics of complaints in MS against unsolicited advertising (including all means) are impressive. The German Bundesnetzsagentur has received around 60,000 complaints related to spam in 2013, i.e. more than twice as many as in 2012. The majority of these complaints (68%) concerned telephone spam. In the UK, 180,000 complaints reached the various competent authorities in 2014 against nuisance marketing calls and texts. For the 12-month period ending October 2015, the ICO received an average of 14,343 complaints monthly about nuisance calls[41]. Similar figures are available for other major MS (see REFIT SWD). In comparison with the other provisions of the ePD, most competent authorities received the highest number of complaints for Article 13. For example, the Greek Data Protection Authority estimates that around 90% of all complaints received in relation to the ePD relate to unsolicited communications.

Moreover, it should be noted that marketing calls or messages sent using VoIP and over the Internet, provided by OTTs, are not clearly covered by the current rules. The use of VoIP and instant messaging has the potential to lower down even further the cost of direct marketing, thus unsolicited communications sent via these channels will be even easier and cheaper to send while imposing a cost on end-users[42].

*1.3.3. **Problem 3**: Businesses face obstacles created by fragmented legislation and differing legal interpretations across MS as well as unclear and outdated provisions*

First, the REFIT evaluation has shown that **the transposition of the ePD rules took place in a very disperse and different manner**. ECS providers and businesses that operate a website or engage in direct marketing across MS face additional costs related to the fact that the ePrivacy rules are interpreted and applied differently across the MS. This entails additional compliance costs, related for instance to the need to verify whether their practices comply with the different implementing laws and their official interpretations in 28 MS, including the use of professional advice. This differential is a barrier for businesses, especially for SMEs willing to establish or operate in other MS, as they need to face additional compliance costs, such as the cost of legal advice and the cost to verify/adapt their businesses processes. Ultimately, the limited harmonisation discourages companies to invest in new enterprises, start-ups, innovation, which in turn makes the EU less competitive in the digital arena. This constitutes a clear limit to the achievement of the internal market and to the ambitions of the DSM strategy.

---

[39] ICO-OFCOM, *Tackling Nuisance Calls and messages* (December 2015): http://stakeholders.ofcom.org.uk/binaries/consultations/silentcalls/JAP_Update_Dec2015.pdf. A survey conducted on UK customers revealed that more than four in five (86%) of participating UK adults reported experiencing unsolicited communications in the observed period. The majority of the calls (89%) were considered to be annoying by participants across all ages, socio-economic group and working status.

[40] Step Change Debt Charity, *Combating Nuisance Calls and Texts*, by Claire Milne, https://www.stepchange.org/Portals/0/documents/media/reports/additionalreports/Nuisance_Calls_Report_FINAL.pdf.

[41] http://stakeholders.ofcom.org.uk/binaries/consultations/silentcalls/JAP_Update_Dec2015.pdf.

[42] A Commission external study concluded that "*All else being equal, there does not seem to be a valid reason for treating ECS and OCS differently in terms of the applicable rules relating to unsolicited communications and, consequently, for providing a different level of legal protection to end users depending on whether the service qualifies as an ECS or not*"; see SMART 2013/0019, cited above.

Second, some provisions such as those regarding security, itemised billing and automatic call forwarding are considered to be outdated or no longer necessary. The rules on **security** essentially require ECS to take appropriate technical and organisational measures to safeguard the security of its services and to notify personal data breaches. However, almost identical provisions have been included in the GDPR, which will enter into force in 2018, and several rules of the telecom framework (also currently under review) have been reinforced. The provision on itemised billing provides for the right for subscribers to receive **non-itemised bills** (not showing the complete numbers called). However, in view of the penetration of cost flat rates, the increasing use of mobile phones, as well as considering the increase of communications service providers that provide a calling service for free (especially among OTT services relying on the internet for providing voice calls), this provision is considered to be outdated.

Third, under the ePD, ECS can only process such data if they have been made anonymous or with the consent of the users, **to the extent that this is necessary to provide a value-added service**. ECS providers stressed that these provisions are too strict because they essentially prevent them from competing with OTTs in an increasingly remunerative segment of the market (i.e. the OBA market) [43]. This argument finds some support in the findings of a recent Commission external study[44]. The main argument developed in the study is that, should the restrictions related to the provision of a value added service be relaxed, ECS would be enabled to compete with OTT platforms by providing services (free-of-charge) financed by OBA.

1.4. Problem drivers

The REFIT evaluation has shown that the ePD lack of effectiveness results from a series of problems and flaws in the drafting and implementation of the relevant provisions, particularly the lack of sufficient technological neutrality[45]. The following drivers have been identified as the main causes of the problem:

1. Rules ill adapted to technical and market changes: The ePD rules are tailored on traditional telecommunications services, i.e. the prevailing electronic communication technology when the predecessor of the ePD was first enacted in 1997. In order to respond to market developments, in 2002, the rules have been extended to cover Internet service providers and reviewed in 2009 to reinforce the rules on security and unsolicited communications. The lack of technological neutrality is, therefore, one of the causes of the problem affecting the ePD according to the REFIT evaluation. Given technological and market changes (see **Annex 4**), the ePD is no longer able to deal with new forms of communications, which were not foreseen when it was adopted.
2. Issues regarding the current consent rules: the REFIT evaluation has shown that citizens are often not adequately informed about the consequences of their consent online. Cookie policies may be often complex, long and unclear[46]. Given the sheer number and complexity of online privacy policies, users find it difficult to get properly informed or feel have few alternatives to accepting[47]. Numerous sources

[43] See DLA Piper, *Study on the revision of the ePrivacy Directive* (study prepared for ETNO), 2016, https://www.etno.eu/datas/publications/studies/DPTS_Study_DLA_04082016_ePrivacy_Final.pdf.
[44] SMART 2013/0019, cited above.
[45] See REFIT SWD, e.g. p. 20-21.
[46] In some cases, tracking may extend even to the content of our communications as demonstrated by the reported cases of **email scanning**. See, e.g, Gibbs S., *Gmail does scan all emails, new Google terms clarify*: https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify.
[47] See Acquisti A., Taylor C., Wagman, cited above. See also survey conducted by the Norwegian DPA, cited above; Kreiken F., Bits of Freedom, *Transparent Consumers*, cited above.

have, for example, highlighted the limitations of the current notice and consent mechanism in the online environment[48]. Moreover, the consent based rules as formulated in the current ePD have, in some cases, proven to be excessively rigid and therefore unfit to the new realities of online communications. For example, the cookie consent provision lacks the necessary flexibility (e.g. in terms of exceptions) to support technical uses that do not present substantial threat for users' privacy. The REFIT evaluation has shown that it has imposed significant cost on a large number of businesses, without much added value in terms of privacy.

3. Unclear/incoherent rules and their inefficient implementation: the implementation of the ePD requirements has been problematic for a number of reasons, mostly related to the unclear or vague formulation of some of its provisions across MS[49]. Moreover, certain provisions have become unnecessary or redundant because the GDPR will cover the same matters with more general rules. The security rules are a clear example of this risk of overlap. In addition, some provisions give ample margin of manoeuvre to MS, thus leading to fragmentation.

4. Insufficient and inconsistent enforcement: the information collected in the framework of a Commission's external study has shown a low level of enforcement in practically all MS[50]. Moreover, the **effectiveness of the rules in cross-border cases is hampered** due to the allocation of enforcement competences to a wide range of authorities that often overlap. This situation fosters different interpretations across Member States. Finally, there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD. This has made coordination, especially in cross-border cases, particularly difficult.

1.5. Who is affected by the problem and to what extent?

(i) Citizens

Consumers are affected by the limited scope of **confidentiality** obligations when using new communications services. Confidentiality of communications is an essential element of democratic systems and a precondition for other fundamental freedoms[51]. The expansion of mobile broadband connections fostered a rapid growth of OTT services, which is exemplified by some reported numbers: (1) by 2013 Skype had international voice minutes equal to almost 40% of the entire traditional international telecom market; (2) WhatsApp reached 500 million users in 2010 and 1 billion users in 2016; (3) by 2016 Facebook Messenger and WhatsApp carried 60 billion messages a day, i.e. three times more than SMS[52]. This gives indications about the seriousness and the size of the

[48] The Working Party 29, the EDPS and EDRI all underline in their respective opinions on the review of the ePD the limits of current implementation of the cookie consent mechanism (based on "cookie walls") under the ePD: Working Party 29, cited above, p. 16, EDPS, cited above, p. 14; EDRI, *e-Privacy Directive Revision*, https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf. See also SMART 2013/0071; Acquisti-Taylor-Wagman, cited above, p. 41; DLA Piper, cited above, p. 29.

[49] See the REFIT SWD for detailed description of these shortcomings. See also SMART 2013/0071, cited above.

[50] SMART 2013/0071, see in particular the information on enforcement included in the country reports.

[51] On the risks for other fundamental rights, like the freedom of speech and freedom of association, see Van Hoboken J. and Borgesius F., *Scoping Electronic Communication Privacy Rules: Data Services and Values*, JIPITEC, 6, 2015, 198, p. 207-208. Acquisti-Taylor-Wagman, cited above, note, however, that citizens' attitude towards privacy is not uniform as privacy sensitivities may differ greatly across the population, based on subjective feelings, class, status, time, and other contextual factors etc. Moreover, it is not always clear how people value personal data. Therefore, they conclude that there is no unequivocal impact of privacy protection (or of sharing information) on welfare. Depending on the context, privacy protection can either increase or decrease individual as well as societal welfare. Empirical evidence exists both for scenarios in which privacy can slow down innovation or decrease economic growth or where the contrary is true.

[52] Williamson B., *Next Generation communications & the level playing field – what should be done*, June 2016, http://www.ccianet.org/wp-content/uploads/2016/06/Next-Gen-Comm-Level-Playing-Field.pdf.

problem and on the fact that, with the growth of the broadband coverage, the situation will likely worsen if privacy rules are not clarified and reinforced.

According to a Commission external study, the number of EU citizens who in 2015 were affected by the problem(s), i.e. the share of the population using Internet to browse online, is about 390 million[53]. This share is projected to increase and approach virtually the entirety of EU population by 2022. Moreover, confidentiality of emails and online instant messaging is very important for consumers. Eurobarometer data shows that 92% of consumers find this important (72% "very important", 20% "fairly important"). Only 7% of consumers indicate that confidentiality of emails and online instant messaging is not important to them[54].

Citizens consider **unsolicited communications** as an annoying interference with their fundamental right to privacy. A recent UK survey shows, for example, that 80% of marketing calls were perceived as annoying and 5% as distressing. Rather few (12%) were considered as being not a problem and very few were considered useful (1%). Participants who considered calls as being annoying or distressing commonly indicated that this was the case because they had received a lot of nuisance calls already, the call interrupted what they were doing, or there was no reply when answering the phone[55].

The **fragmented implementation** of the ePD rules and the uncertainties surrounding their interpretation directly affect consumers as the scope of their rights is not clear and varies among MS. The existence of several national competent authorities within a MS with responsibility for the ePD makes it more difficult for consumers to file complaints. The responses to the public consultation show that a large majority of citizens and consumers believe that because some MS have allocated enforcement powers to different authorities this has led to significant or moderate divergent interpretation of the rules in the EU and to non-effective enforcement. Of those that have reported significant and moderate problems, the main source of confusion is for citizens.

(ii) Businesses

The fact that the ePD does not apply to OTTs leads to a situation in which services which are regarded by consumers as largely substitutable from a functional standpoint are subject to different legal requirements[56]. A 2016 study prepared by Ecorys and TNO on behalf of the European Commission[57] found that end-users increasingly regard OTTs as substitutes for traditional ECSs. The study also indicates that between 2008 and 2014 fixed and mobile revenues have been declining in the EU by 19% - mainly driven by a decline in traffic related revenues. Similar developments have also been observed in non-EU regions. The impact of OTTs on ECS is clearly observed in mobile revenues. The revenues of the telecommunications sector went down by 10% between 2012 and 2016 (forecasted figure). This trend is confirmed by other market studies[58].

Inconsistent, unclear or outdated regulation across MS makes it burdensome and costly for market players to offer services in multiple countries and creates artificial barriers to market integration. A Commission external study[59] estimates that about 2.8 million businesses were affected by at least some of the ePD rules in 2015. Of these,

[53] SMART 2016-0080, cited above.
[54] SMART 2016/079, cited above.
[55] OFCOM (April 2015): *Landline nuisance calls panel Wave 3* (January-February 2015), http://stakeholders.ofcom.org.uk/binaries/telecoms/nuisance-calls-2015/Nuisance_calls_W3_report.pdf, p. 9.
[56] DLA Piper, cite above.
[57] SMART 213/0019.
[58] See CERRE, cited above, p. 15. See also DLA Piper, p. 11.
[59] SMART 2016/0080, cited above.

approximately 2.5 million were microenterprises (less than 10 employees) and approximately 260,000 were SMEs (10-250 employees). For companies that offer services or sell their products online, cross-border or provide the same service in several MS the lack of harmonisation increases compliance costs, thus preventing them from benefitting from economies of scale.

Particularly relevant is the position of ECSs, as the traditional subjects of the sector-specific regulation. In addition to the compliance costs, these operators also face opportunity costs, as the ePD rules limit their capacity to monetise the value of the data they convey, for example by operating in the OBA markets. The exact size of these opportunity costs cannot be quantified. However, the fact that OBA may be a very important source of revenue for ECS is confirmed by a Commission external study[60]. Also in this direction, a research conducted by a civil society organisation estimated that UK mobile operators could be making over half a billion pounds a year just from monetising the location of their customers[61].

(iii) Public authorities

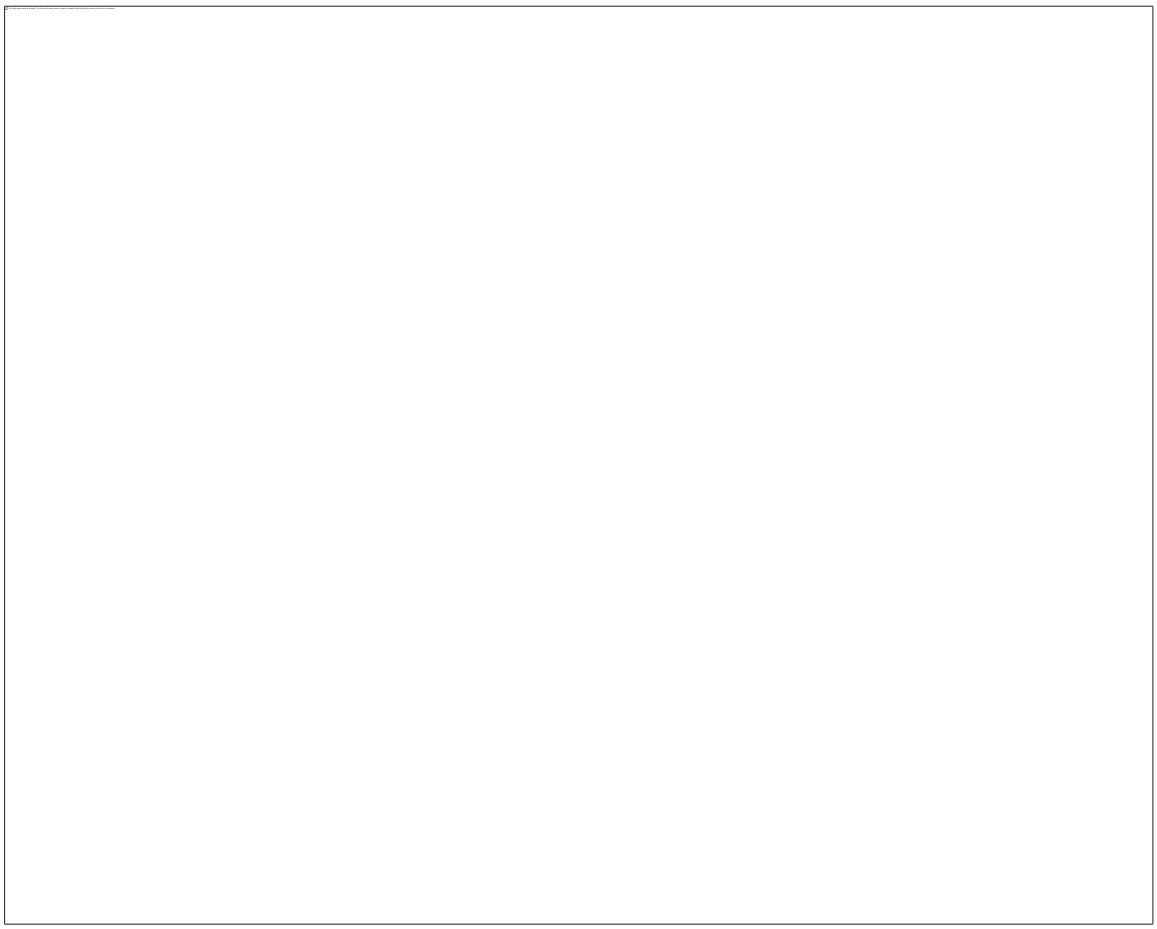
The growing sense of **lack of protection** may reduce the trust of people in the benefits of the digital economy[62]. Public authorities have undertaken considerable investments in making public services accessible online as well as in fostering the digital economy. The potential benefits require citizens' willingness to make use of online offerings.

As to **unsolicited communications**, the impact on public authorities is particularly serious. As the REFIT evaluation showed, the number of complaints from citizens concerning unsolicited advertising is very high. It follows that they have to dedicate substantial resources to this issue, with clear financial consequences in terms of resources allocation. Moreover, some cases may simply not be enforced, for example because of the difficulties related to the lack of sufficient resources compared to the workload of complaints. This may undermine the trust of citizens in the public administration and in the European Union[63].

Public authorities are also affected by unclear provisions and powers (especially in an international context). There may be cases, for example, where multiple authorities are competent to deal with cases, within the same MS or in various MS, whereas economies of scale and scope could be achieved through better coordination. Lack of clarity on jurisdictional issues may lead to the legitimacy of enforcement actions being contested. The case of the Belgian DPA against Facebook illustrates this problem[64].

[60] SMART 2013/0019, cited above.
[61] Open Rights group, *Cashing in on your mobile? How phone companies are exploiting their customers' data*, 2015: https://www.openrightsgroup.org/assets/files/pdfs/reports/mobile-report-2016.pdf. See also Kaye K., *The $24 Billion Data Business That Telcos Don't Want to Talk About*, http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/
[62] See Commission Staff Working Document, *A digital single market strategy for Europe – Analysis and evidence*, SWD (2015) 100 final.
[63] In this context, the UK authority Ofcom explained that the enforcement of Article 13 is challenging. Ofcom highlighted that it is particularly difficult to trace the source of such calls including based on the large number of different sources. For example, during May to October 2015 Ofcom identified nearly 8,000 different telephone numbers as the source of silent and abandoned calls. In some cases, authorities are not able to manage effectively all the workload related to complaints, with the result that either not all complaints are answered on time or some are not answered at all.
[64] Fioretti J, *Facebook wins privacy case against Belgian data protection authority*, http://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV

Figure 1: Problem tree



1.6. Baseline scenario: how would the problem evolve?

The problem relating to **confidentiality** is unlikely to be solved in the absence of intervention. While the most popular OTT operators have consistently made efforts in respect of the protection of privacy and confidentiality (e.g. they largely ask for the consent of their users, have made efforts to improve transparency, enhance users' control, adopted pseudonymisation techniques and end-to-end encryption), these efforts are mostly voluntary and not enforceable. Even *if* the most important players might be considered as already *de facto* complying with confidentiality and the consent rule, respect for fundamental rights cannot be left solely to the good will of the parties concerned. In other words, the obligations relating to fundamental rights must be clearly spelt out in the law and be binding and enforceable vis-à-vis their addressees.

The full implementation of the GDPR would not solve by itself the problems identified[65]. The GDPR will reinforce the notion of consent, inter alia by specifying some clear conditions for the consent to be considered as freely-given[66]. It will also reinforce the

[65] The GDPR was not conceived to replace the ePrivacy rules. Quite to the contrary, it was designed by the EU legislator with the future review of the ePD in mind, as made clear for example in the preamble of this Regulation. Recital 173 of the GDPR read as follows: "*This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à- vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.*"

[66] See Article 7 of the GDPR.

protection of personal data in relation to online services, by among others imposing new obligations on data controllers and creating new rights for data subjects.

However, without action, a growing portion of electronic communications will remain subject to different and less specific rules with regard to confidentiality of communications and terminal equipment. In particular, the asymmetric regulation affecting more strongly the ECS sector will remain an unresolved issue. Moreover, all the issues identified in the REFIT evaluation concerning **unsolicited communications** (see Problem 2) as well as the **lack of clarity, fragmentation and outdated or unnecessary character of some ePD provisions** (see Problem 3) will remain substantially unaddressed. Finally, the coexistence between a general purpose Regulation and a sector specific Directive is likely to raise several consistency issues at national level, since it is not clear whether and under what conditions national laws implementing a directive may specify the provisions of a regulation.

The adoption of standards under the RED provisions would not fill the gap in terms of confidentiality protection between ECS and OTTs. *First*, technical standards under the RED concern the features of the radio equipment and do not, as a rule, apply to OTT communication software applications which are running on them. *Second*, technical standards under the RED can only cover radio equipment and not wire-connected devices. Finally, a number of issues identified in the REFIT evaluation concerning unsolicited communications (see Problem 2) as well as the lack of clarity, fragmentation and outdated or unnecessary character of some ePD provisions (see Problem 3) can obviously not be addressed by RED standards, as such matters clearly fall outside the scope of the that Directive.

Some MS have extended the scope of their national laws to cover explicitly OTTs (see **Annex 9**). However, they represent a minority and it is hard to predict a similar evolution of national legislation regarding the totality of EU MS. In the medium term (5 years) there is therefore a strong risk of growing divergent approaches in the 28 MS. This increasingly fragmented approach would increase business costs, as it does not allow operators to plan centralised privacy policies for the whole of Europe (they instead have to check the laws applicable in 28 MS), create additional obstacles for businesses willing to operate across borders and thus undermine the completion of a Digital Single Market.

Tracking of surfing behaviour is expected to grow more pervasive in the coming years. Current trends in the technical literature show that companies are developing more subtle and latent methods of tracking people's online behaviour, such as for example device fingerprinting, Wi-Fi location tracking, near field communication[67]. Many of these methods differentiate from traditional cookies in the fact that they do not (always) consist in the storing or accessing of information already stored in people's terminal equipment. They are therefore much more difficult to detect as they do not leave traces in the individual's terminal equipment. The consequence could be to reduce trust in the digital economy and reinforce citizens' feeling of being powerless, i.e. not protected by the law.

In the absence of EU intervention, **unsolicited calls** are likely to continue at the current high rate or even increase. The problem of **unclear, fragmented, and outdated provisions** of the framework, moreover, is likely to persist and may worsen, in part because when new technologies and services emerge they lack the harmonisation that was historically required through EU legislation, and may not achieve adequate levels of harmonisation through voluntary standardisation/codes of conduct alone. Moreover, in

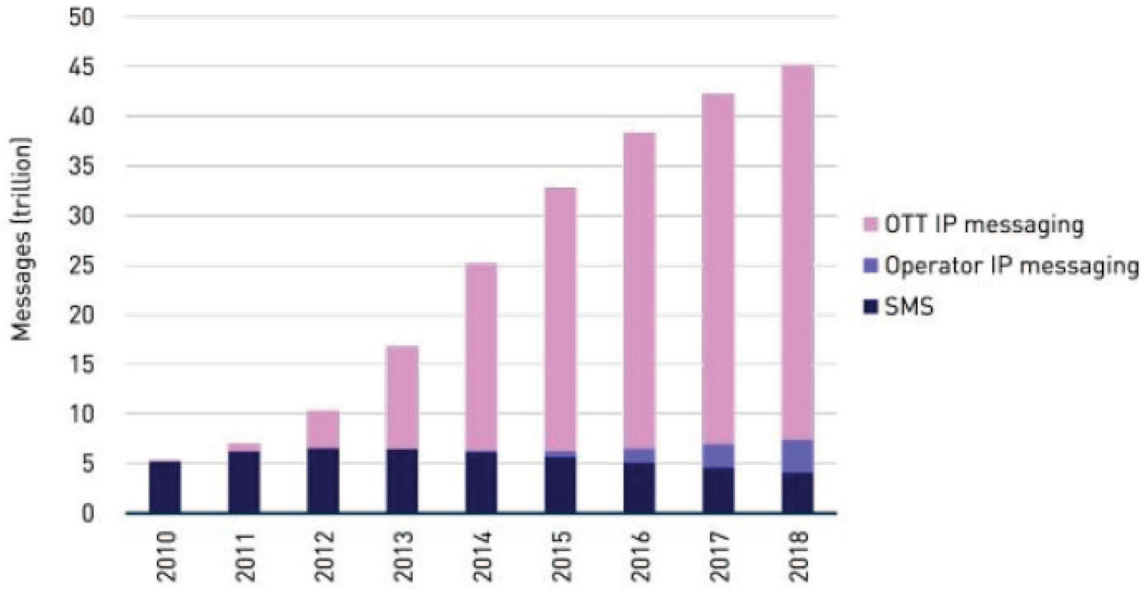
[67] See, e.g. WP29 Opinion 9/2014 on device fingerprinting, cited above.

the absence of a coordination mechanism, authorities will face problems in effectively enforcing the rules consistently at EU level. Lack of consistency with the GDPR would create legal uncertainty and costs for citizens and businesses.

The number of businesses affected by at least some provisions of the ePD is estimated to be growing steadily until 2030, in light of the increasing share of businesses using online communications, such as websites and online platforms. The number of businesses affected is projected to increase from 2.8 million to 3.7 million in 2030. The lion's share of this business will again consist of micro-enterprises (3.3 million)[68]. A Commission's external study calculated that the overall cost of the ePD for businesses operating in the EU through a website using cookies (i.e. around 50% of the total) in the period 2002-2015 has approximately been of EUR 1,861.7 million per year[69]. The increase in the overall number of websites means that the ePD will affect a growing portion of the population.

ECSs are expected to continue to lose ground vis-à-vis OTTs offering competing communication services. Due to the still increasing popularity of smartphones as well as the growing availability of stable mobile broadband services, a study funded by the European Parliament estimates that the usage of OTT communication services will continue to increase significantly in the coming years and would end up reaching a share of 90% of the total messaging market in 2020[70]:

Figure 2: projected evolution of OTT usage



Source: DG for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 31.

The fact that rules on communications services are ill-adapted to technology and market changes also affects **new players in the current value chain** and the future of the Internet of Things. These players may experience some uncertainty about whether or not

[68] SMART 2016/0080, cited above.
[69] SMART 2016/0080, cited above.
[70] European Parliament, Directorate-General for Internal Policies, *Over-the-Top players (OTTs), Study for the IMCO Committee*, 2015, 31, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

they fall within the scope of the framework and this may hinder future planning and investments[71].

2. WHY SHOULD THE EU ACT?

Legal basis

Article 16 and Article **114** of the Treaty on the Functioning of the European Union (TFEU) are the relevant legal bases for the review of the ePD.

Article 16 TFEU reaffirms the right to the protection of personal data, already enshrined in the EU Charter, and introduces a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the MS when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. The GDPR was adopted on this precise legal basis. Since the in most of the cases both components of an electronic communication involving a natural person, i.e. "metadata" and "content", will normally qualify as personal data, the protection of natural persons with regard to the confidentiality of communications and processing of such data, also in view of ensuring the protection of privacy, should be based on Article 16[72].

In addition, the proposal aims at protecting communications and related legitimate interests of legal persons. Article 7 of the Charter contains rights which correspond to those guaranteed by Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("**ECHR**"). In accordance with Article 52(3) of the Charter, Article 7 thereof is to be given the same meaning and the same scope of Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights. Concerning the scope of Article 7 of the Charter as concerns legal persons, case-law of the Court of Justice of the European Union and of the European Court of Human Rights confirm that professional activities of legal persons may not be excluded from the protection of the right guaranteed by both, Article 7 of the Charter and Article 8 of the ECHR.

In line with settled case-law of the Court of Justice of the European Union, other components of the act concerning natural persons that are merely incidental to the main purpose have the effect that the act must be based on a single legal basis, namely that required by the main or predominant purpose, in this case Article 16 TFEU. Since the initiative pursues a twofold purpose and that the component concerning the protection of communications of legal persons and the aim of achieving the internal market for those electronic communications and ensure its functioning in this regard cannot be considered merely incidental, the initiative should, therefore, also be based on Article 114 of the TFEU.

Subsidiarity

The subsidiarity principle requires the assessment of the necessity and the added value of the EU action. The need for EU level legislation on the protection of the right to privacy and confidentiality and the protection of personal data in the electronic communications sector and the free movement of such data and electronic communication equipment and services was already recognized by the European legislator with the adoption of the ePD.

As electronic communications, especially those based on Internet protocols, have a global reach, the dimension of the problem goes well beyond the territory of single MS.

[71] Rathenau Instituut, *Beyond Control, Exploratory study on the disclosure in Silicon Valley about consumer privacy in the Internet of Things*, April 2016, https://www.rathenau.nl/en/publication/beyond-control.
[72] The need for dual legal basis is stressed by the EDPS, cited above, p. 8.

MS cannot effectively solve the problems in the current situation. In order to achieve the internal market in the electronic communications sector, it is necessary to reduce the current fragmentation of national rules and ensure an equivalent level of protection across the whole EU. Moreover, the proper functioning of the internal market requires that the rules ensure a level playing field for economic operators.

The technological developments and the ambitions of the DSM strategy have strengthened the case for action at EU level. The success of the EU DSM depends on how effectively the EU will be on bringing down national silos and barriers and seize the advantages and economies of a truly European digital single market. Moreover, as the Internet and digital technologies know no borders, a level playing field for economic operators and equal protection of users at EU level are requirements for the DSM to work properly.

Respect for communications as a fundamental right recognised in the Charter. It is also in line with the constitutional traditions common to the MS: the majority of MS also recognise the need to protect communications as a distinct constitutional right and usually have a distinct body of national law regulating this area[73]. However, the protection of communications differs widely on scope and content. Whilst it is therefore possible for MS to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of EU rules and would create restrictions on cross-border flows of personal and non-personal data related to the use of electronic communications services to other MS that do not meet the same protection standards.

Finally, in order to maintain consistency with the general data protection rules (GDPR), it is necessary to review the current sector-specific rules on ePrivacy and adopt measures required to bring the two instruments in line.

3. WHAT SHOULD BE ACHIEVED?

Based on the problems identified in section 1, the following policy objectives for the review of the ePD have been established:

3.1. General objectives

The review of the ePD aims at, first of all, completing the achievement of the original objectives of the Directive, taking into account new technological and market developments in the electronic communications sector. These objectives are ensuring an equivalent level of protection of privacy and confidentiality in connection with the processing of personal data in the electronic communications sector and ensuring the free flow of such data and electronic communication equipment and services in the Union.

3.2. Specific objectives

With the general objectives in mind, the review of the ePD intends to achieve the following specific objectives:

1. Ensuring effective confidentiality of electronic communications;
2. Ensuring effective protection against unsolicited commercial communications;
3. Enhancing harmonisation and simplifying/updating the legal framework.

[73] EDPS, cited above, p. 7 and fn 11.

4. WHAT ARE THE VARIOUS OPTIONS TO ACHIEVE THE OBJECTIVES?

The following five policy options were considered to achieve the policy objectives and to remedy the problems identified, on top of the baseline scenario ("Do-nothing"). The first four options identify measures to strengthen confidentiality and privacy in relation to electronic communications ("reinforcing privacy/confidentiality") and to remove the identified barriers for businesses created by fragmented, outdated or unnecessary provisions ("enhancing harmonisation and simplifying"). The measures are presented according to their level of growing ambition (i.e. option 1 is the least ambitious and option 4 is the most ambitious). Policy option 5 considers the option of the repeal of the ePD, as advocated by some stakeholders. To improve the visual understanding of the options, **Annex 12** presents them in a table form. In addition, in that Annex, the various measures are visually grouped in relation to the problems that they intend to address.

All the options would apply to all businesses, irrespective of their size, thus including SMEs. Microenterprises are normally excluded from EU regulations. However, the ePD does not allow a total exclusion of these enterprises in that it is meant to protect a fundamental right recognised under the Charter. Generally speaking, compliance with fundamental rights cannot be made dependent on the size of the businesses concerned. A breach of confidentiality of communications perpetrated by a microenterprise would potentially cause the same harm as one caused by a larger player. Fundamental rights shall be respected by every operators and no fully-fledged derogation is therefore possible for micro-enterprises. Still, mitigation measures were considered and reported in **Annex 7** in relation to the so-called SMEs Test.

4.1. Option 0: Do-nothing.

Under this option, the Commission would maintain the status-quo and not undertake any policy or legislative action. With regard to the three identified problems/objectives, the option would result in the following situation:

Objective 1: *Ensuring effective confidentiality of electronic communications*

1. The ePD has a service/technology based approach (no technological neutrality) and thus applies only to providers of publicly available electronic communications services in public communications networks. OTT communications remain outside the scope of the current ePD and governed solely by the GDPR.
2. It is not clear in every MS whether communications running over publicly available private networks, such as Wi-Fi networks in public spaces (airports, hospitals, malls, etc.) are covered by the principle of confidentiality of communications.
3. It is unclear and subject to national implementing rules and interpretations whether the ePD applies to IoT connected devices.
4. Traffic and location data can be processed only with the consent of the users and to the extent and for the duration necessary for the the provision of value-added services.
5. Privacy and confidentiality of terminal equipment, including in respect of online tracking, are protected only when there is a storing of information, or an access to information already stored, into the users' terminal equipment. Any other interference carried out by other technical means (e.g. certain forms of device fingerprinting) are as a rule not covered.
6. In practical terms, consent online is generally requested by means of banners or pop-up requests every time users visit a website using cookies, irrespective of their privacy intrusiveness.

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

7. Certain forms of unsolicited communications such as emails, SMSs, automated calls, etc., are subject to opt-in consent;

8. An exception for the sending of electronic email is provided where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service (subject to the right to object).
9. For any other forms of unsolicited communications, such as voice-to-voice calls, MS are free to decide whether unsolicited communications should be governed by opt-in consent or a right to object (opt-out consent).

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

10. Several provisions of the ePD are formulated in unclear, broad or un-coherent terms, leaving significant margin of manoeuvre to MS in the implementation and interpretation of such provisions.
11. The issue of applicable law is not regulated and left to varying interpretation across MS.
12. MS are free to appoint several authorities or bodies for enforcing the ePD provisions. The ePD does not provide for an effective system of coordination of national enforcement, especially in cases having a cross-border dimension.
13. The ePD contains rules on security of the personal data with regard to the processing in the electronic communications sector. Such rules include an obligation to notify personal data breaches, partly overlapping with the corresponding rules provided for in other legal instruments such as the GDPR and the Telecom Framework.
14. The ePD provides for specific rules protecting user privacy in relation to itemised billing, calling line identification, automatic call forwarding and directories of subscribers.

4.2. Option 1: Non-legislative ("soft law") measures.

Under this option, the Commission would make extensive use of its implementing powers and use soft policy instruments in order to improve the protection of users. This option would include the measures to address the problems identified in the problem definition, which are listed in the box below. The specific contents of the individual measures cannot be delineated with precision at this stage, as they will emerge as a result of the overall process within the Commission and with the stakeholders.

Objective 1: *Ensuring effective confidentiality of electronic communications*

1. **Increased use of interpretative communications**. The Commission would provide more detailed guidance on the interpretation of certain aspects of the ePD which are unclear or open to different interpretations[74].
2. **Support EU-wide self-regulatory initiatives** building on the existing *ePrivacy acquis* ("co-regulation")[75].
3. **Specify privacy by design requirements of terminal electronic equipment through EU standards**[76].
4. **Research and awareness-raising activities**. The Commission would significantly increase the funds related to R&D projects in the field of online privacy and security by 25%. In addition, it would engage in awareness-raising activities[77].

[74] The subject potentially covered would include 1) the notion of "electronic communications services" and of "publicly available" (clarify, e.g., that the current rules apply to WiFi and IoT devices, which is currently unclear); 2) the cookie provision (clarify, e.g., the extent to which the current rules cover also alternative tracking technologies to cookies); 3) clarify what positive actions constitute consent and the value of consent in situations of economic unbalance.

[75] The Commission would lead and coordinate industry efforts to promote standards and codes of conduct in crucial areas such standard information notices related to the use of location data by ECS providers, online tracking, standardised icons and labels, an EU-wide OBA code of conduct and/or an EU DNT standard.

[76] Article 14(3) and RED.

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

5. **Interpretative communications**, clarifying the interpretation of unclear or ambiguous concepts[78].
6. **Awareness-raising initiatives** instructing citizens on how to defend themselves, how to seek redress from national supervisory authorities.

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

7. Issue **interpretative communications** to promote an application of the current rules, which is business friendly, while preserving the essence of the protection of confidentiality of communications[79].
8. Work closely with **industry** in order to encourage the adoption of **common best practices**[80].
9. **Support MS cooperation** to improve enforcement in cross-border cases as well as harmonised interpretation by organising meetings and workshops with authorities.

4.3. Option 2: Limited reinforcement of privacy/confidentiality and harmonisation

Under this option the Commission would propose minimum changes to the current framework with a view to adjust privacy and confidentiality provisions and to improve harmonisation and simplification of the current rules. In particular, under this Option the Commission would propose the extension of the scope of the ePD to functionally equivalent services (e.g. OTTs) and the extension of the rules on unsolicited marketing to all electronic communications irrespective of the technical means used:

Objective 1: *Ensuring effective confidentiality of electronic communications*

1. **Extension of the scope** of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP. Under this option, OTTs players will be subject to the same rules as ECS providers and thus will be able to process communications data only with the consent of the users. As a consequence, they would no longer be allowed to rely on other legal grounds under the GDPR, such as the legitimate interest of the data controller or the necessity to perform a contract. The rules on calling line identification and automatic call forwarding will be extended to all OTTs using numbers, whereas the provision on directories of subscribers will be extended to all OTTs.
2. Clarify that the ePD applies to **publicly available communications networks**, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. The new instrument would lay down specific rules for the processing of communications data and the tracking of (the usage of the) terminal equipment in such publicly available private networks. Such rules would include the obligation to clearly display information for users[81].
3. Specify that the protection of confidentiality applies to the transmission of information from any machine that is connected to the network (including **M2M communications**, such as for example, a refrigerator connected to a grocery store website). This will imply the following consequences: 1) it will be clarified that the confidentiality obligation covers communications from such connected devices; 2) any interference with the personal devices

[77] Such as setting-up an ad-hoc website and an Internet based advertising campaign, ad-hoc conferences, events (e.g., online communications day) and training for national officials

[78] For example, the issues around the scope of the provision, silent or abandoned calls, the implementation of Robinson lists.

[79] This would cover issues such as the scope of the ePD (e.g., publicly available WiFi networks, IoT devices); modalities to provide consent for tracking, the exceptions to the consent rules under the ePD.

[80] Concerning, for instance, the provision of information and consent mechanisms, thus facilitating a uniform and clear implementation of the current rules.

[81] Working Party 29 Opinion on the ePD review, cited above, p. 8.

connected to the networks, including the storing of information or accessing information already stored into such devices will only be allowed with the user's prior informed consent.

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

4. **Clarify the scope of the provision**: clarify that it applies to any use of electronic communications services for the purposes of sending direct marketing messages, irrespective of the specific technological means used.
5. **Require for marketing calls the use of a special prefix** clearly distinguishing direct marketing calls from other calls. Under this option, those making calls for direct marketing purposes would be obliged to use such a special prefix so as to enable called users to recognise that the call in question is a marketing call.

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

6. **Reinforce cooperation obligations** among the competent authorities, including for cross-border enforcement. Under this option, the Commission would propose an obligation for supervisory authorities to cooperate with other supervisory authorities and provide each other with relevant information and mutual assistance.
7. **Repeal of the security rules** leaving the matter to be regulated by the corresponding rules in the Telecom Framework and the GDPR.

4.4. Option 3: Measured reinforcement of privacy/confidentiality and harmonisation

Under this option, the Commission would propose additional measures further reinforcing the protection and enhancing harmonisation/simplification. This Option would, in particular, reinforce the protection of confidentiality of terminal equipment, by making such protection technologically neutral and enhancing users' control through general privacy settings.

Objective 1: *Ensuring effective confidentiality of electronic communications*

1. The new instrument would propose a technology neutral definition of electronic communications, encompassing all the additional elements under **Option 2** (1, 2 and 3). It would specify a general principle of confidentiality of communications, except with the consent of the parties to a communication (and limited exceptions/permitted uses).
2. On the subject of confidentiality of terminal equipment and tracking of online behaviour the envisaged proposal would reformulate the current approach in favour of a technology neutral approach applying to all forms of tracking of (or other interference with) users' terminal equipment (including with regard to online behaviour), irrespective of the technique employed. The proposal would clarify that **consent can be given by means of the appropriate settings** of a browser or other application. Consent under this option will be in line with the concept of consent under the GDPR[82]. In line with the privacy by design principle, and in accordance with the GDPR and the RED, the proposal would require certain software providers to provide more transparency and provide their products with privacy friendly settings as a means to provide consent and to reinforce user's control over online

[82] See Recital 42 of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,* ***choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data****. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*."

tracking and over the flow of data from and into their terminal equipment.

Under the new rules, users would be prompted at the moment of the first utilisation of the equipment to choose their privacy settings among a specifically established set of privacy options, ranging from higher (e.g. "reject third party cookies" /"do not track") to lower levels of privacy protection. Users will be able to control and modify their privacy options easily and at any point in time. Users with reject third party cookies" /"do-not-track" settings in place would be clearly (but unobtrusively) informed when visiting websites requiring tracking and/or accepting third party cookies that visiting that website requires authorising tracking. It will then be for the user to decide whether to accept the tracking on the specific website or not. The general aim of this provision is to simplify and make the cookie handling by users more privacy friendly.

3. Impose **enhanced transparency requirements** alerting users when information emitted by their devices is captured. Entities collecting such information would be obliged to display clear, concise and conspicuous privacy messages/alerts (including by means of icons). The Commission would have delegated powers to specify the exact form and content of the message to be displayed.

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

4. All the measures from 4 to 5 under **Option 2**.

   Require **opt-in consent for all types of unsolicited communications covered by the current rules**[83].

5. Extend the provision on **presentation of calling line identification** to include the right of users to reject calls from specific numbers (or categories of numbers).

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

6. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions** identified by stakeholders as a source of confusion and legal uncertainty[84]. This will be achieved, in part through the measures identified above, by clarifying applicable law, the scope of the provisions concerning confidentiality of communications, the scope and requirements concerning confidentiality of terminal equipment and the rules on unsolicited advertising.

7. **Reinforce and streamline enforcement powers**: The new instrument would make sure that national competent authorities are provided with effective investigation end enforcement powers, including deterrent administrative fines and remedies. The proposal would entrust the application and enforcement of the provisions of the ePrivacy instrument to the same independent supervisory authorities appointed under the GDPR since confidentiality and privacy of electronic communications are closely linked with the related personal data processing. Under this option, the Commission would also extend the application of the consistency mechanism established under the GDPR to the supervisory authorities established under the ePrivacy instrument.

8. Repeal provisions on **security**[85] and the provisions on **itemised billing**.

9. Repeal the provisions on **traffic data and location data** to reflect the fact that the traffic and location data are more and more a homogeneous category, both in terms of privacy intrusiveness and technological availability ("communications data"). The processing of

[83] Article 13(2).

[84] This would cover in particular more detailed rules on the scope of the ePrivacy instrument, applicable law, the protection of terminal equipment privacy, the exceptions to the consent requirements and the scope of the unsolicited communications provisions.

[85] Article 4.

traffic and location data will be regulated under the general provision of confidentiality of communications[86].

10. Providing for **additional/broadened exceptions to confidentiality/permitted uses** for specific purposes which give rise to little or no privacy risks:

    a. Transmission or provision of a service: the processing of communications data is necessary for the purpose of the transmission of the communication or for providing a service requested by the user.

    b. Security: the processing of traffic data is necessary to protect, maintain and manage the technical security of a network or service, with appropriate privacy safeguards.

    c. Billing: in line with the current provision on traffic data, communications data may be retained insofar as necessary for billing or network management purposes.

    d. For a lawful business practice provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned on behalf of the ECS for the purpose of web analytics and web measurement.

    e. For a lawful business practice (e.g. OBA) where the processing is strictly limited to anonymised or pseudonymised data and the entity concerned undertakes to comply with specific privacy safeguards[87].

4.5. Option 4: Far reaching reinforcement of privacy/confidentiality and harmonisation

Under this option, the Commission would propose more far reaching measures reinforcing the protection of privacy/confidentiality and guaranteeing greater simplification/harmonisation. In particular, under this Option the Commission would propose a general banning on the so-called "cookie walls" and specific Commission implementing powers for ensuring consistent enforcement across MS.

Objective 1: *Ensuring effective confidentiality of electronic communications*

1. All the measures under No 1, 2 and 3 of **Option 3**.
2. Explicitly **prohibit the practice of denying access to a website** or an **online service** in case users do not provide consent to tracking (so-called "cookie-wall").

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

3. All the measures under No 4, 5, and 6 of **Option 3**.
4. Under this option, the Commission would **repeal** the provision allowing direct marketers to send electronic mail to subscribers and users when they have received their contact details in the context of a **previous business relationship**[88].

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

1. Measures under No 7, 8, 9, 10 and 11 of Option 3.

[86] Article 5(1).

[87] All or some of the following safeguards may be included: 1) no data relating to the specific content of the communications is collected; 2) the data stay anonymised or pseudonymised and that no effort or technique will be applied to re-identify the users; 3) the processing complies with the principle of proportionality and subsidiarity; 4) access and further information are guaranteed upon request; 5) the data processed do not constitute special categories of personal data as defined under the GDPR; (6) the entity concerned has carried out a data protection impact assessment under Article 35 of the GDPR; (7) prior authorisation from a supervisory authority. Additional safeguards may be specified, including the differentiation on the basis of the risk, in Commission's delegated acts.

[88] Article 13(2).

2. Introduce Commission's implementing powers for deciding on the correct application of the ePrivacy rules in order to ensure correct and consistent application of the EU law.

4.6. Option 5: Repeal of the ePD

Under this option, the Commission would propose the repeal of the ePD. Several stakeholders, especially in the ECS and OTT sector, have argued that ePD rules are no longer needed and that the objectives of the ePD would be achieved by the GDPR alone. With the repeal of the ePD, the confidentiality of electronic communications would fall under the general data protection regime as laid down in the Directive 95/46 and as of 2018 the GDPR. The objectives would be achieved as follows:

Objective 1: *Ensuring effective confidentiality of electronic communications*

1. The GDPR provides for reinforced rights of individuals and obligations of data controllers, which are in keeping with the challenges of the digital age. The **consent rule** under the GDPR has been in particular **substantially strengthened** with a view to ensure that it is freely-given. The GDPR addressed the issue of unbalance of power between the controller and the processor, requesting that this aspect be taken into account in the assessment of the validity of consent[89]. Also other grounds for processing electronic communications data would be available under the GDPR, such as contract and legitimate interest.
2. The GDPR would guarantee more effective enforcement thanks to the reinforced powers conferred on data protection authorities.

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

3. Unsolicited communications would be essentially regulated under a general an **opt-out** regime across 28 MS[90].

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

4. The new data protection rules would apply equally to all providers of electronic communications without distinctions based on the technology used. The concrete application of Article 7 of the Charter imposing the respect for private life and communications would not be specified in secondary law provisions, hence creating legal uncertainty.
5. There would be no duplication of rules in the security area and the privacy in the electronic communications sector would be regulated solely by the general data protection rules.

5. WHAT ARE THE IMPACTS OF THE DIFFERENT POLICY OPTIONS AND WHO WILL BE AFFECTED?

This section analyses the economic, environmental and social impact of the option in line with the Better Regulation Guidelines together with the coherence with other policy and the views of stakeholders. The description of the impact of the options included in this section is complemented by **an in depth economic analysis conducted by an external contractor supporting the present impact assessment** (see **Annex 8**). The detailed assessment of the impact of the policy option on different categories of stakeholders is included in **Annex 7**. As the external study makes clear, the economic assessment faced some limitations in the collection of data, whose impact was mitigated to a maximum possible extent (the limitation encountered are explained in **Annex 8**). The expected costs and benefits/cost-savings of each option are summarised and compared in **Annex 13**.

[89] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance
[90] See Article 21 of the GDPR.

5.1. Baseline scenario: no policy change

See Section 1.5 in the problem definition.

5.2. Option 1: Non-legislative ("soft law") measures

Effectiveness
Objective 1: *Ensuring effective confidentiality of electronic communications*
While the soft measures identified in this option may to a certain extent contribute to improve implementation, they also present a number of limitations. The **limited scope** of the ePD cannot be effectively extended by interpretative communications or other soft law measures. The CJEU offered an interpretation of the notion of electronic communication service which is clearly linked to the responsibility for the conveyance of signal over the underlying electronic communication network vis-à-vis end-users. The so-called OTTs provide their services in the form of applications running over the internet access service (hence "over-the-top") and are therefore in general not subject to the current EU telecom rules[91]. The Commission could not enforce, therefore, the current ePD against MS for not extending its scope to entities not currently covered. Moreover, interpretative communications would not be binding and could therefore have only limited impact on reducing legal uncertainty and resulting costs. Self-regulation, security and privacy by design standardisation would have positive effects. However, the success of these initiatives depends on the goodwill and agreement of the participating stakeholders. Negotiations may take considerable time and efficient outcomes are not guaranteed. The establishment of EU level self-regulation mechanisms could, in fact, only be achieved meaningfully and effectively with a clear and harmonised legal framework at its foundation. Awareness raising activities would be beneficial, but would however not be sufficient for reinforcing individuals' rights effectively in the absence of a strong underlying legal framework.
Objective 2: *Ensuring effective protection against unsolicited commercial communications*
While the soft measures identified in this option would contribute to improve the current implementation, they present in general the same limitations identified in general in relation to **Objective 1** above.
Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*
The soft measures identified in this option would have a limited positive effect, by introducing additional guidance and cooperation. However, the same limitations as under **Objective 1** apply. The internal and external inconsistency (including with the GDPR) of the ePD would not be effectively addressed in the absence of a legislative change. Similarly, the existing fragmented implementation will not change significantly in the absence of legislative intervention: while it is possible for MS to cooperate and exchange good practices, any change and improvement would take time and not necessarily lead to significant results. Likewise, the costs and business constraints stemming to certain ePD provisions would not be addressed.
Efficiency/Economic impact
The **Commission** would need to bear costs related to the implementation of the measures proposed under this Option: e.g. costs to issue guidance, follow the standardisation efforts, coordinate industry led-initiatives and launch the awareness raising campaign. It is estimated that this would require two administrators and one assistant working full time on these matters (running cost). However, most if not all of these measures could be undertaken by redistribution and refocusing of existing personnel and with the contribution of ENISA and the JRC.

[91] ECJ, C-518/11, C-475/12, cited above.

The launching of an awareness raising campaign may require the help of an external contractor; the cost may be estimated in the region of EUR 250-400,000 depending on the tools employed (one-off cost).[92] The funding of projects under the Secure Societies chapter of H2020, covering awareness-raising and other activities, amounts to EUR 1,694.6 million[93]. Of these, EUR 19.04 million were specifically dedicated to the topic "Privacy[94]" under work programme 2014-2015. A 25% increase would amount to EUR 4.76 million for the period 2014-2020, equalling an average annual increase of 680,000 Euro (running cost for the duration of the intervention).

National authorities will have to be involved in the co-regulatory efforts. This cost would vary according to the number of meetings and the degree of cooperation. Assuming that many issues may be steered by the Commission, a conservative estimate of 3 meetings a year for 3 years, the cost may be estimated to be between EUR 2,500 and 7,000 per authority/per annum (running cost)[95]. Similarly, national authorities would need to finance participation in efforts towards coordinated enforcement. Assuming in this case 2 meetings per year, the annual cost would be between EUR 1,700 and 4,700 (running cost). Minimal compliance costs for MS authorities to get familiar with the new implementing/soft law measures would be around EUR 1,000 per authority (1 day of training) (one-off cost)[96].

The direct impact on **businesses** is negligible. Businesses would continue to face essentially the same compliance costs and costs related to administrative burden. ECS providers would continue facing the same opportunity costs vis-à-vis OTT providers, resulting from the stricter rules they are subject to under the current ePD. It can be assumed that some minor cost savings would occur based on the clarification of the legal framework resulting from the interpretative communications and the Commission's promotion of a business-friendly (but effective) approach to the current rules. At the same time, minor costs could be incurred. Specifically, industry would need to bear certain costs for allocating resources for the participation to the codes of conduct and standard-setting activities. Considering past similar exercises, it could be assumed that the increase of cost would be moderate, as participation would be voluntary and normally only a relatively small proportion of businesses participate in such activities (running cost for the duration of the standardisation activities). In this context it is to be noted that some businesses already participate in such activities[97]. Businesses would be more extensively affected by the specification of privacy by design requirements of terminal equipment through EU standards, as they would need to implement the new standards (one-off cost and lower running cost ensuring updates). Depending on the content of such standards, the companies concerned may be more significantly affected.

In conclusion, this option presents *moderate/weak* implementation costs for the Commission and MS and *weak* benefits/cost savings for businesses.

Impact on SMEs, competiveness and competition

This option is expected to have limited impact on the overall macroeconomic context as the rules, the conduct of the operators concerned as well as the level of compliance with ePrivacy rules, are not expected to change significantly. Small positive impacts may be expected based on the increased efforts to ensure correct implementation and the support for EU-wide self-regulatory initiatives. Both would slightly contribute to greater harmonisation.

[92] This means that costs will be lower in case e.g. only an online campaign would be launched. In case e.g. an EU-wide awareness-raising campaign is launched with printed materials, informative events, discussion rounds etc., the costs will of course be higher than this estimate.
[93] Regulation (EU) No 1291/2013, ANNEX II, O.J. L 347, 20.12.2013, p. 104.
[94] See: http://ec.europa.eu/rea/pdf/2_security_societies_calls.pdf.
[95] This is based on assuming that between one and two persons per MS might join, that they need to spend time on travel, the meeting itself and preparation considering the hourly salary quoted by the Commission and that they need to pay for flight and in some cases for one night accommodation.
[96] Familiarisation/training costs= 3 staff-members per authority needing training * hours spent on training per staff (8 hours) *staff costs per hour (hourly wage rate EUR 41.5, Eurostat data 2012).
[97] An example is a German self-regulation initiative relating to online advertisement and the use of cookies of the Deutschen Datenschutzrat Online-Werbung (DDOW). See: http://www.iqm.de/digital/nutzungsbasierte-onlinewerbung/

The policy option aims to make the ePD implementation and application more effective, inter alia by introducing and disseminating new guidance, standards and best practices. For microenterprises and SMEs this implies the onus to understand and apply such guidelines, if necessary introducing the necessary changes in their processes. Some costs for microenterprises and SMEs may derive from the participation in standard setting or co-regulation activities, even though such participation is voluntary. On this basis, it is expected that Option 1 would create some additional costs for such companies. At the same time, the dissemination of additional guidance may contribute to enhance legal certainty and accordingly businesses may need to spend less in interpreting certain provisions.
Environmental impact
No significant environmental impact expected for any of the objectives.
Social impact
No significant social impact expected for any of the objectives.
Coherence with other policies
Internal market
The impact on internal market may be considered mildly positive. Interpretative communications from the Commission, self and co-regulation initiatives as well as standardisation activity at EU level would contribute to a certain extent to greater harmonisation of the current rules. However, there are also important limitations to the harmonising effects that these measures could achieve. Indeed, the interpretation and enforcement of privacy requirements is the task of independent national authorities. It rests ultimately upon the judgment of these authorities and national courts whether guidance from the Commission on the interpretation of the ePD provisions should be followed. Moreover, the success of self-regulatory measures depends on a number of circumstances, such as the degree of participation and compliance by the industry concerned.
Impacts on Fundamental Rights
The impact on fundamental rights is difficult to predict, as it largely depends on the content of the measures adopted and on the degree of implementation in practice. In general, considering that any improvement would only be possible within the limitations of the current rules, it may be assumed that any positive impact could only be moderate.
Impacts on innovation
Option 1 would have no or negligible impact on innovation.
Stakeholders' support
The striking majority of stakeholders across all categories criticised the current rules and asked for a change. Citizens and civil society organisations request more privacy protection. Public authorities (EDPS, WP29 and BEREC) expressed similar views. Operators concerned in the ECS[98] sector and OTTs both support deregulation and consider that the general data protection rules provide sufficient protection. Therefore, they recommend the ePD to be essentially repealed. These measures would thus not find substantial support in any group of stakeholders.

5.3. Option 2: Limited reinforcement of privacy and harmonisation

Effectiveness
Objective 1: *Ensuring effective confidentiality of electronic communications*

[98] DLA Piper, cited above.

Option 2 would significantly contribute to achieve the objective, although only in part. The extension of the scope of the instrument would fill considerable gaps in the protection guaranteed by the current ePD. However, the present option presents two fundamental limitations. *First*, it would not address the issues identified in relation to the so-called cookie consent rule, i.e. consent fatigue, lack of transparency and freely-given nature of the consent. *Second*, it would not effectively address the issues connected with enforcement (see Section 1.4 on problem drivers).

Objective 2: *Ensuring effective protection against unsolicited commercial communications*

Option 2 would partially contribute to achieving the objective. The clarification of the scope would ensure that all forms of unsolicited electronic marketing are caught by the provision, irrespective of the technology used. This change would ensure that the proposal remains technology neutral and thus fit for purpose despite technological developments.

The introduction of a special prefix is expected to increase transparency and allow citizens to reject or not answer calls identified as such thanks to the prefix. It is considered that such proposal would help reducing the nuisance generated by repeated or unwanted cold calls. Assuming that most marketers effectively comply with such rule, citizens would identify the call as being a marketing call and be able to freely decide at any time whether they intend to pick-up the call or not. It is therefore an additional safeguard for citizens to defend themselves against nuisance calls.

The effectiveness of this measure is, however, somewhat reduced by the fact that some phones may not display the calling number or that some companies may not provide this service for free. While the vast majority of mobile phones today would be technically equipped with a calling line identification function, the situation is different for landline fixed telephones. First, some telephone terminal equipment (old phones or vintage phones) do not have a display; second, in some MS, some telecom providers may not offer a calling line identification service or offer it as a premium service against the payment of a monthly fee. The introduction of the prefix would therefore not benefit those fixed telephone lines where the calling line identification is either not offered or not requested by the user.

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

The clarification of the rules regarding the scope (see under Objective 1) and unsolicited communications (see under Objective 2) would help eliminate/reduce the risk of divergent transposition and implementation by MS. Moreover, the present option wold reinforce cooperation, by including a specific requirement for exchange of information and cooperation in cross border-cases. However, in the absence of more specific and formalised coordination rules, the impact on overall consistency of the enforcement is expected to be limited.

The repeal of the security rules would simplify the legal framework by eliminating regulatory duplication with other legal instruments, such as the GDPR, the Telecom Framework and the NIS Directive.

Efficiency/economic impact

The costs for the **Commission** are not very high and essentially coincide with the legislative process. Costs for the Commission to oversee the implementation and functioning of the new instrument would not change significantly compared to the current situation.

MS will have to implement the new rules. If the new ePrivacy rules are contained in a directive, the new ePD would need to be transposed into MS laws. This would normally require some targeted changes to the current legislation. While the changes are not extensive, the enlargement of the scope may pose complex legal and technical issues to be resolved by national legislator. If the rules are contained in a Regulation, MS costs relating to the adaptation of the legal framework will be more limited.

The extension of the ePrivacy rules to new actors, such as OTTs (e.g. with regard to confidentiality and unsolicited communications) would add-up to the supervisory duties of **national authorities**, thus increasing their administrative workload (running cost).

Strengthening cooperation among national authorities would entail additional costs for public authorities that are currently not equipped with appropriate powers and adequate resources (running cost). It is difficult to estimate such costs in detail, given the differences in the size, available resources and sources of funding, tasks and powers of national DPAs. Costs will be higher for those MS whose authorities are currently not equipped with the appropriate tasks, powers and resources to ensure effective international cooperation. On the other hand, the impact is expected to be moderated by the experience already formed in the framework of the Article 29 Working Party and BEREC. The interaction already existing within these groups is likely to reduce learning and other transaction costs in this respect, at least by providing an already existing template for cooperation.

Industry would face some additional costs compared to the current situation based on the introduction of additional requirements for some operators previously not covered by the framework. As a consequence of the extension of the scope, OTT providers would no longer be able to rely on all legal grounds for processing personal data under the GDPR and would only be allowed to process communications data with the consent of the users. OTT practices in MS will have to be revised in order to ensure compliance with the ePrivacy rules on confidentiality (large one-off cost to adapt their data processing activities to the new rules and progressively smaller operational costs for updates and maintenance of processing systems) and other ePD rules on calling line identification and automatic call forwarding (for OTT using numbers) and directories of subscribers (all OTTs) (as above large one-off cost and smaller operational costs). This would entail a careful review and adaptation of the current data processing practices, based on a thorough legal analysis likely requiring external professional advice.

However, the extent to which costs would change would depend on the sector concerned and specific circumstances. These costs, in particular, are not expected to be particularly high for big/medium enterprises, which have consolidated experience in the application of privacy rules. In particular, these changes would not substantially affect those OTT (such as especially the largest players) that already operate on the basis of consent. Finally, the impact of the option would not be felt in those MS that have extended already the scope of the rules to OTTs. In these cases, the overall added burden (in terms of compliance and opportunity cost) is expected to be fairly contained at least in relative terms.

As for **unsolicited communications**, the rules will be formulated in a technology neutral way, which would imply their applicability to ads sent through OTTs falling within the scope of the new instrument. The applicability to such OTTs is not clear based on the current ePD and interpretations differ among MS. This implies therefore a potential extension of the scope of the current rules to other players not previously covered, at least in some MS. This would increase compliance costs for these businesses by an amount corresponding to the tasks needed in order to ensure that either prior consent is collected or users having opted-out do not receive marketing messages (e.g. one-off cost to adapt a website in order to include mechanisms to require consent or allow opt-out). Some further costs would ensue from the obligation to use a specific prefix in order to distinguish direct marketing calls from other calls (annual running cost for subscribing to the prefix service). It can be assumed that this would amount to a small one-off cost for the introduction of this prefix. According to the external study supporting the impact assessment, the cost for the introduction of the prefix would be of around EUR 500 yearly per company[99].

While the impact on compliance costs is not expected to be significant, this option would certainly have an impact on **opportunity costs** for OTT providers. **OTTs would face stricter standards compared to the current situation**, namely with regard to the obligation to process communications data only with users' consent as well as with regard to the limitation concerning traffic and location data. To assess the magnitude of these costs, it is important to consider that several popular OTT communication providers operate today on the basis of consent and have put in place significant measures aimed at improving the transparency and security of their data processing activities (e.g. end-to-end encryption). However, even though

[99] SMART 2016/0080, cited above.

consent is given by users in these cases, it will have to be verified whether the format of and the extent to which such consent can be considered in line with the notion of consent pursuant to the GDPR. The existing consent used would thus need to be reviewed and aligned with the GDPR concept in case the ePrivacy rules would also apply to these players, leading to compliance costs and potentially also to opportunity costs in cases where OTT players would be obliged to revert to less effective *moda operandi* or business models. Under this perspective, opportunity cost may be significant for providers which do not operate already in line with the GDPR consent notion. The limitations concerning traffic and location data further increase the impact.

Eventually, the negative effects on opportunity are likely to be mitigated by two concomitant factors: 1) the fact that a significant number of users may be willing to share their data in order to benefit from personalised services[100]; 2) the ability of providers to adapt and innovate their *modus operandi* by offering more privacy friendly alternatives, thus spurring competition and innovation on privacy features of their services. Overall, it is considered that the extension of the scope would raise opportunity costs for OTTs, but that this impact may be, at least in part, mitigated by the above factors.

The external study supporting the present impact assessment attempted to estimate the impact on costs of each option, on the basis of a pragmatic model based on a wide range of assumptions reflecting the general scarcity of data. Taking these limitations into account, the external study supporting the present impact assessment has estimated that this policy option would increase the overall compliance cost for the businesses affected by a 15% compared to the baseline scenario, leading to an additional EUR 203.3 million compared to the baseline scenario. Far from being a precise figure, this gives however a rough idea of what the magnitude of the overall impact on businesses could be. The tables including the calculations relating to the key quantitative findings are in **Annex 8**. While the increase in cost in absolute terms is high, it should be considered that this reflects the fact that (some provisions of) the ePD covers a very broad range of affected entities, i.e. all businesses having a website. In average terms, the increase in costs is much more measured and cannot be considered a priori excessive in light of the underlying objectives. Being an average figure, this does not mean of course that the increase in costs may not be significantly greater for some companies (e.g. because significantly wider or more complex processing operations are at stake) or significantly smaller for other companies (e.g. because much smaller or less significant processing operations are at stake).

In conclusion, this option presents *moderate* transposition/implementation costs for MS and compliance costs for some categories of businesses (OTTs). Moreover, the extension of the rules to OTTs would raise *moderate/high* opportunity costs for these operators.

Impact on SMEs, competiveness and competition

Option 2 would ensure that all players offering communication services would face equal regulatory standards. However, the level playing field would be ensured essentially by extending the current regulatory constraints beyond ECS, without providing for additional flexibility. This may limit competitiveness.

The impact on **SMEs** of this option is generally connected with the extension of the ePrivacy instrument to OTTs and the clarification that the instrument also applies to publicly available private networks. It can be foreseen that a greater number of SMEs would be caught within the scope of the confidentiality rules and subject to the restrictions concerning the processing of electronic communications data. This implies **additional compliance costs and opportunity costs**. As highlighted above, it is possible that existing business models of OTT providers would need to be revised to the extent that they will no longer be able to rely on other legal bases under this option than consent. Thus, this specific sector would be significantly affected, at least in the short term. These costs would be higher for smaller players and newcomers that

[100] On the so-called privacy paradox, see e.g.: https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf.

do not operate on the basis of consent. These OTTs may find it more expensive, as a result of tighter confidentiality rules, to obtain users' consent and establish the critical mass of users needed to compete with the established operators.

Environmental impact

No significant environmental impact expected.

Social impact

No significant impact is expected.

Coherence with other policies

Internal market

Option 2 would have a positive effect on the internal market. The measures at stake would cover some gaps of the existing ePD, solving the problems related to its unclear, inconsistent and fragmented scope. They would also clarify the rules on unsolicited communications. Accordingly, the option is expected to slightly or moderately enhance harmonisation. The increased cooperation may foster consistency. However, the plurality of enforcement authorities, which has been seen as a major hindrance to consistent enforcement, will not be addressed.

Impacts on Fundamental Rights

This option would have positive effects on the level of protection of confidentiality of communications and related personal data as it would increase the protection by extending/clarifying the principle of confidentiality to communications not currently covered. However, shortcomings relating to online tracking would not be addressed.

Impacts on innovation

Option 2 would have a composite effect. Greater protection of privacy of electronic communications may to a certain extent limit innovative business models relying on a large availability of data, such as free online personalised services. However, by extending confidentiality requirements to OTTs, the present option is expected to stimulate research and innovation on privacy-enhancing solutions.

Stakeholders' support

The public consultation shows that an overwhelming majority of citizens and civil society and public bodies find that **OTTs should provide the same level of protection when they provide communications services as ECS providers**. As far as the industry is concerned, only (over) a third of the industry agrees, which includes ECSs and OTTs[101]. The **need to guarantee confidentiality of communications regardless of the technology used** is also confirmed by the Eurobarometer on e-Privacy[102], the Article 29 Working Party[103] and the EDPS[104]. **Civil society strongly supports** the extension of the rules to OTTs and reinforcement of protection of security and confidentiality.[105] Close to 90% of citizens, civil society and public authorities favour an opt-in regime whereas 73% of industry favours an opt-out regime.

Therefore, the Option is in line with the views of citizens and public authorities. However,

[101] Question 17 of the Public Consultation.
[102] More than **nine in ten** (92%) participants say it is **important** that the **confidentiality of their e-mails and online instant messaging is guaranteed:** SMART 2016/079, cited above.
[103] Working Party 29, Opinion on the ePD review, cited above.
[104] EDPS, cited above.
[105] EDRI, cited above.

business organizations demanding the total repeal of the ePD would be against the proposal of maintaining the current dual regime of data protection/privacy regulations[106]. OTTs would not support the extension of the ePrivacy rules to cover their activities[107].

5.4. Option 3: Measured reinforcement of privacy/confidentiality and harmonisation

Effectiveness
Objective 1: *Ensuring effective confidentiality of electronic communications*
This Option would achieve the objective. In addition to the positive aspects remarked in relation to Option 2, this option would introduce a more comprehensive and technology neutral notion of interference with the privacy and confidentiality of terminal equipment. This measure would make sure that the protection established by the provision in question would cover any interference with users' privacy. In particular, it would cover the technique of device fingerprinting, which is currently at least in part not covered by the present provision. By mandating applications enabling access to the Internet such as browsers to implement and preconfigure privacy friendly settings, this option would reinforce user's control and at the same time greatly *simplify* the management of privacy preferences. Users will be able to manage their preferences in a centralised way regarding access to information stored in their terminal equipment. At the same time, it is expected that this option would significantly reduce the interference provided by cookie banner with users' browsing experience. In the online world, users are increasingly overloaded with notices and requests for consent. Given the limited time available and the increasing complexity of online interactions, users are less capable of coping with the growing amount of notices and requests. A centralised system governing users' privacy choices with regard to all third party interactions with their terminal equipment would greatly simply and make the level of protection more effective. Finally, by streamlining and strengthening enforcement rules, notably by specifically entrusting them to the same supervisory authorities as those enforcing the provisions of the GDPR, this option would create the conditions for a more effective and consistent enforcement. This option would further reinforce the transparency of tracking technologies. The provision of clear and concise standardised information is expected to contribute to resolving the problems caused by tracking practices in public spaces. Privacy sensitive citizens will be better informed and be able to freely decide whether to agree or to move to a competing, more privacy friendly solution. By contrast, the introduction under this Option (see under Objective 3) of a derogation to the consent rule for the processing of communications data (e.g. traffic and location data) for marketing purposes (measure No 10(e)) undermines at least to a certain extent the effectiveness of the option vis-à-vis its objective of reinforcing the protection of confidentiality of communications. The possibility for OTTs and ECSs to interfere with the confidentiality of electronic communications without the consent of the users reduces citizens' control over their communications and therefore constitutes a significant limitation in relation to the present objective. While the negative effects on privacy protection would be limited by strict safeguards, i.e. as approved by the competent authorities, this element reduces the effectiveness of this option.
Objective 2: *Ensuring effective protection against unsolicited commercial communications*
Option 3 would significantly contribute to achieving the objective. In addition to the positive elements of Option 2, the generalisation of the opt-in consent is expected to reduce the

[106] DLA Piper, cited above.
[107] DIGITALEUROPE response to Commission ePrivacy Directive Consultation, http://www.digitaleurope.org/Digital-Headlines/Story/newsID/501.

possibility of error by direct marketers, i.e. reaching persons that do not want to be reached (but have not subscribed to an opt-out list or in cases where opt-out lists are not functioning properly) and shift the burden of proof from citizens to callers to demonstrate that they have obtained consent. By contrast, it should be noted that the enforcement against unlawful calls is particularly difficult, especially where callers conceal or disguise their identity. Considering that the evidence collected during the impact assessment did not lead to conclude unequivocally that the problems related to unsolicited communications are caused by the opt-out systems, but rather as the result of its ineffective implementation, there is no precise guarantee that this measure would effectively improve compliance. Finally, the **clarification of the rule on calling line control** would make it easier for citizens to avoid unwanted marketing calls, as they would be able to block certain (categories of) numbers.

Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*

Option 3 would satisfactorily achieve the objective. In addition to the positive elements of Option 2, the **clarification and specification of certain rules** would contribute to simplification and harmonisation. This would improve the situation for businesses. It would also increase transparency for citizens. By reinforcing and streamlining enforcement rules, ensuring that the same supervisory authorities, namely the data protection authorities, entrusted to enforce data protection rules under the GDPR, are also competent to enforce ePrivacy rules, this option would significantly improve the current situation of incoherent and differentiated enforcement. The allocation of the enforcement to data protection authorities and the extension of the GDPR consistency mechanism would ensure consistency, simplify the regulatory framework and thus reduce the administrative burden.

The **changes to Article 5(3)** would also contribute to simplification. In particular, citizens would be able to manage their privacy settings in a centralised way, which is valid and binding for all third parties. Information society services engaging in tracking activities would be able to rely on the general privacy preferences set by the users.

In addition, this option would ensure that the new instrument would be in line with the market and technological reality. For example, the introduction of exceptions for Article 5(3) means that non-privacy invasive techniques are no longer covered by this provision. On this basis, fewer websites would be covered by Article 5(3)[108].

Even if the scope is extended to entities which are currently not subject to the rules, these entities will be able to use the additional flexibility introduced under this option (i.e. process communications data with consent or with privacy safeguards). ECSs will have more opportunities to process communications data and engage in the data economy.

Efficiency/economic impact

The costs for the **Commission** and for MS are essentially the same as **option 2** (*low*). However, in this case the Commission would need to devote resources to issue the necessary delegated and implementing acts concerning the transparency measures. It is estimated that this would require one administrator working full time on these matters (one-off and running cost). As per Option 1, most of these measures could be undertaken by redistribution and refocusing of existing personnel and with the contribution of ENISA and the JRC.

The streamlining and strengthening of enforcement powers would entail additional costs for **MS** authorities. The main costs for competent authorities would relate to the changes needed to allocate competence regarding all the provisions of the proposed ePrivacy instrument to the supervisory authorities of the GDPR (i.e. data protection authorities or DPAs) (one-off cost) and the extension of the consistency mechanism to aspects relating to the ePD (running cost). It should be noted that these costs will have to be borne specifically by the authorities in those MS that have not attributed competence to apply the ePD to the same supervisory authorities

[108] Based on the 2014 Cookie Sweep, 74 out of 474 websites only used first party cookies. In addition, 15 out of 474 only used session cookies (first and third party). Article 29 Data Protection Working Party (2015), Cookie Sweep Combined Analysis – Report, WP 229.

competent for applying the GDPR. Member States have followed very different approaches in this respect. Some Member States have designated DPAs (e.g. Bulgaria, Estonia, France), others the telecom national regulatory authority (NRAs) (e.g. Belgium, Finland, Denmark) and still others appointed both DPAs and NRAs (e.g. Austria, Germany, Greece) for the ePD enforcement. In some Member States, competence concerning the ePD is even shared between three or four different authorities[109], including in addition to DPAs and NRAs e.g. consumer protection authorities. The table included in **Annex 11** presents an overview of the situation in each Member States[110].

For MS not having entrusted the ePrivacy enforcement to DPAs, the following types of costs are expected to arise: one-off costs relating to the shifting of enforcement powers from other authorities to DPAs (including e.g. organisation costs, costs for setting up new IT systems, costs for training staff), as well as on-going costs for carrying out the tasks related to the ePrivacy rules.

As concerns the one-off costs, it is important to note that the greater majority of DPAs appears to already have some or all the competences to apply the ePD (for example 22 MS have data protection authorities competent for at least some confidentiality rules). For these authorities, the cost would be rather contained, as it can e.g. be expected that the number of additional staff that needs to be trained is low and the relevant IT systems already exist. As concerns the on-going tasks, it can be expected that most of the costs could be compensated by means of redistribution or refocusing of existing staff. Moreover, additional resources could derive from the increase of the powers to impose sanctions for breaches of ePrivacy rules.

Having regard to the extension of the consistency mechanism, it was estimated in the related impact assessment that authorities would need at least 2 or 3 persons working on matters in relation to the consistency mechanism (running cost)[111]. The application of the consistency mechanism to the ePrivacy rules is not expected to appreciably raise costs for the ***EDPS*** for providing the secretariat of the European Data Protection Board, with respect to the issues already covered by the present consistency mechanism under the GDPR. As a matter of fact, the GDPR already applies to the matters relating to the electronic communications sector that are not specifically regulated by the ePD. Therefore, the Board can be considered to be already sufficiently equipped to be involved in such matters[112].

The **industry** would face additional costs compared to the current situation based on the extension of the scope to entities previously not covered (e.g. OTTs) (large one-off cost to review and adapt data processing activities and smaller operational costs for updates and ad hoc legal advice), although the extent to which costs would change depends on the sector concerned and specific circumstances. As explained in relation to **Option 2**, while compliance costs are not expected in general to be high, the extension of the scope is expected to raise opportunity costs for OTTs. The option would not lead to additional costs for **ECSs**, as they process communications data already on the basis of consent.

As concerns the new rules relating to tracking, information society services engaging in online tracking such as **website operators** would strongly benefit from the simplifications introduced in this area. First of all, the present option would introduce additional exceptions for first party cookies presenting no or non-significant privacy implications, such as cookies used for web measurement. This would exonerate a significant number of websites from the obligation to request consent, with connected significant savings. Additional savings are expected in relation to the introduction of the centralised setting of the privacy preferences. The new rules would

[109] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.
[110] SMART 2016/0080, cited above.
[111] Commission Staff Working Paper on *Impact Assessment on the General Data Protection Regulation proposal*, 25.01.2012, SEC 2012(72), p 103.
[112] This reflects as well the current situation with respect to the ePD and the DPD where the WP29 already carries out its tasks with regard to matters covered by the ePD, namely the protection of fundamental rights and freedoms in the electronic communications sector.

indeed clarify that consent to tracking could be given by means of the appropriate setting of an application such as Internet browsers. Furthermore, it would require these operators to put in place privacy settings in a way that they can indeed be used to signify consent. Users would be prompted at the first utilisation of the equipment to choose their privacy settings on the basis of clear alternatives. Users would be able to control and modify their privacy options easily and at any point in time. As a consequence, website operators will not be in principle obliged to display cookie messages asking users to consent. This would greatly simplify website administration with connected significant savings.

Basic compliance costs relating to the cookie consent rule have been estimated around EUR 900 per website (one-off)[113], with more than 3.7 million websites potentially affected in 2030[114]. The Commission external study supporting this impact assessment, however, reported that this figure could be much higher and even reach the levels hundred thousand euro for larger websites engaging in more complex processing operations[115]. Given the wide formulation of the cookie-consent provision, and the limited scope of the related exceptions, this cost has currently to be borne not only by those websites engaging in web-tracking by means of third-party cookies, but essentially by all websites using cookies, even if only technical first party cookies that present little privacy invasiveness are used (except if such cookies can be considered covered by one of the strictly interpreted exceptions[116]). The magnitude of the total savings potentially stemming from exemption from consent is therefore significant.

While the impact on compliance costs is expected to be significantly positive, a large number of businesses would potentially incur large opportunity costs to the extent that OBA tracking would become more difficult. From a rather extreme perspective, if users would not accept third party cookies or would opt for do-not-track, such solution could undermine the availability of an essential input for OBA profiling. The reason for this is that consumers may be inclined to set their preferences on “reject third party cookies”/ "do-not-track" by default. However, in a moderate and more plausible scenario, an impact on the OBA / ad-network market might not be so significant considering that:

- Solutions for users to manage whether they want OBA tracking already exist in the market; and many privacy minded users have installed them; these solutions are part of the toolboxes related to tracking and thereby to some extent available to customers using these toolbox solutions.
- Under the present option, users with “reject third party cookies”/ "do-not-track" settings activated would be informed when visiting websites requiring tracking that visiting that website requires authorising tracking. In cases end-users choose the setting "never accept cookies" or "reject third party cookies", websites may still convey requests or place banners in their web sites requesting the user to change his/her view and accept cookies for the particular website. End-users shall be able to make informed decisions on a case-by case basis. It would then be for users to decide whether to continue to browse or to revert to alternative websites/services[117]

Additional costs would ensue for the limited number of **providers of browsers** or similar software as these would need to ensure privacy-friendly settings (one-off costs to revise their settings and running costs to ensure technical updates/services). These costs would essentially relate to the revision of existing offers and IT costs for implementing new solutions. In this context it has to be noted that some of these parties may already comply with such standards. The magnitude of direct compliance costs for providers of browsers or similar software cannot

[113] Castro, D. and Mcquinn, A. (2014), *The Economic Costs of the European Union’s Cookie Notification Policy*, ITIF, p. 5.
[114] Given that the estimated average lifetime of a website is of 3 years, the study supporting the impact assessment has assumed a financial cost of 300 per year. See SMART 2016/0080, cited above.
[115] SMART 2016/0080, cited above.
[116] Article 29 Working Party, Opinion 04/2012 on *Cookie Consent Exemption*, WP 194.
[117] For the assessment of opportunity costs, see SMART 2016/0080, cited above.

be estimated in quantitative terms but it is, for the above reasons, not expected to be very high. In general, this element only concerns a small fraction of all businesses applying the ePD. The browser market itself is highly concentrated in Europe: Users of *Google*'s *Chrome* browser account for a half of all website visitors, while close to a third of all users relies on Safari and Firefox. Four major companies dominate the market of browsers used by consumers: 94% of all website visitors in Europe rely on software from *four companies*. In addition, there are some additional browser operators with smaller market shares[118]. On this basis, an overall moderate increase for browsers may be expected for all three solutions.

With regard to *unsolicited communications*, the same cost analysed in relation to Option 2 in relation to measures concerning the clarification of the scope and the introduction of the prefix applies here. Imposing a general opt-in requirement will imply some additional compliance costs for **businesses**, as they will have to review their business models and limit marketing only in respect to those subscribers for which they have received consent. This is expected to raise the costs of a marketing campaign, as businesses would have to revise their practices and update the mechanisms they use to obtain consent (one-off cost to review current practices and update website to include mechanisms to request consent and running costs for technical updates). This effect will be felt only in those MS that have at present adopted the opt-out system. In particular, as far as fixed lines are concerned, 8 MS adopted an opt-in, 17 an opt-out, whereas 3 MS have mixed systems depending on whether consumers (opt-in) or other players (opt-out) are concerned. As far as mobile lines are concerned, 12 MS adopted an opt-in, 13 an opt-out, whereas 3 MS have mixed systems depending on whether consumers (opt-in) or other players (opt-out) are concerned. The analysis of the data concerning the situation in MS, however, has shown that the largest majority of traders would be affected by this change, especially as far as fixed line calls are concerned (88% of traders) but also for mobile phones (61%).[119] On the other hand, businesses operating in different MS would no longer have to implement different regimes, neither deal with different kind of competent authorities; thus potentially leading to savings in terms of compliance costs for those businesses operating cross-border.

Further cost savings can be expected for those sectors already applying the ePD based on the simplification of the legal framework and further harmonisation. In particular, the repeal of Article 4 on security obligations and Article 7 on itemised billing, the merging of Articles 6 and 9 on traffic and location data would lead to a moderate decrease in compliance costs and administrative burden for businesses[120].

The external study supporting the present impact assessment attempted to estimate the impact on costs of each option, on the basis of a pragmatic model based on a wide range of assumptions reflecting the general scarcity of data. Taking these limitations into account, the external study identified three distinct implementation scenarios, according to the entity who will establish the dialogue box between the user having chosen "reject third party cookies"/ "do-not-track" settings and websites visited wishing the Internet user to reconsider his/her choice[121]. The entities who could be put in charge of this technical task are three: 1) the software providers concerned; 2) the third party tracker (e.g. the advertising networks); 3) the individual publishing websites. According to the study, this option would lead to **overall savings** in terms of compliance cost compared to baseline scenario of 70% (948.8 million savings) in the first scenario (browser solution), 60% (813.2 million) in the second scenario

[118] Data for geographic Europe only, based on visitors of a sample of 3 million websites globally accessible on http://gs.statcounter.com/

[119] See **Annex 10** and SMART 2016/0080.

[120] It was estimated that currently 3,000 data breach notifications take place in the EU for the telecoms sector every year, calculated on the basis of 319 data protection breaches reported to the UK DPA in 2008/2009 and extrapolated for the EU28. The average cost for businesses for dealing with these notifications was assumed to be 400 Euro. Commission Staff Working Paper on *Impact Assessment on the General Data Protection Regulation proposal*, 25.01.2012, SEC 2012(72), Annex 9 and p. 101.

[121] The web site may decide to set tracking as a condition for accessing the content. In case users wish to access the content in the "tracking" website they would receive a request to authorise the tracking for that specific website (or for all the web sites that are related to a third party tracking) and then would have to decide whether to accept or refuse.

(tracking company solution) and of 5% (67.8 million) in the third scenario (publisher solution). As overall savings largely derive from a very significant decrease of the number of affected businesses, the individual amount of compliance costs one business is expected to incur – on average – would be higher than today. Far from being precise figures, they give however a rough idea of what the magnitude of the impact on businesses could be. The tables including the calculations relating to the key quantitative findings are in **Annex 8**, together with an overall explanation of the model, the related assumptions and limitations.

In conclusion, in addition to the same impact as Option 2, this option would generate *high* cost savings for businesses (website owners), next to additional *moderate* costs for MS (streamlining enforcement and consistency) and for some business categories (marketers and Internet browsers).

Impact on SMEs, competiveness and competition

This option is expected to have a positive impact on the business environment, especially on cross-border trade within the digital single market, as consumer **confidence and trust** that their rights are respected would increase. Traders operating over several markets would benefit from uniform regulatory conditions.

ECSs and **OTT** would be able to compete on an equal footing as far as privacy legislation is concerned. As highlighted in relation to Option 2, the tightening of the rules for OTTs may have a negative effect on the capacity of online providers to collect big data about subscribers or users. This effect is likely to be felt more by small players or newcomers than by big established players with an already significant installed users' base. However, the potentially negative effect would be mitigated by the **further flexibility** introduced in the legal framework through brand-new exceptions and derogations.

The impact on **SMEs** of this option is mixed. SMEs who are ECSs would have greater opportunities to monetise the value of data than it is the case today deriving from the addition legal grounds to process traffic and location data. Most importantly, SMEs having a websites (60-85% of the total[122]) would draw significant benefits from the reduction of the compliance costs with regard to the cookie consent option under the application exceptions and derogations and the simplification related to browser settings. Since costs related to the cookie consent provision are considered to be the main source of cost for SMEs of the current ePD, these savings are expected to drive compliance costs significantly down.

On the other hand, SMEs who are OTTs would be negatively impacted by the extension to them of the scope of the ePrivacy rules. As highlighted in relation to Option 2, this would imply an increase of compliance costs and, in particular, of opportunity costs. As highlighted above, the provision on of do-not-track browser settings would have a negative impact on the effectiveness of OBA models, although such impact for the reasons explained above is not expected to be significant or disruptive. In general, the additional costs are expected to affect in proportion more heavily SMEs than bigger players, given the lower amount of resources and installed customer base that smaller firms can rely on.

Environmental impact

No significant environmental impact expected for any of the options.

Social impact

No significant social impact is expected.

Coherence

Internal market

Option 3 would have a positive effect on the internal market due to the greater clarity, harmonisation and consistency of the rules across 28 MS. The streamlining and strengthening

[122] SMART 2016/0080, cited above.

of enforcement would contribute to greater consistency. Finally, the generalisation of the opt-in requirement would have a positive effect on the internal market as it would reduce the risk of diverging implementation in MS concerning the provisions on unsolicited advertising.

Impacts on Fundamental Rights

The right to respect for private and family life and communications is a fundamental right in the EU (Article 7 of EU Charter of Fundamental Rights). This option would increase the level of protection, boost legal certainty, and make EU confidentiality of communication more effective. The proposal is compatible with the GDPR.

By enhancing the protection of confidentiality of communications, which is a necessary condition for the freedom of expression and other related rights, such as personal data protection, the freedom of thought and the freedom of association, the present option is expected to impact positively on these connected rights and freedoms. At the same time, the introduction of the possibility to process communications data without consent of the users for marketing purposes (measure No 11(e)), albeit under strict privacy safeguards, reduces users' control over the confidentiality of their communications and actually reduces the degree of protection of a fundamental right.

The option does not aim to address per se consumers protection issues (Art. 169 TFEU). However, it cannot be excluded that some of the above highlighted changes would benefit consumers in their buying and selling experiences. This could be the case for instance of the measures providing for greater transparency, measures limiting aggressive marketing behaviours (phone calls) or allowing users to say no to tracking/discriminatory practices through privacy settings.

Impacts on innovation

Option 3 would have a composite effect. Greater transparency and protection of privacy of electronic communications may to a certain extent limit innovative business models relying on a large availability of data, such as free online personalised services. This may reduce the capacity to grasp the benefits of the data economy. However, as already observed, the present option includes some crucial elements of flexibility, such as additional exceptions and derogations with adequate safeguards. Therefore, any negative effect is expected to be limited. Moreover, the new rules could lead to the emergence of innovative, privacy friendly business models and technical solutions.

Given the emphasis on confidentiality requirements, the present option is also likely to stimulate the R&D in privacy preserving technologies. Research on anonymisation and pseudonymisation techniques, for instance, is expected to be significantly boosted. From this point of view, the option would facilitate the introduction and dissemination of new production methods, technologies and products in this emerging sector.

The review of the ePD could support the development and use of the IoT and digitalization of industry inter alia by fostering more regulatory certainty for all players throughout the IoT value chain contributing to a better investment climate and end-users confidence about security, privacy and confidentiality.

Stakeholders' support

National consumer authorities, **consumer and trade organisations**, as well as the **European Parliament** have been consistently calling for an increase in privacy protection in relation to electronic communications as a means to ensure greater levels of trust in the DSM. This option goes in the direction of these instances.

The proposal to impose **privacy by default in browser setting** was strongly supported by **89%** of the respondents to the Eurobarometer[123], national data protection authorities[124] and the EDPS.

[123] SMART 2016/079, cited above.

A majority of citizens and civil society, industry and public bodies believe that the allocation of enforcement powers to different authorities led to divergent interpretation of rules in the EU and to non-effective enforcement while they considered the DPAs to be the most suitable authorities to enforce ePrivacy rules. This supports measures enhancing the consistency and effectiveness of enforcement, including entrusting the rules to one category of competent authorities[125]. Likewise, the consensus for clarifying the rules and increase harmonisation is high across virtually all stakeholders groups[126].

National data protection authorities and the EDPS both called for a clarification of the rules on **unsolicited communications** and for the generalisation of the opt-in requirement (except in the context of a previous business relationship[127].

Consumer organizations strongly support the extension of the rules to OTTs and reinforcement of protection of security and confidentiality. Close to 90% of citizens, civil society and public authorities favour an opt-in regime whereas 73% of industry's an opt-out regime.

To the extent that they demand the **repeal of unnecessary provisions**, ECS should support the results guaranteed in this direction by the repeal of the security provisions and the provisions on itemised billing, and automatic call forwarding.

This option would not be supported by those **industry members** who call for the full repeal of the ePD (63% of the businesses responding to the public consultation). **OTTs**, in particular, will be against the extension of the ePrivacy rules to online communications.

5.5. Option 4: Far-reaching reinforcement of privacy/confidentiality and harmonisation

Effectiveness
Objective 1: *Ensuring effective confidentiality of electronic communications*
The present option would guarantee the greatest protection of confidentiality in that it would limit the online tracking by forbidding making the access to a particular website conditional upon the consent to accepting the use of cookies or equivalent tracking practices (so called "cookie wall"). As in Option 3, the effectiveness is reduced by the possibility to process metadata for marketing purposes without consent.
Objective 2: *Ensuring effective protection against unsolicited commercial communications*
Option 3 will further reduce the nuisance of unsolicited communications, to the extent that it will prevent the use of opt-out in the context of a previous business relationship.
Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*
Commission's implementing powers to decide on the correct application of the rules in specific cases would provide the maximum results in terms of harmonisation and simplification. However, the tightening of the consent mechanism (banning of cookie walls) would introduce a significant element of rigidity, thus compromising the full achievement of the objective.
Economic impact (compliance, administrative costs)
For the **Commission** and **MS** the costs will be the same as per option 3. However, there may be a slight increase of costs for **MS authorities** following the introduction of the ban on cookie walls, as the checking of compliance may be more time consuming and it is possible that the

[124] Working Party 29, cited above, p. 17
[125] See e.g., Working Party 29, Opinion on the ePD review, cited above, p. 5, EDPS, cited above, p. 8, EDRI, cited above; DLA Piper, cited above, p. 39.
[126] *Ibidem*.
[127] See Working Party 29, Opinion on the ePD review, cited above, p. 20, EDPS, cited above, p. 20.

number of complaints by citizens could increase (running cost). The **Commission** would face some additional costs in terms of human resources for the adoption of implementing powers (running cost). The number of resources needed would depend on the extent to which these powers are effectively used. It is expected that the impact would be moderate, including because the Commission retains discretion on whether and when using these powers and because the consistency mechanism is introduced at the same time and also gives a forum for handling cases with a European impact. On this basis, it may be estimated 1 to 2 additional FTEs (administrator level) may be sufficient to handle these cases. These additional costs may be covered by shifting or refocusing of existing effectives, and with the technical support of ENISA and JRC.

In addition to the impact analysed in relation to Option 3, this option would present additional compliance and opportunity costs for **industry**. The ban on cookie walls would entail costs for service providers to evaluate and amend their current practices (large one-off cost). Unlike in **Option 3**, under this option businesses will need to amend their websites/services so that they are also available to the extent possible without the use of cookies/tracking. For example, this could mean that in effect two versions of website need to be offered[128]. It may be assumed that only a very limited percentage of users would accept tracking cookies (or equivalent techniques) for the purpose of OBA. Still, publishers could not refuse access to their content in these cases. Ultimately, this is likely to affect the financial viability of business models that are largely financed by means of advertising. The complete elimination of the opt-out regime for unsolicited marketing by email would result in further loss of revenue for traders, as marketing to previous clients is restricted.

The external study supporting the present impact assessment attempted to estimate the impact on costs of each option, on the basis of a pragmatic model based on a wide range of assumptions reflecting the general scarcity of data. Taking these limitations into account, the external study has estimated that this option would determine a reduction of the overall compliance costs (-5%, i.e. 67.8 million) and administrative burden (-3%, i.e. 0.007 million), compared to the baseline scenario. Again, even if the overall impact on costs is positive, in average terms this would translate according to the model on higher compliance costs for individual firms, reflecting indeed the lower number of firms on which this reduced overall cost is divided. Far from being a precise figure, this gives however a rough idea of what the magnitude of the impact on businesses could be. The tables including the calculations relating to the key quantitative findings are in **Annex 8**[129]**,** Opportunity costs resulting from the significantly tighter restrictions on processing data for OBA purposes are likely to be high, as explained, and may even undermine the viability of OBA based business models.

In conclusion, in addition to the same impact as Option 3, this option would generate *high* compliance and *high* opportunity costs for businesses (marketers, publishers and advertising business) and, potentially, *high* costs for citizens related to availability of (free of charge) online services. Commission's implementing powers for ensuring consistency of enforcement would generate some *moderate* benefits for businesses.

Impact on SMEs, competiveness and competition

This option introduces much stricter regulation of online tracking by means of cookies, by prohibiting websites owners to deny access to their websites in case users do not consent to tracking. As explained above, this would lead to an increase in compliance costs for website owners, an increase which will be more strongly felt by microenterprises and SMEs, given their smaller size. Other than direct compliance costs, opportunity costs also are expected to rise. Additional costs derive from the tightening of the rules on unsolicited communications (i.e. no exception to opt-in). The measures at stake are therefore expected to raise the costs for **businesses** and affect **competitiveness**, and ultimately hamper the viability of widespread OBA-based business models. The impact on **SMEs** is possibly more significant, given that they

[128] SMART 2016/0080, cited above.
[129] SMART 2016/0080, cited above.

have fewer resources to adapt to a more complex legal framework. The impact on the online news publishing industry is of particular concern, given the importance of OBA for the viability of their businesses.

Environmental impact

No significant environmental impact expected for any of the options.

Social impact

For Objective 1, the measures may have negative impacts on employment in the short-medium term, to the extent that it could undermine the legal viability of some OBA based online business models.

As to Objective 2, the general removal of the opt-out for sending messages by email to existing customers may reduce the effectiveness and thus the attractiveness of marketing campaigns even further compared to Option 2. This may in theory have some effects on employment in this sector, although it is likely that resources would be shifted to other forms of marketing.

Coherence with other policies

Internal market

This option would have a positive effect on the internal market as much as the previous option. Commission's implementing powers would help removing further interpretative uncertainty and fragmentation.

Impacts on Fundamental Rights

This option is expected to have a very positive impact on confidentiality of communications and related personal data, as it would substantially reduce online tracking.

The option is not per se incompatible with the GDPR, even though the empowerment of the Commission to issue implementing acts for the implementation of certain ePrivacy rules can be seen as inconsistent, to the extent that the same powers are not foreseen for the application of GDPR rules.

This option could have an effect as regards property rights and freedom to conduct business, to the extent that imposes some serious limitations to online business models based on OBA. The risks for the viability of these business models could ultimately hinge on the freedom of the press and pluralism of information, insofar as they affect one important source of financing for the online press.

Impacts on innovation

Option 4 would restrain the freedom of action of online operators, thus reducing their capacity to grasp the benefits of the data economy. The lower capacity to engage in the data business is thus expected to adversely affect the innovation potential in a number of sectors.

Stakeholders' support

This Option is supported by citizens and civil society organisations. In particular, national data protection authorities, the EDPS and civil society groups have all recommended measures to reduce the impact of cookie walls in order to ensure that consent to tracking is freely given. On the contrary, it is strongly opposed by the industry[130].

5.6. Option 5: Repeal of the ePD

Effectiveness

[130] DLA Piper, cite above; DIGITALEUROPE, cited above.

Objective 1: *Ensuring effective confidentiality of electronic communications*
Option 5 would not satisfactorily achieve the objective. Having heard stakeholders' views in detail, within and outside the framework of the public consultation, and in light of the findings of the ePD ex-post evaluation, the conclusion has been reached that **an ePrivacy legal instrument protecting confidentiality of electronic communications is still necessary and that the repeal of such an instrument would leave citizens without an essential protection in respect of a fundamental right** recognised by the European Charter. The main reasons underpinning this conclusion are laid down below. *First*, the ePD and the GDPR do not have the same scope. The GDPR applies only to the processing of personal data of individuals. The ePD protects the **confidentiality of electronic communications as such, irrespective of whether or not personal data are being processed**. The GDPR does not apply, therefore, to communications not including personal data and does not protect legitimate interests of legal persons. For these reasons, more detailed rules were considered necessary after the adoption of Directive 95/46 for the protection of privacy and data protection in the electronic communications sector, which led to the adoption of the ePD. These reasons are still valid today. *Second*, the ePD provides for specific protection of confidentiality of communications in keeping with the general framework of protection of personal data laid down in the GDPR. While **personal data under the GDPR can be processed under a variety of legal bases**, including the necessity to perform a contract and the controller's legitimate interest, **the ePD allows confidentiality of communications to be derogated or interfered with only with the consent of the users**. In light of their particularly sensitive nature, electronic communications are given special protection under Article 7 of the Charter and in line with the constitutional traditions common to the MS. The Court of Justice has recognised on various occasions the utmost importance of ensuring effective confidentiality of electronic communications, for example in the *Digital Rights Ireland* case[131], which has led to the invalidation of the Data Retention Directive 2006/24/EC. ***Third, the ePD gives citizens specific rights and protections***. This is for example the case of the protection of confidentiality and integrity of terminal equipment (Article 5(3)), allowing interference with smart devices to be put in place only with the user's informed consent (thus protecting users against viruses, spyware or other malware), the specific protection against spamming and direct marketing, the obligation to delete traffic data, the right not to appear in directories of subscribers, the right to block calls from certain numbers, etc. Under this option, **users would lose rights that today they are granted under current EU legislation**. While the impact of the repeal on the level of confidentiality of communications will very much depend on how national authorities and courts would interpret and enforce the GDPR rules, in the absence of specific information and guarantees on this issue it is appropriate to consider that the present option may lead, at least in theory, to a reduction of the level of protection of confidentiality.
Objective 2: *Ensuring effective protection against unsolicited commercial communications*
Unsolicited commercial communications would be covered by Article 21 of the GDPR which gives data subjects the right to object to data processing for direct marketing purposes. The repeal of the ePD would thus constitute a step-back in terms of protection for a number of marketing communications that are currently subject to the opt-in regime such as automated calling machines and electronic mail.
Objective 3: *Enhancing harmonisation and simplifying/updating the legal framework*
Option 5 will achieve the objective. While in principle the full applicability of the GDPR may

[131] Cited above.

guarantee high level of harmonisation, at the same time, the matters currently set forth by the ePrivacy Directive would need to be interpreted and applied by supervisory authorities. The removal of the specific rules may lead to further discrepancies across MS in the future, insofar as authorities may have different views and apply the GDPR rules differently.

Efficiency/economic impact

The Commission and MS would have to bear the cost of the legislative process as per under Option 2, 3 and 4. For the rest, as the ePD would be repealed under this Policy Option, all costs stemming from the ePD for the Commission and ePD would be abolished.

The ECS industry will have to adapt to the new environment. Since certain requirements laid down in the ePD will no longer apply to them, it can be expected that no costs related to compliance and administrative burden with the ePD will be incurred. It has to be noted in this regard that, while these costs would no longer be based on the ePD, businesses would still need to implement certain rules based on the GDPR or other legislation. For example, the GDPR also contains obligations in relation to personal data breach notifications.

In conclusion, the present option would generate cost savings in terms of technological neutrality and some simplification.

Impact on SMEs, competiveness and competition

This option is expected to have positive impact on ECS providers, by removing the specific rules in the electronic communications sector. This would increase their competitiveness vis-à-vis OTTs on the OBA side of the market. The GDPR would apply to all operators in the ECS market, thus guaranteeing a **level playing field**. There could be a consequential increase in revenues and competitiveness from ECS and a potential shift of revenues from OTTs to ECSs.

This option would significantly clarify and simplify the legal framework. SMEs would benefit from such additional clarity and simplification of the legal framework, other than from the cost savings relating to the repeal of the ePD. This would translate into lower costs for online businesses, many of which are start-up and therefore very small enterprises.

Environmental impact

No significant environmental impact expected for any of the options.

Social impact

Option 5 may produce positive effects for the employment, to the extent that they may encourage ECSs to invest more in the data economy and thus hire more people in new projects/areas.

Other impacts

Internal market

The impact of internal market of this option is rather mixed. The removal of the specific rules on confidentiality of communications may lead to further discrepancies across MS in the future, to the extent that MS are no longer bound by harmonised rules in this context.

Impacts on Fundamental Rights

As explained in relation to Objective 1, the repeal of the ePD would remove the specific protection of the fundamental right under Article 7 of the Charter. The impact on this fundamental right is thus negative.

Impacts on innovation

The impact on innovation is positive. Since they are no longer bound by the ePD, ECS providers would be able to invest resources in innovative business models capitalising on the wealth of data on electronic communications they have access to. This may translate into new innovative offerings in the market for consumers and businesses and greater spin in the data economy.

Stakeholders' support
In the Public Consultation, a strong majority of respondents acknowledged that the rules on confidentiality of communications in the electronic communications sector **remain largely relevant**[132], although there are differences depending on the types of stakeholders asked[133]. More specifically, close to two thirds (61.0%) of all respondents indicated that there is an **added value of specific rules ensuring confidentiality of electronic communications**. This view is in particular supported by **citizens and civil society as well as public bodies (83.4% and 88.9%** respectively). Public authorities (EDPS, WP29 and BEREC) expressed similar views. None of these stakeholders backed up the option of repealing the ePD. **Operators** concerned in the ECS sector and the tech industry broadly support the deregulation of the sector and consider that the general data protection rules provide sufficient protection[134]. Close to one third (63.3%) of the industry respondents did not consider that there is an added value of having specific rules on confidentiality of electronic communications.

6. HOW DO THE OPTIONS COMPARE?

6.1. Comparison of options

In this section, the comparison of the options in the light of the impacts identified is presented. The options are assessed against the three core criteria of effectiveness, efficiency and coherence. **Annex 13** summarises and presents in table form the comparison of the policy options in terms of effectiveness, efficiency and coherence as well as comparison of impact on each category of stakeholder. It also presents a table comparing the overall expected costs and expected benefits/cost-savings of each options.

6.1.1. Effectiveness

The analysis of the **baseline scenario** (section 5.1) has shown that if no action is taken, **the problems are likely to continue** and grow more important as the time passes. While the measures identified in **Option 1** may **to a certain extent improve** the quality of implementation, there is no guarantee that the objectives could be effectively achieved without a change in the law. Many of the issues identified can only partially and hypothetically be tackled by interpretative communications or standards.

Option 2 would **partially achieve all the objectives**. The extension of the scope of the ePD would fill important gaps in the protection and ensure a level playing field. The selective measures in the field of unsolicited communications would reinforce citizens' protection against nuisance calls. The clarification of certain provisions combined with the selective repeal of some others would also contribute to the objectives. However, the Option presents some limitations as it does not sufficiently address the weakness of the current cookie consent mechanisms. Finally, the option would not completely address the problem relating to the lack of cooperation and consistency in cross-border cases.

Option 3 achieves the objectives in a significant way. In addition to the benefits of Option 2, the introduction of clear transparency requirements with regard to e.g. tracking in public spaces would contribute to significantly increasing consumer awareness and would help them make informed decisions. By mandating privacy-friendly settings in

[132] Question 6 of the Public Consultation.
[133] Question 6 of the Public Consultation.
[134] DLA Piper, cited above and Joint Industry Statement signed by 12 associations representing telecom and tech businesses; http://www.gsma.com/newsroom/press-release/empowering-trust-innovation-repealing-e-privacy-directive/. See also CERRE, *Consumer Privacy in Network Industries*, http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf, p. 15.

browsers and/or similar software, this Option would greatly facilitate the user-centric management of privacy and security related permissions concerning online browsing. The generalisation of the opt-in requirement would further enhance the protection of users against unsolicited commercial communications. At the same time, the option would enhance harmonisation and simplification. The broadening of the exceptions for the consent requirement, with adequate privacy safeguards, would guarantee this flexibility. The repeal of redundant provisions would simplify the legal framework. Finally, the allocation of enforcement powers to a single category of authorities, the authorities competent to enforce the provisions of the GDPR, with the extension of the GDPR consistency mechanism shall support a uniformed interpretation of the rules and more effective enforcement.

By contrast, the introduction under this Option of a possibility to process communications data (e.g. traffic and location data) without users' consent to profile and deliver targeted advertisement (measure No 10(e)), albeit under strict privacy safeguards, undermines the effectiveness of the option vis-à-vis its objective of reinforcing the protection of confidentiality of communications. The possibility for OTTs and ECSs to interfere with the confidentiality of electronic communications without the consent of the users strongly reduces citizens' control over their communications and therefore constitutes a significant limitation in relation to the present objective. While the negative effects on privacy protection would be limited by strict safeguards, i.e. as approved by the competent authorities, the overall compatibility of this element with the general objective of reinforcing confidentiality of communications is questionable.

Option 4 contains most of the measures included in Option 3, but it goes further in the protection in a number of respects. Under this perspective, the ban on "cookie walls" would significantly limit online tracking. However, it should be noted that cookies/OBA allow to finance freely-accessible content. Websites may need to put in place paying subscriptions; if users are not willing to pay with money, this may affect their revenues. With respect to unsolicited commercial communications, the repeal of the exception to the opt-in rule would further strengthen the protection of users from unsolicited communications by electronic mail (e.g. email and SMSs). In conclusion, the option is expected to significantly enhance protection and thus achieve Objectives 1 and 2 (except for the measure allowing processing without consent), but also adversely affect business models financed on OBA and thus go, in part, against objective 3 aiming to simplify the legal framework.

Under **Option 5,** confidentiality of communications will decrease because operators would be allowed to process communications data in the absence of the user's consent. Communications not containing personal data which are not covered by the GDPR would not be covered. As far as unsolicited communications are concerned, the generalisation of the opt-out rule would be a step-back as today a large portion of communications is subject to an opt-in consent. By contrast, Option 5 would achieve to a great extent the simplification objective, by ensuring a single set of rules applicable across all services, the necessary flexibility and a strong system of enforcement.

In conclusion, **Option 3** and **4** are the most effective options.

6.1.2. Efficiency

The **baseline scenario** would not entail any additional cost. A Commission's external study[135] calculated that the overall cost related to the ePD for businesses operating in the

[135] SMART 2016-0080, cited above.

EU a website using cookies amounted to approximately EUR 1.8 billion in the period 2002-2015. However, this cost is projected to gradually decrease until 2030 to approximately EUR 1.4 billion per annum.

Options 1 and 2 would entail additional costs compared to the baseline[136]. The estimate of the magnitude of these costs has been quantified by a Commission external study[137]. According to the Study, **Option 1** would entail additional costs for 5% compared to the baseline. The additional compliance costs of **Option 2** are estimated to be higher (15% compared to the baseline). **Option 3** would instead lead to a substantial reduction in overall compliance costs essentially thanks to the measures streamlining and simplifying the consent rules and greater harmonisation (up to 70% lower compliance costs in the best case scenario). **Option 4** would finally lead to a much lower reduction in compliance cost by (5%). **Options 2 and 4** are expected to present significant opportunity costs as well. Opportunity costs are expected to be present also in Option 3, although to a significantly lower extent.

Imposing a general opt-in requirement under **Option 3 (and 4)** implies, by contrast, some additional compliance costs for businesses, as they will have to review their business models and limit marketing only in respect to those subscribers for which they have received prior consent. This is expected to raise the costs of a marketing campaign, as businesses would have to review and update their practices. This effect will be felt only in those MS that have at present adopted the opt-out system. The analysis of the data concerning the situation in MS, however, has shown that the largest majority of traders would be affected by this change, especially as far as fixed line calls are concerned (88% of traders) but also for mobile phones (61%). Considering that the evidence collected during the REFIT evaluation did not lead to conclude unequivocally that the problems related to voice-to-voice unsolicited communications are caused by the opt-out systems, but rather as the result of its ineffective implementation, the proportionality of the option does not seem to be demonstrated.

Option 5 is considered to be the least expensive option. The repeal of the ePD would significantly simplify the legal framework, by abolishing the sector-specific regulation in the ECS sector. However, while these costs would no longer be based on the ePD, the sector-specific rules now laid down in the ePD would be replaced by corresponding provisions of the GDPR. For example, the GDPR also contains obligations in relation to personal data breach notifications. Thus, some of these costs would still be incurred even after the repeal of the ePD, but for other reasons.

In conclusion **Option 5** and **3** are the most efficient options.

6.1.3. Coherence

The **Baseline** and **Option 1** would not entirely solve the internal and external coherence issues identified. In particular, the asymmetric regulation of ECS and other forms of online communications would not be removed. Inconsistent enforcement would not be effectively addressed.

Option 5 would enhance the overall coherence of the system, as it would eliminate the dual regime of the protection of personal data in the electronic communications sector and make the GDPR the only legal instrument in the field of data protection. However,

[136] We take into account here essentially compliance costs, as costs stemming from administrative burden are much less significant overall according to the study.
[137] Id.

the repeal of the specific rules of confidentiality of communications would remove the specific protection of confidentiality of communications in line with the Charter, especially with regard to legal persons and communications not involving personal data, which are not protected under the GDPR.

Options 2, 3 and **4** do not present specific coherence issues, although they represent a significant deviation from the status quo and result in a significant expansion of the scope of the current ePrivacy instrument. The scope would be enlarged in relation to OTTs. While this may be seen as a significant extension, it is also a necessity given the need to ensure confidentiality of communications, irrespective of the technology used (i.e. technological neutrality). The same arguments apply as well to the clarification of the applicability of the confidentiality rules to publicly available private networks such as Wi-Fi and to IoT connected devices.

As far as the GDPR is concerned, the relationship with the general data protection rules will not change under **Options 1, 2, 3** and **4**. The ePrivacy instrument will remain a specific law aiming to protect confidentiality of electronic communications in accordance with Article 7 of the Charter. If personal data are involved, the GDPR rules will continue to apply on the top of the ePrivacy instrument for any matters that is not specifically regulated by the latter. In line with the expansion of the scope of the ePrivacy rules, some matters that were previously covered exclusively by the GDPR will be covered in the future also by the ePrivacy instrument. This is the case, as already mentioned, for OTTs, publicly accessible Wi-Fi networks and IoT connected devices related communications. Option 3 and 4 will further boost alignment with the GDPR, as they will provide for the application of the GDPR enforcement and consistency system.

While the basic relationship with the RED will not change, **Options 3** and **4** will include the additional requirement for some software acting as "user agent" to set out specifically described privacy settings. User agent software would include, for example, Internet browsers. This requirement is considered coherent with the RED, which covers radio equipment and includes a requirement for such equipment to incorporate privacy safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected[138]. The options in question would not otherwise affect in any manner the operation of the RED and the power of the Commission to adopt delegated acts or European standards under that Directive to further specify the practical implementation of this requirement.

6.2. Outcome of the comparison

Based on the above comparison, it appears that **Option 3** is the best option to achieve the objectives, while taking into account its efficiency and coherence.

Options 3 and **4** are the most effective options to achieve the objectives of the review, with **Option 4** guaranteeing greater user protection and thus achieving the objectives 1 and 2 to a greater extent. However, in terms of efficiency, **Option 4** is more expensive and thus less efficient, both in terms of compliance and opportunity costs. Under this perspective, Option 3 is considered a more proportionate, and thus preferable, solution compared to Option 4. By contrast, **Option 3** has positive effects in terms of efficiency, as it is expected to drive compliance costs down (while potentially raising some non-insignificant opportunity costs). **Option 3** is also coherent both internally and externally. **Option 1** and **2** are much less effective options. While **Option 5** would have very positive effects in terms of efficiency, it does not guarantee that the objectives are satisfactorily achieved.

[138] Article 3(e) of the RED.

Although **Option 3** is the best option, while taking into account its efficiency and coherence, specific measures included in this option raise particular concerns in terms of effectiveness and efficiency (cost-effectiveness). In particular, **the possibility to process communications data without consent** of the users for marketing purposes (measure No 10(e)), albeit with privacy safeguards, would strongly limit the effectiveness of the option vis-à-vis the objective of ensuring effective confidentiality of electronic communications. In addition, **the introduction of a mandatory opt-in regime** for voice-to-voice live calls would generate costs, without offering sufficient guarantees that the underlying issues would be resolved by this measure.

In view of the above, the elimination of the measure of processing for marketing purposes without consent would ensure a better result in relation to Objective 1. At the same time, the elimination of the extension of the opt-in would ensure a better result in terms of efficiency. There is no sufficient evidence that this would significantly undermining objective 2. **These two measures of Option 3 should therefore not be retained**. **The preferred option is, therefore, Options 3 without these specific measures (processing without consent for marketing purposes** measure No 10(e) **and mandatory opt-in for voice-to-voice marketing calls** (measure No 4)**).**

6.2.1. REFIT Dimension of the preferred option: simplification and administrative burden reduction

The preferred policy option presents several elements of simplification and reduction of the administrative burden on businesses. These elements, which have all been explained in the context of the analysis of the impacts, are also listed below and, where possible, quantified:

- **Technological neutrality**: The proposal would introduce a fully technologically neutral approach, thus ensuring that the rules are future proof and remain effective despite the evolution of technology;
- **Privacy by design and technological solutions to manage complex issues related to consent online**: The proposal would require certain software providers (user agents) to enable general settings in a way that they can be used to manage privacy choices in a centralised way. This would greatly simplify the management of consent online for users, as the latter will be able to set their privacy choices once for all websites and applications (this does not exclude the possibility to derogate in specific instances). This would bring out significant savings for businesses having a website (up to -70% of the costs related to the ePrivacy as estimated in the external study[139]). At the same time, it would greatly simplify Internet browsing, limiting the interference of invasive cookie banners.
- **More consistent enforcement**: thanks to the streamlining of enforcement by means of the consistency mechanism, and in particular the allocation of enforcement to GDPR authorities, greater consistency and legal certainty in cases having cross-border dimension would be ensured.
- **Greater transparency of unsolicited marketing calls**: thanks to the introduction of the prefix and other measures relating to the transparency of marketing calls, most users (unless their telephone equipment does not display the identity of the calling line) will be enabled to identify a marketing call before

[139] SMART 2016-0080, cited above.

picking up the phone. This will increase transparency and allow users to reject particular calls. In perspective, this may reduce complaints against unsolicited marketing calls.

- **Clearer exceptions to the privacy of terminal equipment**: the proposal would spell out more clearly and in a more comprehensive manner the cases where interferences with the privacy of terminal equipment are permitted. In this way, the proposal would identify permitted uses for specific legitimate purposes not presenting concrete privacy risks, thus reducing false positives caused by the over-inclusive character of the present rules.
- **Elimination of redundant or outdated provisions**: the proposal would eliminate the provisions on security of the processing of personal data in the electronic communications sector, which strongly overlap with the corresponding provisions in the GDPR and the Telecom Framework, thus further simplifying the legal framework. Moreover, it would eliminate the provision on itemised billing, which has been judged as no longer necessary in view of the evolution of technology and market reality.

The external study supporting the present impact assessment attempted to estimate the impact on costs of the preferred policy option, on the basis of a pragmatic model based on a wide range of assumptions reflecting the general scarcity of data. Taking these limitations into account, the external study identified three distinct implementation scenarios, according to the entity who will establish the dialogue box between the user having chosen "reject third party cookies"/ "do-not-track" settings and websites visited wishing the Internet user to reconsider his/her choice[140]. The entities who could be put in charge of this technical task are three: 1) the software providers concerned; 2) the third party tracker (e.g. the advertising networks); 3) the individual publishing websites. According to the study, this option would lead to **overall savings** in terms of compliance cost compared to baseline scenario of 70% (948.8 million savings) in the first scenario (browser solution), 60% (813.2 million) in the second scenario (tracking company solution) and of 5% (67.8 million) in the third scenario (publisher solution). As overall savings largely derive from a very significant decrease of the number of affected businesses, the individual amount of compliance costs one business is expected to incur – on average – would be higher than today. Far from being precise figures, they give however a rough idea of what the magnitude of the impact on businesses could be. The tables including the calculations relating to the key quantitative findings are in **Annex 8**, together with an overall explanation of the model, the related assumptions and limitations.

[140] The web site may decide to set tracking as a condition for accessing the content. In case users wish to access the content in the "tracking" website they would receive a request to authorise the tracking for that specific website (or for all the web sites that are related to a third party tracking) and then would have to decide whether to accept or refuse.

Impacts	Baseline Option 0	Option 1: Soft law measures	Option 2: limited reinforcement and simplification	Option 3: measured reinforcement and simplification	Option 4: far-reaching reinforcement and simplification	Option 5: Repeal of the ePD
Effectiveness	**0**	✓✓	✓✓✓	✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	≈
Economic	**0**	×	×××	✓	×××××	✓✓✓
Environmental	**0**	**0**	**0**	**0**	**0**	**0**
Social	**0**	**0**	**0**	**0**	×	**0**
Coherence	×	×××	✓✓✓	✓✓✓✓	✓✓✓	✓
Stakeholders' support	**0**	×	✓(citizens) × (industry)	✓✓(citizens) ××(industry)	✓✓(citizens) ××× (ind.)	✓(industry)/× (citizens)
Total	×	×××	✓✓✓	✓✓✓✓✓✓✓✓✓✓	✓✓✓	✓✓✓✓

Table 6: Overall impact of the various policy options. The symbols "✓" and "×" indicate respectively positive (✓) and negative (×) impacts, the number of the symbols is the net result of the summing-up of the respective individual ratings of the policy option as indicated in **Annex 13** and indicates the magnitude of the change.

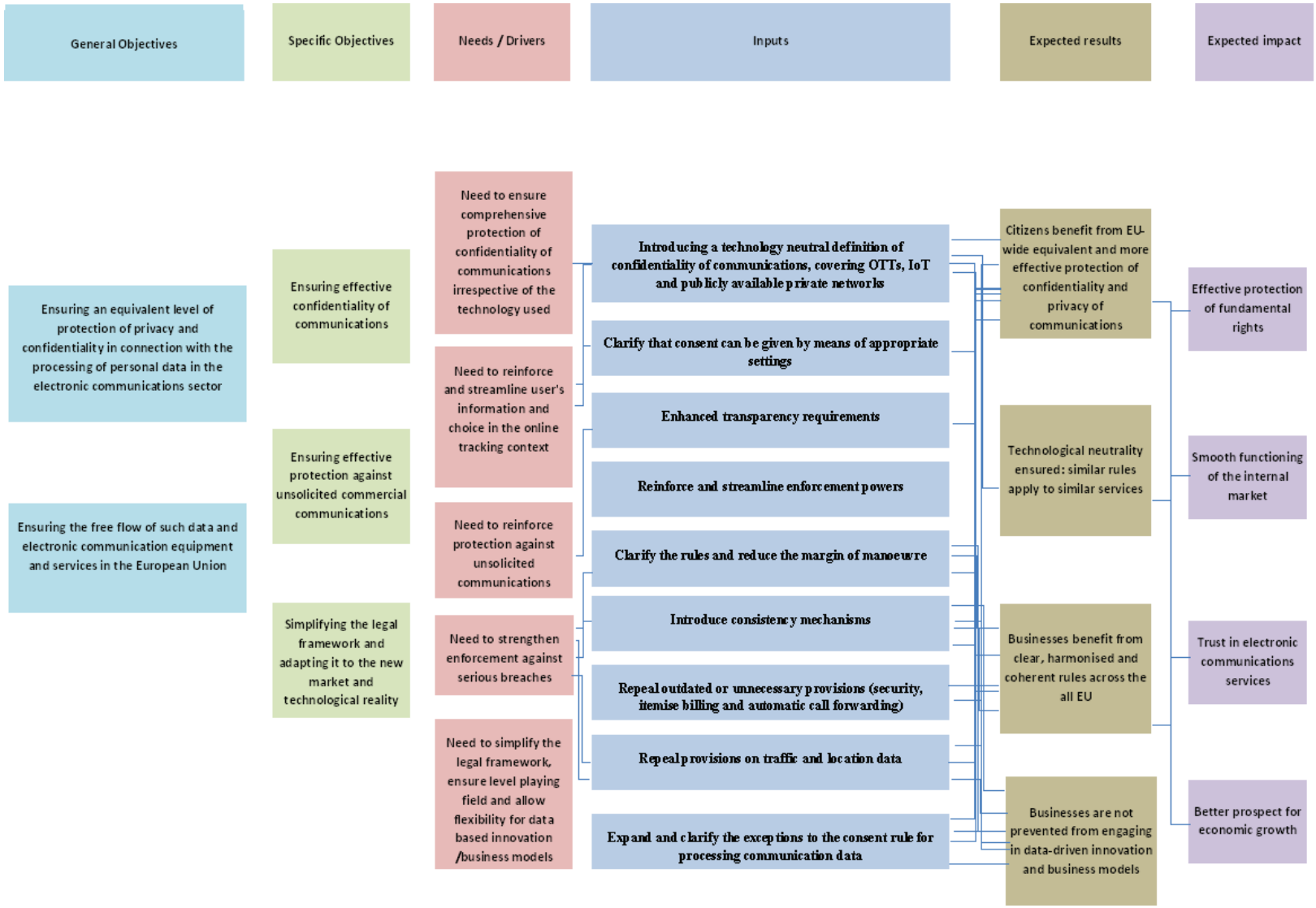
6.3. Choice of legal instrument

The preferred option entails EU legislative intervention as only a binding instrument can guarantee the translation into practice of the measures proposed and the achievement of the related specific objectives.

A regulation would be directly applicable and would not need to be implemented in national law as it would have immediate effect and is a particularly suitable instrument when the objective is the uniform application of rules in a certain area. This type of instrument would be the best to achieve the objective of ensuring a higher level of harmonisation and consistency, which is a main objectives of the ePD review. This would be particularly important for online services present in different territories. Moreover, the relationship of a revised Directive with the GDPR would be legally complicated and might lead to legal uncertainty, as it is not clear whether national laws implementing a directive can particularise or complement a general regulation.

The experience with the implementation of the ePD has shown that the minimum harmonisation approach has not guaranteed the level of harmonisation required to ensure the internal market objective. The principle of confidentiality of communications has been implemented differently across MS. This has given rise to fragmentation and created barriers in the internal market, as businesses operating cross-border have had to deal with several different national regimes. The future ePrivacy instrument would therefore adopt an approach aimed at ensuring a higher level of harmonisation by means of more detailed and precise rules than it is the case today. Nonetheless, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation where this is necessary to ensure an effective application and interpretation of such rules and to the extent that they do not conflict with any provisions of this Regulation.

Figure 3: Legislative intervention logic



7. MONITORING AND EVALUATION

This section describes the monitoring and evaluation that could be applied to assess the impact of the objectives and the preferred option. The approach to monitoring and evaluation is outlined with respect to the three main objectives that the preferred policy option will address.

Monitoring will start right after the adoption of the legislative act. It will focus on how the future instrument is applied in the MS by the market participants in order to ensure a consistent approach. The Commission will organise meetings with MS representatives (e.g. group of experts) and the relevant stakeholders in particular to see how to facilitate transition to the new rules. A report on the implementation and application of the instrument will be prepared every year, taking stock of the state of play, the progress towards the achievement of the objectives and unresolved issues.

The following list of impact indicators could be used to monitor progress towards meeting the general objectives:

Table 7: implementation strategy

Objective	Operational objective	Monitoring indicators
Ensuring effective confidentiality of communications	• Ensure that confidentiality is protected in relation to OTTs, publicly available private networks (WiFi) and IoT devices	• After 3 years of the entry into force of the regulation more than 50% of MS corresponding to 50% of the EU population have taken enforcement actions or issued general guidance on issues related to OTTs, Wi-Fi and IoT devices. • Positive feeback in Eurobarometer satisfaction survey concering online trust (+50%)
	• Ensure user-friendly management of online privacy settings	• Adoption of implementing rules (either by Commission or EU standard) • All major operators concerned (e.g., 90% of the market) adopt privacy setting solutions
	• Enhance transparency requirement	• Adoption of implementing rules (either by Commission or EU standard)
Ensuring effective protection against unsolicited commercial communications;	• Reduce the number of nuisance calls	• Positive feeback in Eurobarometer satisfaction survey (+50%)
	• Increase transparency of marketing calls	• Take-up of the prefix in MS (all MS after 1 of the adoption)
Enhancing harmonisation and simplifying the legal framework.	• Reduction in the number of competent authorities competent to apply ePrivacy rules in each MS	• Less authorities than it is the case today are competent to supervise compliance with the ePrivacy rules
	• Reduce notification fatigue	• Positive feeback in Eurobarometer satisfaction survey (+50%)

No later than 5 years after the date of application of the new legal instrument, and every five years thereafter, the Commission shall carry out an evaluation and submit the main

findings to the European Parliament, the Council and the European Economic and Social Committee.

The evaluation report will include an assessment on the basis of the five evaluation criteria of the Better Regulation Guidelines, including on whether the operational objectives of the revised instument have been reached. A particular focus will be cast on the application of the provision on confidentiality of communications.