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?

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

[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.

properly informed or feel have few alternatives to accepting[47]. Numerous sources 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

[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.

[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.

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 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].

---

[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.
[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.

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, 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.

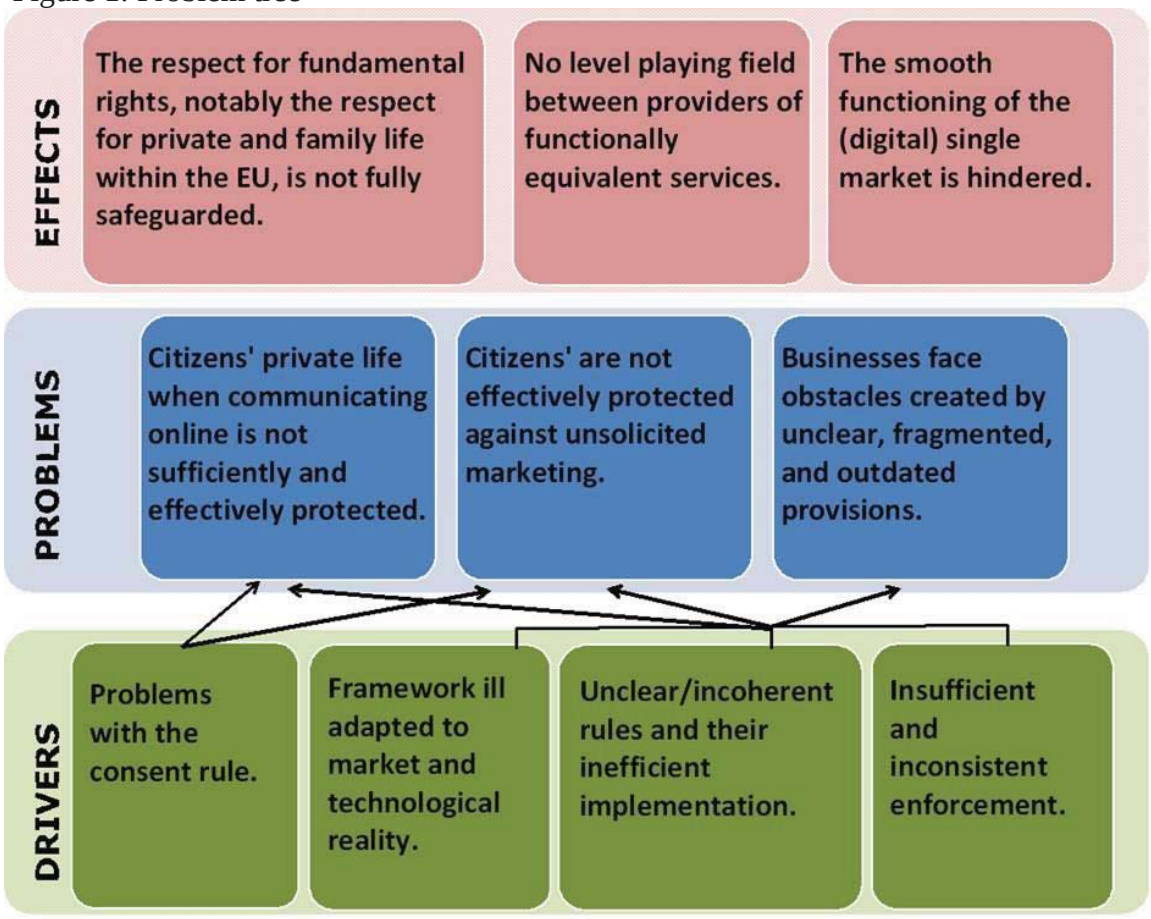
As to **unsolicited communications**, the impact on public authorities is particularly serious. As the REFIT evaluation showed, the number of complaints from citizens concerning unsolicited advertising is very high. It follows that they have to dedicate substantial resources to this issue, with clear 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

[59] SMART 2016/0080, cited above.
[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.

jurisdictional issues may lead to the legitimacy of enforcement actions being contested. The case of the Belgian DPA against Facebook illustrates this problem[64].

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

[64] Fioretti J, *Facebook wins privacy case against Belgian data protection authority*, http://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV

[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*

conditions for the consent to be considered as freely-given[66]. It will also reinforce the 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**

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.

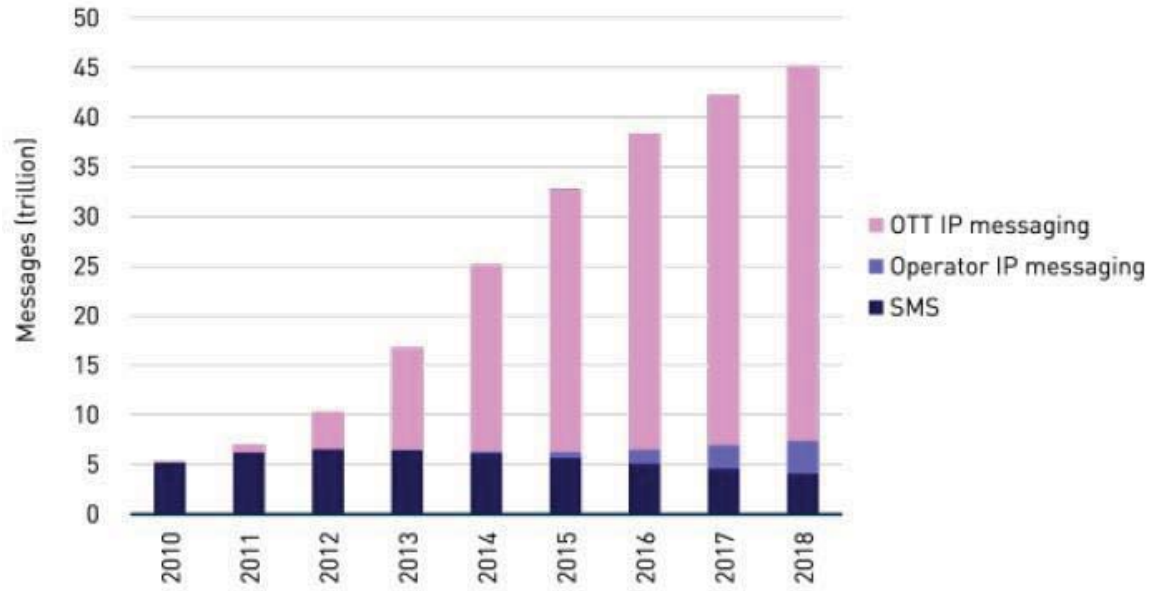
[67] See, e.g. WP29 Opinion 9/2014 on device fingerprinting, cited above.

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 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



[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.

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 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

[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.

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. 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.

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

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.

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].

[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.

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].

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

[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.
[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.

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 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**

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

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 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

[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.*"

[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.

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 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").

[85] Article 4.
[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.

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.
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.

[88] Article 13(2).
[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. 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**.

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

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

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.

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

[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).

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.

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.

[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/

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*
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

[98] DLA Piper, cited above.

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 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

[99] SMART 2016/0080, cited above.

[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.

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 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, **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

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

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 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

[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.

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 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

[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.

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 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

[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.
[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.

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 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

[117] For the assessment of opportunity costs, see SMART 2016/0080, cited above.
[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.

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 (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

[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.

[122] SMART 2016/0080, cited above.

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 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.

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.

[123] SMART 2016/079, cited above.
[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.

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 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

[128] SMART 2016/0080, cited above.

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 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

[129] SMART 2016/0080, cited above.

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

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

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

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 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

[131] Cited above.

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.

[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.

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 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 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

[135] SMART 2016-0080, cited above.
[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.

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, 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.

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)**).**

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

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 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

[139] SMART 2016-0080, cited above.

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.

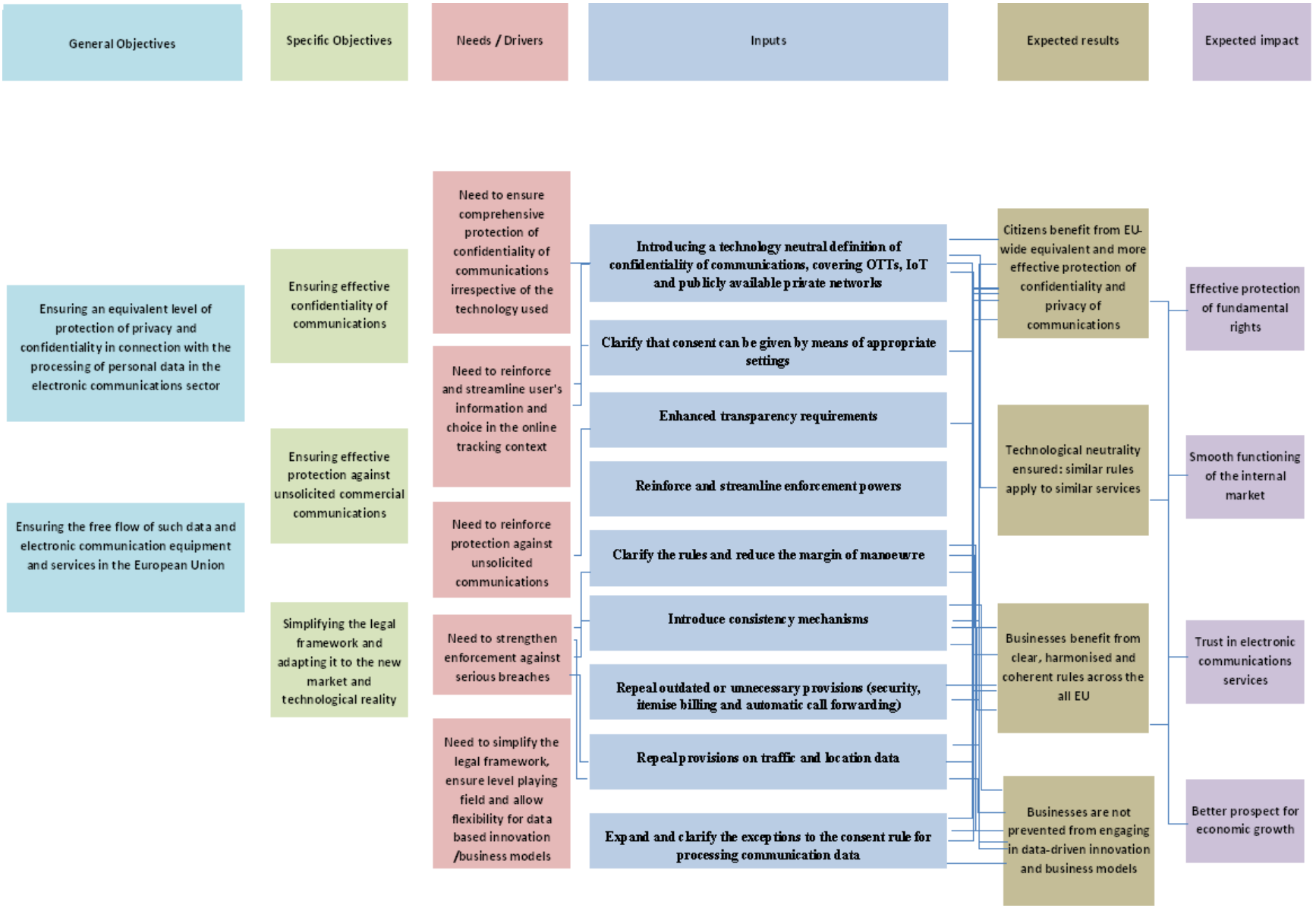
6.3. Choice of legal instrument

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.

EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 3 final

PART 2/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for 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}

LIST OF ANNEXES

ANNEX 1: PROCEDURAL INFORMATION

1.1. Identification

This Staff Working Document was prepared by Directorate H "Digital Society, Trust & Cybersecurity" of Directorate General "Communications Networks, Content and Technology". The RWP reference of the initiative "reform of the e-Privacy Directive" is 2016/CNECT/007.

This Staff Working Document is accompanied by the Fitness Check SWD for the current ePrivacy Directive, conducted in the context of the REFIT programme. The reference of the "REFIT evaluation of the E-Privacy Directive" is 2016/CNECT/013. The ePrivacy Directive is assessed not only in terms of achievement of the original goals, but also in view of potential simplification and reduction of the regulatory burden.

1.2. Organisation and timing

Several other services of the Commission with a policy interest in the review of the ePrivacy Directive (ePD) have been associated in the development of this analysis. The ePD Inter-Service Steering Group ("**ISSG**") met for the first time on the 24 February.

A second ePD Inter-Service Steering Group meeting took place on, 26 July 2016.

A third ePD Inter-Service Steering Group took place on and 26 August 2016.

A fourth and final meeting took place on 12 December 2016.

In the ISSG, chaired by SG, DG CONNECT, was flanked by DG CNECT, DG COMP, DG JUST, DG GROW, DG ECFIN, DG FISMA, DG TAXUD, DG TRADE, DG RTD, DG JRC, DG EMPL, DG EAC, DG HOME, DG ENV, DG REGIO, DG HOME, DG ENER, DG MOVE, EUROSTAT, EPSC, together with the Legal Service.

DG CONNECT also benefited from the support received by the JRC Cyber & Digital Citizens' Security Unit for the assessment of technical aspects relating to online tracking and security and ENISA on the assessment of the ePD provisions relating to security and privacy of terminal equipment.

1.3. Consultation of the Regulatory Scrutiny Board

The Impact Assessment Report was examined by the Regulatory Scrutiny Board on 28 September 2016. The Board gave a positive opinion on the understanding that the report shall be adjusted in order to integrate the Board's recommendations with respect to the following key aspects:

Board's Recommendations	**Implementation of the recommendations into the revised IA Report**
1. The report should clarify the scope and coherence of the initiative, notably in relation to the existing ePrivacy Directive, the General Data Protection Regulation and the Radio and Telecommunication Terminal Equipment Directive. It should provide credible assurances that overall consistency will be ensured and overlaps avoided	*1. The scope of the initiative and the assessment of the coherence with complementary legal instruments, including the General Data Protection Legislation, the Telecom Framework and the Radio Equipment Directive and the need for a separate ePrivacy instrument, has been further clarified and developed, thereby ensuring that overlaps would be avoided (see Section 6.1.3). A specific section was added in Annex 4 clarifying the scope, objectives and the main content of the current ePD and its relationship*

	with other related pieces of legislation.
2. The baseline scenario should be further elaborated and the options should be described with more detail	*2. The baseline scenario has been clarified in the revised report, notably by evaluating more precisely how the situation would evolve with no policy change with respect to the ePrivacy Directive and full implementation of the GDPR and the RED (see Section 1.6). Moreover, the revised report has clarified and further specified the scope and implications of each of the privacy options. In particular, the measures concerning confidentiality of terminal equipment and related online tracking and the measures concerning enforcement and supervisory authorities were specified (Chapter 4).*
3. The analysis of impacts should be more balanced across the options and strengthened as regards the overall costs and benefits, notably affecting SMEs	*The analysis of the impacts has been strengthened and made more balanced across all the options, clarifying and reinforcing the description of the expected costs and benefits (see the respective parts in Chapter 5, see in particular the economic assessment parts of Option 2 (Section 5.3) and 3 (Section 5.4)). The analysis of the impact of each option on SMEs has been expanded and streamlined, both in the report and in an annex (see the respective parts in Chapter 5 and Annex 7). The report clarifies that the proposal is future-proof, highlighting the technology neutral and funcionality and value-based approach of the preferred policy option (see, e.g., Sections 4.4. 5.4 and 6.2.1). Finally, the report explains more comprehensively the analysis of the impact of the proposal on OBA business models (see Section 5.4).*
4. In the context of REFIT, the report should emphasize the simplification and burden-reduction elements of the various provisions of the preferred option and bring out the quantitative elements of the analysis	*A specific section has been added to the report describing the elements of the preferred policy option that simplify the legal framework or reduce administrative burdens (see Section 6.2.1).*

1.4. Evidence used

The Commission gathered qualitative and quantitative evidence from various sources:

(1) The contributions to the ePD review **public consultation**, a summary of which is attached in Annex 2 to this report.
(2) A **Eurostat community survey on ICT usage by households and individuals** of December 2015, (specific questions on citizens' level of awareness of cookie tracking)[1];
(3) **A Eurobarometer on e-Privacy** (Flash Eurobarometer 443) was conducted on 7th and 8th of July throughout the 28 Member States over the phone with in total 26,526

[1] http://ec.europa.eu/eurostat/data/database?node_code=isoc_cisci_prv.

respondents which specifically enquired about citizens' views on online privacy and the relevance of existing provisions of and possible changes to the ePrivacy Directive.

(4) **Ad hoc consultations** of (and discussions with) relevant EU expert groups: BEREC[2], ENISA[3], the Article 29 Working Party[4], the European Data Protection Supervisor, the REFIT stakeholder platform, Europol[5], COCOM and the CPC Network between January and July[6].

(5) **Targeted consultations** with EU expert groups which led to the following contributions:
   i. Article 29 Working Party Opinion[7]
   ii. EDPS[8]
   iii. BEREC[9]
   iv. ENISA[10]
   v. JRC[11]
   vi. CPC network[12]

(6) **Two workshops and two roundtables organised by the Commission:** one workshop was open to all stakeholders (12 April 2016) and one was limited to the national competent authorities (19 April 2016). The roundtables were chaired by Commissioner Oettinger; included stakeholders representing different interests.

(7) **Ad hoc meetings** with representatives of the affected industry, public authorities and civil society organisations as well as written input received from these stakeholders.

(8) **Evidence gathered through COCOM:** Already as of September 2014, the Commission sent a questionnaire through the Communications Committee (COCOM), which gathers the representatives of authorities responsible for electronic communication, requesting Member States to detail how they have implemented Article 4.2 of the ePrivacy Directive**.** More generally speaking, regular discussions took place with the COCOM committee on the implementation of the ePD in the context of COCOM meetings.[13]

(9) **Literature review of relevant reports.** This includes among others Opinions of Article 29 Working Party, Opinions of BEREC, Opinions of the Berlin Group on Telecommunications, Opinions of the EDPS[14] as well as reports and studies from the industry[15], many sent in the context of the public consultation.

---

[2] Body of European Regulators for Electronic Communications.
[3] The European Union *Agency* for Network and Information Security.
[4] The Article 29 Working Party is composed of all the data protection authorities of the EU.
[5] The European Union law enforcement agency.
[6] The CPC Network is s a network of authorities responsible for enforcing EU consumer protection laws. Some of these authorities are in charge of enforcing the national provisions implementing Article 13 of the ePD.
[7] Article 29 Working Party Opinion 03/2016 on the evaluation and review of the ePrivacy Directive 2002/58/EC, WP 240.
[8] EDPS opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.07.2016.
[9] BEREC response to the ePrivacy Questionnaire, 29.07.2016.
[10] ENISA working paper on the review of the ePrivacy Directive - Article 4 – security of processing, July 2016; ENISA working paper on the review of the ePrivacy Directive – Article 5.3 – cookies and similar techniques, July 2016.
[11] Informal inputs were requested from JRC on experience in lab with cookie banners and on technical aspects related to security.
[12] The CPC network did not reply collegially but invited its members to reply to the ad hoc consultation. Repliers were received from Spain, Norway, Denmark and Romania.
[13] See CIRCABC website on COCOM committee.
[14] E.g. EDPS Opinion for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC, 18 July 2008, C181/1 OJ; 2nd EDPS Opinion on the review of Directive 2002/58/EC

(10) **Desk research and literature review done in-house by DG CONNECT;**

(11) **External expertise** collected in three studies:

- Study "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071[16]). The study examined whether the ePrivacy Directive has achieved its intended effects and puts forward recommendations for future revision and also assesses how the ePrivacy Directive and the proposed Data Protection Regulation (GDPR) will operate together.

- Study "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector" (SMART 2016/0080 under Framework Contract SMART 2013/0065 Lot 2). The study supports the Commission in gathering the evidence base needed to evaluate the ePrivacy Directive (and covering the provisions not evaluated in the first study). It also assists the Commission in assessing the various policy options, notably from an economic perspective. The final report of the study will be published in the fourth quarter of 2016.

- Study on "future trends and business models in communications services and their regulatory impact" (SMART 2013/0019). The Study assesses future trends and business models in the communications services markets, with particular focus on the relationship between electronic communication services providers and the so-called over-the-top providers.

---

concerning the processing of personal data and the protection of privacy in the electronic communications sector, 9 January 2009, C128/04; EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data 7 October 2011; Article 29 WP Opinion 1/2003 on the storage of traffic data for billing purposes of 29 January 2003; Article 29 WP Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive; Article 29 WP Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC of 27 February 2004; Article 29 Working Party, Opinion 2/2006 on privacy issues related to the provision of email screening services, WP 118 adopted 21.02.2006; Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171 adopted 22.06.2010; Article 29 Working Party, Opinion 13/2011 on Geolocation services on mobile devices, WP 185 adopted 16.05.2011; Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP 194 adopted 07.06.2012; Article 29 Working Party, Opinion 02/2013 on apps on smart devices, WP 202 adopted 27.02.2013; Article 29 Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208 adopted 02.10.2013; Article 29 Working Party, Opinion 9/2014 on the application of Directive 2002/58/EC to device Fingerprinting, WP 224 adopted 25.11.2014; Article 29 Working Party, Report Cookie Sweep Combined Analysis, WP 229 adopted 03.02.2015; Berlin International Working Group on Data Protection in Telecommunications Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential of 15-16 April 2013; Norway Datalsynet THE GREAT DATA RACE How commercial utilisation of personal data challenges privacy; Report, November 2015. ENISA (June 2016) Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing; Working Paper: Update on Privacy and Security Issues in Internet Telephony (VoIP) and Related Communication Technologies, 59th meeting, 24-25 April 2016, Oslo (Norway). DLA Piper, ETNO "*Study on the revision of the ePrivacy Directive"*; August 2016 and previous versions; VDAV study Quelle Ipso November 2015; CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets", 2014, 15; European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019), p54, 56, 60; The Information Technology & Innovation Foundation, Daniel Castro and Alan McQuinn, "*The Economic Costs of the European Union's Cookie Notification Policy"*, November 2014 (US); Directorate-General for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015.

[16] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080), https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

ANNEX 2: REFIT EVALUATION OF THE E-PRIVACY DIRECTIVE EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

The ePrivacy Directive (2002/58/EC) sets forth rules guaranteeing the protection of privacy in the electronic communications sector. It aims to ensure that the protection of confidentiality of communications, in line with the fundamental right to the respect of private and family life enshrined in Article 7 of the EU Charter of Fundamental Rights, is guaranteed.

The ePrivacy Directive requires providers of electronic communications services such as internet Access and fixed and mobile telephony to:

(1) take appropriate measures safeguarding the security of electronic communications services (specific objective);
(2) ensure confidentiality of communications and related traffic data in public networks (specific objective).

The Directive also provides protection for users and subscribers [17] of electronic communications services against unsolicited communications.

In 2015 the Commission considered it necessary to assess whether the rules of the ePrivacy Directive have achieved their main objectives, namely ensuring an adequate protection of privacy and confidentiality of communications in the EU, and whether these rules are still fit for purpose in the regulatory and technological context. The Regulatory Fitness and Performance (REFIT[18]) evaluation assessed the Directive against a number of indicators pursuant to the Better Regulation guidelines, namely: effectiveness, efficiency, relevance, coherence and EU added-value. The Commission also sought scope for simplification of the rules, whenever appropriate, without undermining the objectives of the ePrivacy Directive.

The evaluation covers the whole EU and the period from 2009 to 2016. The assessment is based on evidence gathered by a public consultation, a Eurobarometer, structured dialogues, external studies, monitoring reports, policy documents of the Commission and other relevant literature. Robust economic data to support the assessment have been difficult to find. Statistics and other quantitative data on the compliance costs stemming from the ePrivacy Directive either do not exist, or are not disclosed by the entities subject to the obligations. To corroborate the findings of the evaluation, the evaluation process has therefore built on the sources mentioned before.

[17] This ensures the application of the Directive not only to information related to natural persons but also to information related legal persons.
[18] OM(2012) 746, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Regulatory Fitness, 12.12.2012.

Findings

The provisions of the Directive remain fully **relevant** to meet the objectives of ensuring privacy and confidentiality of communications but some of its rules are no longer fit for purpose in light of technological and market developments and changes in the legal framework. This is the case for the rules on security and notification of personal data breaches which are entirely mirrored in the General Data Protection Regulation adopted in April 2016, making them redundant. As regards confidentiality of communications, the rules have achieved their objectives vis-à-vis providers of electronic communication services, but have failed to ensure an adequate protection of citizens when they use 'Over-the-Top services' (e.g. voice over IP or instant messaging), given that the Directive does not apply to such services. This regulatory asymmetry has placed electronic communication service providers at a competitive disadvantage *vis-à-vis* these new players and led to varying degrees of protection according to the means of communications used.

Overall, the Directive appears to have provided an appropriate framework for protecting privacy and confidentiality of communications in the EU; but a series of issues were encountered with respect to its **effectiveness**.

The practical application and enforcement of the principles (e.g. confidentiality of communications and of terminal equipment) set forth in the Directive has proven to be challenging in a number of ways. A majority of Member States have established multiple authorities competent for the ePrivacy Directive, sometimes with overlapping competences, thereby creating confusion as to which body is responsible for enforcement. The evaluation also found that the application of the consent rules on the confidentiality of terminal equipment[19], often referred to as the "cookie rule" and aimed at empowering individuals, has not been fully effective. Citizens are presented with requests to accept tracking cookies without understanding their meaning because of complex language and in some cases, are even exposed to cookies being set without their consent. Furthermore, the consent rule has been assessed as being over-inclusive, as it also applies to non-privacy intrusive practices such as first party analytic cookies, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device. In the context of unsolicited commercial communications the sheer number of complaints from citizens indicates that the rules may not deliver its intended goals.

As regards the **efficiency,** it is necessary to acknowledge the difficulty to obtain reliable and representative quantitative data. The majority of stakeholders consulted were not able to estimate relevant figures for the provisions of the Directive such as for example the costs related to the requirement to set up security measures and the requirement to place cookie banners (to collect consent). According to the supporting study to this REFIT, it appears that the compliance costs would be around EUR 658 per business[20].

The evaluation found no evidence of major inconsistencies between the Directive and the other relevant EU piece of legislation with which it interacts. However, a series of redundancies have been identified in particular with the General Data Protection

[19] These rules require users' consent for using technologies such as cookies to store or access information on smart devices.
[20] SMART study 2016/080, Final Report, p 206.

Regulation (e.g. the security rule). Finally, the evaluation concludes that the ePrivacy has **EU added-value** as it imposes harmonised provisions on confidentiality of communications and traffic data which, in the light of an increasingly transnational electronic communications market, are becoming ever more important.

Lastly, based on the fact that the quantitative evidence remain scarce, the evaluation also shows that an effective system for monitoring the application of the Directive is currently lacking and should be put in place in the future.

ANNEX 3: STAKEHOLDER CONSULTATION

3.1. Stakeholder strategy

In order to ensure that the general public interest of the Union - as opposed to special interests of a narrow range of stakeholder groups - is well reflected in the review of the ePrivacy Directive, the Commission developed a stakeholder strategy with the view to ensure the widest possible consultation.

The aim of the stakeholder consultation was (i) to deliver a high quality and credible evaluation of the ePD by allowing interested parties to provide feedback and (ii) to invite stakeholders to contribute with suggestions for possible policy options to revise the directive. This also ensures transparency and accountability in the Commission's work.

The stakeholder consultation process took place through two main activities. On the one hand, we ran an online public consultation (Section 3.2) and on the other hand, we organized targeted consultations with key EU expert groups, workshops and informal meetings (see Section 3.3). In addition, we ran a Eurobarometer survey in order to receive citizens views (see Section 3.4).

In view of the wide variety of sources and stakeholders consulted and the relatively high degree of responses and input received from all stakeholders' group, the stakeholders views hereby discussed are considered as representative.

3.2. Results of the Public consultation

The public consultation on the review of the ePrivacy Directive took place between **12 April 2016** and **5 July 2016**. The consultation aimed to gather input for the REFIT evaluation of the Directive and to seek views on the possible changes to the ePD.

The consultation gathered a total of **421** replies, **162** contributions from citizens, **33** from civil society and consumer organisations; **186** from industry and **40** from public bodies, including competent authorities to enforce the ePD.

The key findings of the public consultation as to the **way forward** are the following:

- *Are special privacy rules for the electronic communications sector still necessary?*

83% of the responding citizens and civil society believe that there is a clear added value in having special rules for the electronic communications sector to ensure the confidentiality of electronic communications, which is a basic element underpinning trust in technological developments and the digital society and economy.73% believe this is the case also for traffic and location data. They also support the need for special rules on billing, calling and connected line identification, automatic call forwarding and directories, but these areas seem to be less essential to them than the other areas mentioned. Industry responses were much more sceptical on the need for special rules; 31% see a need for rules on confidentiality and 26% see a need for rules on traffic data. Almost all public authorities responding to the consultation see the need for special rules in all of the areas listed.

- *Should a new instrument cover new communication services (instant messaging, VoIP)?*

76% of citizens and civil society believe that the scope of the rules should be broadened to cover the so-called over-the-top service providers (OTT) when they offer communications services such as VoIP or instant messaging. 43% of respondents from

industry also believe that the rules should be extended, 42% of the industry are against extension, while 5% do not have an opinion. 93% of public authorities believe that some or all of the provisions should be broadened to cover over-the-top players.

- *Is there a need to allocate enforcement to one single authority? Which one?*

Close to 70% of the combined total responses from industry, citizens and civil society say that one single national authority should be entrusted to enforce the rules, while half of the public bodies who responded to the consultation are not convinced that this is needed. For respondents who consider that one single authority should enforce ePrivacy rules, a majority, across all categories, find that the national data protection authority is the best suited authority.

- *How to deal with tracking cookies?*

77% of citizens and civil society and 70% of public authorities believe that information service providers should not have the right to prevent access to their services if users refuse the storing of identifiers, such as tracking cookies, in their terminal equipment. Three quarters of industry on the other hand disagree with this statement.

- *Opt-in or opt-out for direct marketing calls?*

All groups of respondents agree that Member States should not retain the possibility to choose between a prior consent (opt-in) and a right to object (opt-out) regime for direct marketing calls to citizens. The stakeholder groups are however split on which regime should apply: close to 90% of citizens, civil society and public authorities favour an opt-in regime whereas 73% of industry favour an opt-out regime.

2.3 Ad hoc consultations of EU expert groups and workshops

In parallel to the public consultation, the European Commission conducted ad hoc consultations of the following EU expert groups in the course of the summer 2016. It also organised a series of workshops to receive additional inputs from stakeholders.

3.3.1. REFIT platform groups

On 29 June 2016, the REFIT platform groups advising the European Commission adopted 2 opinions on the review of the ePrivacy Directive: one from the REFIT stakeholder group and one from the REFIT governance group.

a) – REFIT stakeholder group

The opinion, which was led by the Danish Business Forum (DBF), overall recommended that the rule should be amended in a manner which will both decrease industry costs of implementation and raise awareness of privacy among users. The Commission, Member States and Data Protection Authorities should ensure that the future instrument is aligned and consistent with the GDPR, in terms of approach and of choice of legal instrument.

The Commission and Member States should seek greater harmonisation in the implementation and enforcement of the rules, including the provisions related to cookies and the enforcement mechanisms, while promoting the use of European standards. The rules related to cookies and tracking technologies, as well as the rules on unsolicited communications, should be reviewed to ensure that they are future proof. Reforming the legislation should not open any back doors for tracking users and any exceptions to the consent rule should only affect cookies which do not create any privacy risks.

b) – REFIT governance group

The opinion of the REFIT governance group, which was led by Spain, drew a special attention to the so called "cookie" provision. It stressed the importance of assessing whether that rule has achieved its specific objective of raising citizens' awareness, in the light of the costs incurred by businesses. In this respect, the group underlined the importance of taking into account the feedback gathered throughout the consultation exercise. The opinion recommends that the Commission amend Article 5.3 when putting forward a legislative proposal; while other institutions are invited to speed-up the legislative process on this file and competent authorities to share best practices on enforcement.

3.3.2. Article 29 Working Party

The Article 29 Working Party was expressly consulted by the Commission. The latter adopted an opinion on the evaluation and review of the ePrivacy Directive (2002/58/EC)[21]. The key findings of this opinion are the following:

- It supports maintaining specific rules on confidentiality of communications;
- It clarifies that the GDPR will not apply "*in cases where the ePrivacy Directive contains specific obligations with the same objective*";
- The new ePrivacy instrument should at least maintain and reinforce its current principles, to guarantee the confidentiality of electronic communications;
- The scope of the rules on geolocation and traffic data should be extended to all parties;
- The new instrument must seek to protect the confidentiality of functionally equivalent electronic communication services (such as, for example, WhatsApp, Google, GMail, Skype and Facebook Messenger)**;**
- The broad scope of the consent requirement under Article 5(3) should be clarified while there is a need to create more specific exceptions to allow for the processing of data that causes little or no impact on the privacy of users;
- It acknowledges the high intrusiveness of tracking over time of traffic and location data and call on a uniformed regime suggesting the merger of the current Articles 6 and 9 and the introduction of more exceptions to the consent rule;
- When consent is the applicable legal basis, users must be provided with truly easy (user friendly) means to provide and revoke consent.

3.3.3. European Data Protection Supervisor

The views of the EDPS were expressly requested by the European Commission.

In his opinion on the review, the EDPS expresses similar views than those of the Article 29 Working Party, of which he is a member. In particular, the EDPS also endorses the need to **keep specific rules to ensure confidentiality of communications** at EU level

[21] Article 29 Working Party opinion of 19.07.2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240.

that would complement the GDPR. In this respect, he made the following recommendations:

- The scope of new ePrivacy rules needs to be broad enough to cover all forms of electronic communications irrespective of network (public or private [22]) or communication services used;

- Individuals must be afforded the same level of protection for all types of communications regardless of the technology used (e.g. telephone, Voice over IP, services, mobile phone messaging app, Internet of Things);

- No communications should be subject to unlawful tracking and monitoring without freely given consent, whether by cookies, device-fingerprinting, or other technological means. This means that the so called cookie rule should be revised to address any tracking techniques;

- Users must also have user-friendly and effective mechanisms to give their consent. In this respect cookie walls (where users are forced to give their consent to access a webpage) should be prohibited;

- In order to increase confidentiality and security of electronic communications, the consent requirement for traffic and location data must be strengthened and apply horizontally (i.e. to any processing of such data);

- The new rules should complement, and where necessary, specify the protections available under the GDPR;

- The rules should also maintain the existing, higher level of protection in those instances where the ePrivacy Directive offers more specific safeguards than in the GDPR. In this respect, the EDPS supports maintaining the rules on subscribers' directories and calling and connected line identification;

- The rules protecting against unsolicited communications, such as advertising or promotional messages, should be updated, made technology neutral and strengthened by mandating the recipient's prior consent for all forms of unsolicited electronic communications.

3.3.4. CPC Network

The European Commission also specifically consulted the Consumer Protection Cooperation Network through a tailored questionnaire. The network was not in a position to provide a coordinated reply and invited its members to reply individually.

Replies were received from consumer authorities from Spain, Romania, Norway, and Denmark. The key points of their replies are summarised below:

- All respondents considered that the ePD only partially achieved its objectives;

[22] The updated rules should ensure that the confidentiality of users is protected on all publicly accessible networks, including Wi-Fi services in hotels, coffee shops, shops, airports and networks offered by hospitals to patients, universities to students, and hotspots created by public administrations.

- As to which provision in particular is problematic, several authorities refer to Article 13. Some considered that the high number of complaints received on unsolicited calls show the need to review. Others emphasised some flaws of the rules, such as difficulties to apply the rules to new technological development such as social media; difficulties to prove unsubscribing to a mailing list and difficulties for companies to understand the rules;

- One authority considered that Article 5.3 failed to achieve its objectives in the light of diverging interpretation and enforcement;

- Overall the respondents agreed that the wide diversity of competent authorities has created difficulties that have led to diverging interpretation and/or fragmented enforcement. One authority specifically referred to the uncertainty that this created among competent authorities as to which authority should act. Another considered that this may cause a concurrent action of authorities leading to increased cost of enforcement;

- A majority of respondents agreed that a regulation would be the better suited instrument to achieve the objectives of the current ePD;

- They all agreed that the rule on unsolicited communications should be reviewed and that the choice left to Member States between opt-in and opt-out is not coherent under Article 13.3 with the opt-in rule under Article 13.1. While a majority of them considered that opt-in should apply to all situations for unsolicited communications towards individuals; the position is not clearly defined for legal persons. A majority support the opt-in rule to apply to social media;

- All respondents that expressed a view, considered that member states should not retain the possibility to choose between opt-in and opt-out for individuals (under Article 13.3), while 2 out of 3 considered that they should not retain this possibility for legal person as well[23].

3.3.5. BEREC

BEREC, the EU body gathering NRAs (competent telecom authorities) was expressly consulted by the Commission and sent its views on the 31st of July.

Overall, BEREC considered that:

- There is still a need to have data protection rules and privacy rules addressing the electronic communications sector;

- The rule on confidentiality of communications should apply equally to ECS and new OTT players (so called OCS) while its wording should be adapted to technological changes;

[23] One respondent did not express his views on this.

- There is a still a special interest to regulated traffic and location data over the GDPR given the sensitiveness of these data[24];

- So called consumer provisions (on itemised bill, calling & connected line identification etc.) should be maintained and extended to new OTT players;

- The security rule including notification requirement should be maintained and aligned with the ones of the GDPR;

- Regarding the question of extending the protection of the rules to semi-private network (e.g. airport, cafes etc.), the authority underlined the need to ensure that the rules should be adjusted so that they do not act as a detriment to the further development of non-commercial Wi-Fi-access;

- Regarding Article 5.3 the authority underlines that the current system does not allow a meaningful consent and that the rules need to be revised and focus more on the purpose of tracking rather than on the access and storing of information.

3.3.6. Workshops and meetings with stakeholders

The European Commission organised **two workshops** in April 2016 to collect further views of stakeholders, using participatory techniques.

The **first workshop** was open to all stakeholders and took place on 12 April. There were around 120 participants, representing industry, competent authorities and civil society. The main views that were expressed are summarised below:

- Representatives of the telecom industry argued for the need to push for the economic growth, emphasising job opportunities and innovation by removing specific provisions of the ePD, such as those on traffic and location data;

- Representatives from the OTT industry underlined the difficulties for these companies operating across border to comply with different national rules on access to communications by law enforcement authorities;

- Representatives from consumer organizations argued for keeping the requirement for user consent on tracking, location and traffic data while promoting privacy by design/default;

- Representatives from competent authorities underlined the benefit of supporting user friendly measures such as Do-Not-Track (DNT) to protect privacy and called for fully harmonising privacy rules in a regulation;

- Academics supported an extension of the ePrivacy rules to OTT services, while stressing the interdependence of privacy with other fundamental rights like the freedom of expression or right to private property.

---

[24] BEREC reply p. 6: "*As technology has developed, so have the threats to confidentiality of communications. Nowadays, it is for instance possible* ***to automatically analyse network traffic in real time (i.e. Deep Packet Inspection), even on a core network level****. Such analysis could be used for anything from traffic management to profiling of the network users for marketing purposes*."

The **second workshop** gathered the **national competent authorities** in order to receive their specific inputs to the review. The discussions focused on Article 5.3, the rules on traffic and location data, the need of a security provision and the provisions on subscribers directories and unsolicited communications. At the meeting with the competent authorities of 19th April no specific policy options were presented by the Commission, but it enabled national competent authorities (DPAs, NRAs or other) to give their views on the review and to highlight the problems they encounter. The meeting allowed them to give input at an early stage. On top of the stakeholder meeting, the Commission consulted the Article 29 Working Party, which encompasses all DPAs, and BEREC, which encompasses all NRAs – the authorities of the stakeholders meeting of 19th April. Both bodies gave an extensive contribution in which they presented their views on the review. A summary of these contributions, representing broadly the views of Member States, is provided above.

3.4. The Eurobarometer on e-Privacy

Between the 7th and 8th July 2016, around 27,000 citizens from different social and demographic groups were interviewed throughout the EU via telephone (mobile and fixed line) on questions related to the protection of their privacy. Below is a summary of the results of this Eurobarometer survey[25].

Citizens' use of tools to protect their privacy online:

- A 60% of the respondents acknowledge that they have changed their privacy settings of their internet browser for instance to delete browsing history or delete cookies;

- 41% of respondents avoid certain websites because they are worried their online activities would be monitored while roughly a third of the respondents acknowledge using software that protects them from seeing online adverts and/or being monitored online.

Citizens' assessment of importance of measures protecting their privacy online and confidentiality of their communication

More than nine in ten respondents throughout the EU consider the following as important:

- Personal information (e.g. photos, calendar, contacts) on their computer, smartphone or tablet can only be accessed with their permission[26];

- The confidentiality of their emails and online instant messaging is guaranteed[27];

- Tools for monitoring their activities online (such as cookies) can only be used with their permission[28].

Almost nine in ten respondents (89%) agree with the proposal that the default settings of their browser should stop their information from being shared.

---

[25] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).
[26] 92 % with 78% considering this as very important.
[27] 92% with 72% considering this as very important.
[28] 82% with 56% considering this very important.

Nine in ten agree they should be able to encrypt their messages and calls, so they are only read by the recipient (90%), with 65% saying they totally agree with this.

Citizens' views on the acceptability of business models around access to information:

A strong majority of respondents do consider it not really acceptable or not acceptable at all to:

- Have their online activities monitored (for example what they read, the websites they visit) in exchange for unrestricted access to a certain website (i.e. 67%);

- Have companies sharing information about them without their permission (even) if this helps these companies to provide them with new services they may like (i.e. 71%).

76% of respondents do not want to pay as an alternative not to be monitored when being on a website.

Citizens' views on unsolicited communications

- 61% of respondents agree they receive too many unsolicited calls offering them goods or services;

- Respondents in the UK (78%), Italy (76%) and France (74%) are the most likely to agree they receive too many unsolicited calls offering them goods or services, where the regime of these calls is under opt-out;

- Respondents who use a landline or mobile phone were asked their preferred approach for people telephoning them to sell goods or services29. The majority of respondents think commercial calls should always display a special prefix (59%), while just over one in five (22%) think these calls should be allowed as long as they display their phone number.

[29] Q7 Which of the following would be your preferred approach to people telephoning you to sell goods or services?

ANNEX 4: LEGAL AND SOCIO-ECONOMIC CONTEXT

4.1. Legal context

4.1.1. Historical background

The ePrivacy Directive lays down a framework governing the protection of privacy and personal data in the electronic communications sector in the EU. It complements and particularises the Data Protection Directive 95/46/EC ("**DPD**")[30], which is the central legislative instrument in the protection of personal data in Europe[31]. The General Data Protection Regulation ("**GDPR**") will replace the DPD in 2018 with new modernised rules fit for the digital age.

Following the adoption of the DPD in 1995, more detailed rules were considered necessary for the protection of privacy and data protection in the **electronic communications sector**, which led in 1997 to the adoption of the first incarnation of the ePD.[32]

The EU legislator considered that the new technologies in public telecommunications networks gave rise to specific requirements concerning the protection of personal data and privacy of the user, which in turn required specific protection of the fundamental right of confidentiality of communications[33].

With the same objectives in mind, in 2002 the EU legislator adopted a new ePD, considering that the old ePD had to be adapted to developments in markets and technologies in order to provide an equal level of protection of users, regardless of the technology used, broadening its application from traditional voice telephony to include data transmission and use of the Internet. In 2009, the ePD was amended by Directive 2009/136/EC[34].

4.1.2. Objectives, scope and main content

The ePD sets forth rules concerning the protection of privacy in the electronic communications sector. One of the main elements of the ePD is to ensure protection of confidentiality of communications, in line with the fundamental right to the respect of private and family life (including communications) enshrined in Article 7 of the EU Charter of Fundamental Rights (hereinafter the "**Charter**").

---

[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ, L 281, 23.11.1995.

[31] The DPD is the legislative basis for two long-standing aims of European integration: the Internal Market (in this case the free movement of personal data) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important.

[32] Directive 97/66/EC of the European Parliament and of the Council, on concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L24/1, 30.1.98.

[33] See Recitals 2, 3 and 7 of the 1997 ePD.

[34] Directive 2009/136/EC of the European Parliament and of the the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ, L 337/1, 18.12.2009, p.11.

- Objectives

According to its Article 1, the ePD provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data and the electronic communications sector and to ensure the free movement of such data and of electronic communications equipment and services in the EU. Moreover, it provides for protection of the legitimate interests of subscribers who are legal persons.

The ePD serves therefore three main objectives. ***First,*** it seeks to ensure respect of fundamental rights set out in Articles 7 on the respect for private life and communications[35] and 8 of the Charter on the protection of personal data[36]. In particular, one of its main objectives is the protection of the right to privacy and confidentiality with respect to the electronic communications sector, as guaranteed under Article 7 of the Charter, Article 8 of the European Convention on Human Rights as well as under other international instruments relating to human rights.

Next to the fundamental rights aim, the ePD pursues also important internal market objectives. The ***second*** objective of the ePD is to ensure free movement of data processed in the electronic communications sector. Just as Directive 95/46/EC, the ePD aims to harmonise legal, regulatory and technical provisions adopted by the Member States ("**MS**") concerning the protection of personal data, privacy and legitimate interests of legal persons, in order to avoid obstacles to the internal market for electronic communications.

The ***third*** main objective of the ePD, which is also connected with the EU internal market, is ensuring the free movement of electronic communication terminal equipment and services in the EU. The ePD pursues this objective by harmonising the rules on privacy and confidentiality in the electronic communication sector in the EU, but also by providing specific rules on technical features and standardisation. For example, Article 14 of the ePD provides that in implementing the provisions of the ePD, MS may not impose mandatory requirements for specific technical features on terminal or other electronic communication equipment which could hinder the free circulation of such equipment in the EU.

- Scope

The ePrivacy Directive applies to "*the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*"[37]. In particular, its provisions apply to providers of "electronic communications networks and services"[38].

To be covered by the Directive:

(1) the service should be an *electronic communications service*,

(2) the service should be offered in an *electronic communications network*,

---

[35] Article 7 provides that "Everyone has the right to respect for his or her private and family life, home and communications".

[36] Article 8 provides that "Everyone has the right to the protection of personal data concerning him or her".

[37] Articles 1 and 3 of the ePD.

[38] Defined in Article 2 of Directive 2002/21/EC, OJ L 108, 24.4.2002, p. 33–50.

(3) the aforementioned service and network should be *public(ly available)*, and

(4) the network or service should be provided *in the Community*.

Therefore, the Directive applies to electronic communication services such as voice telephony, access to the Internet, etc., provided by ECS providers, i.e., traditional telecommunication operators. On the basis of the above definition, information society services providing communication services over the Internet are not subject to the ePD, as the latter have no control and responsibility of the conveyance of signals over the networks (a function which is performed by ECS).

Furthermore, as the ePD only applies to *publicly available* electronic communications networks, this means that **closed (private) user groups and corporate networks** are in principle excluded from the scope of the ePD. In this context, there is a lack of clarity as to which services qualify as a publicly available electronic communications services in public communications networks. Indeed, MS have diverging views on whether **Wi-Fi Internet access offered at airports, in internet cafes or shopping malls** qualifies as publicly available electronic communications services in public communications networks[39].

Finally, it remains unclear to which extent the **electronic communications** of the **Internet of Things[40] ("IoT")** are covered by the ePD as its Article 3 expressly refers to "*public communication networks supporting identification devices*"[41]. According to the European Data Protection Supervisor ("**EDPS**"), this seeks to clarify that the protection of communications privacy is not dependent on whether humans speak or listen, type or read the content of a communication, but that they may rely on the increasingly smart features of their terminal devices to communicate content on their behalf, enjoying the expected level of protection[42]. Moreover, Recital 56 of Directive 2009/136/EC provides that the provisions of the ePD, in particular those on **security, traffic and location data and on confidentiality of communications** apply to RFID.

- Main content

The **main content** of the ePD can be summarised as follows:

1. It requires Member States to ensure confidentiality of communications in public communication networks and extends this principle to users' terminal equipment by requiring prior informed consent to store or access information in the users' terminal equipment (phones, tablets, etc.). This applies, for example, to the storage of cookies[43].

---

[39] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 5.

[40] Based on existing communication 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).

[41] OJ L 337, 18.12.2009, p. 11–36.

[42] EDPS Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.07.2016, p. 11.

[43] A cookie is a small piece of information placed on a person's computer when they visit a website. They can be used to remember the users' preferences, record items placed in a shopping basket and carry out various other tasks based on how that person uses the site. Some cookies, known as third party cookies, are

2. It requires that traffic[44] and location data be erased or made anonymous when they are no longer required for the conveyance of a communication or for billing, except if the subscriber has given their **consent for another use** and to the extent that processing of these data is necessary for providing a value-added service.

3. It requires **mandatory opt-in rules for unsolicited marketing** by means of automated calling machines, telefaxes, and e-mails, including SMS messages. This means that commercial communications can only be sent if the recipient has taken an affirmative action indicating his consent to receiving marketing emails (for example, by clicking an unclicked box on a web form).

4.1.3. Relationship with other existing legal instruments

- Data protection legislation

The Data Protection Directive 95/46/EC (hereinafter "**Data Protection Directive**" or "**Directive 95/46/EC**")[45] is the central legislative instrument in the protection of personal data in Europe.

Directive 95/46/EC is the legislative basis for two long-standing aims of European integration: the Internal Market (in this case the free movement of personal data) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important. The General Data Protection Regulation ("**GDPR**") will replace Directive 95/46/EC in 2018 with new modernised rules fit for the digital age.[46]

Directive 95/46 protects the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality. It sets out specific rights of data subjects, including the right to be informed of the processing and the right to access their personal data, and obligations of data controllers.

The ePD particularises and complements Directive 95/46/EC by, among others, setting up specific rules concerning the processing of personal data in the electronic communication sector. It does so, for example, by requiring users' consent before their phone numbers can be listed in a public directory.

---

placed by a website different from the website that one has visited. They are often used to record information about individuals' surfing behaviour (website visited, interactions, time, location) etc. This is used to develop specific profile and provide individuals with advertisements tailored to match their inferred interests (Definition provided by Article 29 Data Protection Working Party, Press Release on the Cookie Sweep Combined Analysis Exercise: 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).

[44] **Traffic data** means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. This includes for instance calling and called numbers, Internet Protocol (IP) address, name and address of the subscribers concerned; date, time and duration of a communication; location. These data are commonly referred to also as "metadata".

[45] OJ L 281 , 23/11/1995 P. 0031 - 0050.

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

The relationship between Directive 95/46 and the ePD is that existing between a *lex generalis* (Directive 95/46) and a *lex specialis* (the ePD). All matters concerning the protection of personal data in the electronic communications sector which are not specifically addressed by the provisions of the ePD are covered by Directive 95/46 (and in the future by the GDPR). For example, this covers the rights of individuals such as the right to obtain access to their personal data.

- Telecom Regulatory Framework

The ePD is part of the Telecom Framework, which comprises a Framework Directive 2002/21/EC ("**FD**") and four specific directives. The Telecom Framework was last amended in 2009[47] and it is currently under revision. The ePD borrows from the telecom framework a number of crucial elements, including the definition of its main scope and some important definitions. The scope of the ePD and the FD coincides in that they both apply to the ECS providers, as defined above. Moreover, the FD provides the definition for some very important terms which are used in the ePD, such as "electronic communication service", "electronic communication network", "user" and "subscriber".

It can be argued that the ePD has somewhat a dual nature, given its close links on the one hand with the data protection legislation and, on the other hand, with the telecom regulatory framework. While from a functional perspective, the ePD can be considered to be closer to the data protection legislation, in that his main objective is to protect fundamental rights, from a technical/sectorial perspective it can be considered closer to the Telecom Framework, as it regulates a specific economic sector/activity.

In 2015, the Commission initiated a review of the Telecom Framework which led in September 2016 to the adoption of a Commission's legislative a proposal for a Directive establishing the European Electronic Communications Code.[48] In this context, and in view of the close links of this instrument with the data protection legislation, it was decided that the ePrivacy Directive would have been subject to a separate review, following the final approval of the GDPR. The rationale of having a separate initiative for the ePrivacy review reflects, in particular, the dual nature of the ePrivacy rules and the need to ensure full consistency with the GDPR.

- Radio Equipment Directive

The RED ensures a single market for radio equipment by setting out essential requirements for safety and health, electromagnetic compatibility and the efficient use of the radio spectrum. This applies to all products using the radio frequency spectrum and thus includes mobile electronic communication terminal equipment, such as smartphones, tablets, Wi-Fi devices etc. There are strong synergies between the ePD and the RED.

Several aspects of the RED are relevant in relation to the ePD and the objective of protecting privacy and confidentiality of electronic communications. In particular, the RED establishes that, before being put into the market, radio equipment must comply with certain essential requirements. One of these requirements is that radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the

[47] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF.
[48] COM(2016) 590 final.

subscriber are protected. The Commission may adopt delegated acts specifying the categories or classes of radio equipment subject to the above requirement.

Compliance with the above requirement is presumed for radio equipment which is in conformity with harmonised standards the references of which have been published in the Official Journal of the European Union. Moreover, in accordance with Regulation (EU) No 1025/2012 on European standardisation ("**Regulation 1025/2012**"), the Commission may request European standardisation bodies to issue a standard for the purpose of ensuring conformity with the above essential requirement.

The above delegated acts and technical standards are particularly relevant for the ensuring the effective implementation of the ePD provisions. The interaction between the two instruments is explicitly reflected in Article 14(3) of the ePD, which empowers the Commission to adopt measures under the RED and Regulation 1025/2012 to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect their personal data. No such measure has been adopted so far by the Commission.

- The former Data Retention Directive

The former Data Retention Directive 2006/24/EC harmonised national laws concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each MS in its national law.

The Data Retention Directive was annulled by the Court of Justice of the European Union in its judgment of 8 April 2014 in the *Digital Rights Ireland* case. The Court found, in particular, that the Directive did not comply with Articles 7 and 8 of the Charter on privacy and data protection. The Directive was not considered by the Court as a proportionate interference with the above fundamental rights because it did not specify in sufficient detail the limits and the conditions of the interference and did not provide for adequate safeguards against abuse.

In the current absence of EU legislation in the field of data retention, MS may still establish or maintain national data retention legislation, based on Article 15(1) of the ePD so far as they comply with the general principles of Union law. Article 15 of the ePD allows MS to derogate to some ePrivacy rules[49] (e.g. the confidentiality of electronic communications) for the purposes of "safeguard(ing) national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system". It also provides that these measures must constitute a necessary, appropriate and proportionate measure within a democratic society, in accordance with the jurisprudence of the Court of Justice of the EU and the European Court of Human Rights ("ECtHR").

In line with the European Agenda on Security[50], the Commission does not envisage coming forward with any new initiative on data retention for the time being. Instead, the Commission will continue monitoring legislative developments at national level.

---

[49] These are mainly the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of the ePD.

[50] COM(2015) 185 final.

4.2 Market context

4.2.1. Main socio-economic drivers

The past 5-10 years have been characterised by a series of very significant and correlated developments in the field of privacy and electronic communications. The main developments are summarised below:

- The rise of new business models, the so called **over-the-top service providers** (OTTs) providing communication functions free of charge essentially through an Internet software platform. As outlined above, these providers do not convey the signals over the network and are therefore normally considered outside the scope of the Telecom Framework and the ePD.

- The **exponential growth of the information processed globally**, estimated to be in the region of 1.2 zettabytes, or 1,200,000,000,000,000,000 bytes) and growing by 60% every year.[51] **A big contribution to this big data is made by online services** that track users' online communications in order to build detailed commercial data-banks, which can be used for online behavioural advertising, marketing campaign or other purposes.

- The rise of free online services has enticed a **shift in citizens' attitude to share information related to their surfing behaviour**. While citizens generally value privacy and confidentiality very much, they are prepared to **give up part of their privacy for convenience and performance**[52].

- **Information asymmetry in the online sphere**. Users are very often not aware of what is done with the information about their surfing behaviour and related profiles[53]. Cookie policies are normally complex, long and unclear. Citizens have grown increasingly irritated by the continuous requests for consent online and most likely click them away to get rid of them. Internet has become so widespread that users are virtually obliged to use certain online services, even if they do not want to be tracked. Nevertheless, they overwhelmingly want to be asked for their permission before their personal information is accessed from their smart devices or before being monitored online[54].

- **Lack of technical knowledge** to control tracking and protect the content of one's equipment. While surveys of consumers' attitudes consistently show that individuals value their privacy and consider that monitoring their online activities should only occur with their permission, many do not seem to be able to set up the

[51] CERRE, Consumer Privacy in Network Industries, http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf, p. 8.
[52] Only one third of respondents to the 2016 Eurobarometer on e-Privacy say it is acceptable to have their online activities monitored in exchange for unrestricted access to a certain website (33%). See alsoStudy for the EP IMCO Committee, Over the Top players (OTT), 2015, p. 54-55.
[53] 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.
[54] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

appropriate tools to protect themselves against tracking and to protect the content of their equipment[55].

- **The increasing social and economic importance of online communications**. Citizens are increasingly dependent on these services. Communicating online, sharing pictures, videos, links or other information has become a primary social need. Having a phone number, an Internet connection and an email address is an indispensable requirement for working and communicating with others. Certain schools require their students to have a social account.

- The **prevalence of the "free-of-charge" model**. The largest majority of online services are offered to consumers free of charge, but data about consumer surfing behaviour and preferences are collected in order to monetise this information in the online advertising market. Over time, people have got used to accessing these services for free, i.e. without paying any monetary fees, thinking almost that having free access would be a natural right[56].

- The **changing notion of privacy** in an evolving digital environment. While citizens are generally concerned about their privacy, they are not prepared to reconsider or limit their online behaviour or to pay a fee for accessing online services[57]. Recent statistics say that especially young people have a different perception of privacy and share information about themselves voluntarily much more than the rest of the age range[58].

These contextual factors are crucial for the understanding of the complexity of the problem and for the assessment of the policy options. In particular, they show that the protection of privacy of online communications is a complex, multifactorial zero sum game where every gain from a market participant is normally balanced by losses of other participants.

[55] Only a third of respondents to the 2016 Eurobarometer on e-Privacy said they use software that protects them from seeing online adverts (37%) or from being monitored (27%).
[56] See, e.g., 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.
[57] Almost three quarters (74%) of respondents to the 2016 Eurobarometer on e-Privacy say it is not acceptable to pay in order not to be monitored when using a website while only one quarter of respondents[57] (24%) say it is acceptable,
[58] According to the 2016 Eurobarometer on ePrivacy, 45% of the youngest respondents say it is acceptable to have their online activities monitored, compared to 24% of those aged 55+.

4.2.2 The market covered by the ePD (source: Deloitte[59])

- The size of the telecommunications sector in the EU

Within the European Union, the telecommunication sector[60] is one of the crucial industries for the completion of the Digital Single Market. The table below provides an overview of the:

- Number of enterprises (2014);
- Number of persons employed (2014); and
- Annual turnover in 2014 of the EU telecommunications sector.[61]

The statistics provided in the table serve as a first high-level entrance point for the further analysis of the market covered by the ePD.

Member State	Number of enterprises (in thousands, 2014)	Number of persons employed (in thousands, 2014)	Annual turnover in 2014 (in million)
Austria	0.3	15.1	5,444.8 €
Belgium	1.5	24.3	12,296.1 €
Bulgaria	0.7	20.1	1,502.9 €
Croatia	0.3	9.0	1,644.5 €
Cyprus	0.1	3.9	671.2 €
Czech Republic	1.0	17.3	3,843.0 €
Denmark	0.4	18.7	5,697.7 €
Estonia	0.2	4.3	699.3 €
Finland	0.4	12.2	4,368.3 €
France	5.4	167.3	61,428.5 €
Germany	2.8	111.6	60,471.2 €
Greece[62]	0.2	22.6	6,411.8 €
Hungary	1.2	18.9	3,579.9 €
Ireland[1]	0.4	12.4	5,650.7 €
Italy[1]	4.3	94.0	44,077.6 €
Latvia	0.5	5.0	729.0 €
Lithuania	0.3	6.0	769.2 €
Luxembourg	0.1	4.8	4,377.4 €
Malta[63]	0.0	1.6	- €
Netherlands	1.4	31.2	16,881.4 €

[59] The content of this section is provided by the Commission external study prepared by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080)..

[60] Eurostat defines this sector as being composed of business activities of providing telecommunications and related service activities, such as transmitting voice, data, text, sound and video.

[61] See Eurostat: http://ec.europa.eu/eurostat/statisticsexplained/images/8/88/Key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_2012_A.png.

[62] Eurostat data for 2012, final numbers for 2014 not available.

[63] No data on annual turnover available.

Member State	Number of enterprises (in thousands, 2014)	Number of persons employed (in thousands, 2014)	Annual turnover in 2014 (in million)
Poland	5.7	48.8	10,048.7 €
Portugal	0.7	15.0	5,533.7 €
Romania	2.4	43.4	4,271.4 €
Slovakia	0.3	10.5	2,208.3 €
Slovenia	0.3	5.0	1,361.6 €
Spain	4.9	59.7	31,020.8 €
Sweden[1]	1.0	27.2	12,666.5 €
United Kingdom	7.7	209.8	78,184.9 €
EU28	44.7	1,019.8	385,840.4 €

Source: Eurostat.

According to Eurostat, around 44.7 thousand enterprises are active in this market, accounting for a share of 0.2% of all businesses active in the EU. Around 90% of these enterprises are micro-enterprises, 99% are SMEs. Around 52% of all EU telecommunication enterprises were established in the United Kingdom, Poland, the Netherlands, Germany and France in 2014.

Overall, approx. one million citizens are employed in the telecommunications sector of which roughly 20% are active in SMEs.[64] In total, 56% of all employees in the EU telecommunications sector worked for enterprises in United Kingdom, France, Germany, Poland, and the Netherlands in 2014. When putting the number of persons employed in the telecommunications sector in relation to the overall number of citizens per Member State, it can be seen that Luxembourg, Cyprus, Denmark, Estonia, and the United Kingdom have comparatively high shares of citizens working in the telecommunications sector. None of these Member States, however, exceeds a share of 0.9%.[65]

The sector generates an annual turnover of 385 EURb. The United Kingdom, France, Germany, Poland, and the Netherlands accounted for 59% of the entire EU28 turnover in the telecommunications sector in 2012 (overall roughly 227 EURb). In terms of contribution of the telecommunication sector to the annual GDP pf each Member State, Eurostat data shows that the sector is largest in Luxembourg (9.5% of overall annual GDP in 2012), Estonia (4.5%), Bulgaria (4.3%), Croatia (4.1%), and the United Kingdom (3.8%).[66]

[64] Figure from 2011. Actual figure today likely to be higher. See: http://ec.europa.eu/eurostat/statistics-explained/images/4/4f/Sectoral_analysis_of_key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_EU-28%2C_2012_A.png.

[65] This is based on internal calculations and cannot be directly concluded from the information sources we used for our analysis.

[66] Figures relate to 2012. The actual figures today are likely to be higher. See Eurostat: http://ec.europa.eu/eurostat/statistics-explained/images/9/9c/Key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_EU-28%2C_2012.png.

- Over-The-Top services (OTTs)

A 2016 global forecast of the market for Over The Top (OTT) providers[67] shows that market is estimated to grow from USD 28.04 Billion in 2015 to USD 62.03 Billion by 2020 with a CAGR of 17.2%.[68] The report argues that market is in the growing stage in Europe and therefore OTT platforms in these regions have immense scope for enhancement. Overall, the North American region is expected to contribute the maximum market share to the overall OTT market.[69] As can be seen below, around 40% of primaries in the OTT market are expected to be established in North America by 2020 while 25% are expected to be European.

Figure 1 – Expected breakdown of profiles of primaries (in 2020)

Source: MarketsandMarkets

The report also acknowledges that diversified government regulations and policies present across domestic and international borders are restraining the growth of the OTT market.

According to the report, the European market is expected to grow at a similar pace (i.e. with a similar CAGR) as the North American market – albeit with a smaller overall market size. The Asian-Pacific, Middle East and African, and Latin American markets are smaller the the European and North American markets in terms of absolute size but are expected to grow faster than these two until 2020. This is depicted in the following figure.

[67] (Over The Top) is a generic term commonly used to refer to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content. The term over-the-top (OTT) is commonly used to refer to online services which could substitute to some degree for traditional media and telecom services. Definition provided in the study of the European Parliament, Directorate-General for internal policies, policy department A: Economic and Scientific Policy, Over-the-Top (OTTs) players: Market dynamics and policy challenges, dd.December. 2015,http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

[68] http://www.marketsandmarkets.com/Market-Reports/over-the-top-ott-market-41276741.html.

[69] http://www.prnewswire.com/news-releases/over-the-top-market-worth-6203-billion-usd-by-2020-572232561.html.

Figure 2 – OTT market size and growth by region (in 2020)

Source: MarketsandMarkets

Most provisions of the ePD do not apply to online communication services. This includes communication services that are not covered by the definition of electronic communication services employed by the ePD. Examples include *Skype* or *WhatsApp*.

Recent Eurobarometer data shows that mobile phones to make calls or send text messages are used by 74% of consumers every day while more traditional fixed phone line services are used by 38% each day. However, a large part of consumers also uses services every day that are not covered by the ePD: E-mail is used by 46% of consumers every day, OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[70], and online social networks are used by 38% every day.[71]

The results of the public consultation on the evaluation and review of the regulatory framework for electronic communications demonstrate that consumers increasingly recognise a functional equivalence between traditional SMS/MMS services and OTT services like *WhatsApp* or traditional voice calls and OTT *Voice-over-IP* (VoIP) services like *Skype* and a potential for their substitution.[72]

The majority of popular OTT social network services was launched around 2010, notable exceptions being *Skype* (2003) and *LinkedIn* (2003), *Facebook* (2004) or *Twitter* (2006). Among these OTT services, there seems to be no imperative that older services necessarily have larger user bases than more recent market entrants: A recent survey from 2015 reports the most popular OTT call and messaging services among respondents

[70] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.

[71] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At the stage of drafting this report, the Eurobarometer results are only of provisional character.

[72] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 11; see also https://ec.europa.eu/digital-single-market/en/news/full-synopsis-report-public-consultation-evaluation-and-review-regulatory-framework-electronic.

from EU MS to be *Skype* (49%), *Facebook Messenger* (49%), *WhatsApp* (48%) and *Twitter* (23%).[73]

From a macro perspective, the number of OTT subscribers has grown in two waves since 2000. First on desktop devices from 2000 to 2010, and again with the increasing adoption of smartphones after 2009/2010.[74] Regarding adoption patterns from a micro perspective, OTT messaging and voice call services often experience growth in form of an s-shaped curve: After up to two years needed to gain a critical mass of users, the service frequently experiences exponential growth rates until the market is saturated.[75] Nevertheless, adoption and usage patterns may vary significantly in cross-country comparison for individual apps. In addition, there seem to be country-specific preferences for certain OTT messaging and *VoIP* services and the number of parallel services used (depending on the MS, more than one third to half of respondents use multiple OTT social networks).

Considering actual traffic volumes, the use of OTT services has increased considerably: The OTT's share of overall messaging traffic has already increased from 8.31% (2010) to 66.96% (2013) and is projected to rise to 90% until 2020.[76]

Conversely, the use of SMS continues to decrease in almost all EU MS since 2010, albeit at a different pace: In Finland and Germany, SMS volumes have dropped to levels of 2006, while the decline has been slower in countries like Spain and France. Few countries observed stagnant volumes (Poland) or even a growth from previously low levels (Estonia).[77]

On the individual level, the average *WhatsApp* user is reported to send approximately 40 (while receiving around 80) messages per day as opposed to an estimated number of 4.5 SMS. This ratio of approximately 1:10 for daily SMS versus OTTs messages is likely to be much higher in practice, due to the reported parallel use of multiple messaging apps. [78]

Turning from messaging to voice call services, the developments appear to be similar but less pronounced in their magnitude. In general, European Electronic Communications Services (ECS) providers have been observing a steady decline in fixed line calls and steady increase of mobile calls (that have overtaken fixed line traffic shares ever since 2010). Despite this general trend, considerable variance across EU MS remains concerning the popularity or volume of fixed line phone calls.[79] The relationship of ECS and OTT providers offering voice calls is hard to ascertain. With regard to international

[73] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 37, 39.
[74] Ibid. p. 41.
[75] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 40.
[76] Ibid. p. 15.
[77] Ibid. p. 45.
[78] Ibid. p. 41.
[79] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 42-44.

calls, ETNO reports a rapidly growing popularity of *VoIP* services – despite still lagging behind traditional voice calls and their advantage of any-to-any connectivity with other providers, higher end-to-end quality and more reliable emergency services. The traffic volume of *Skype* increased by 36% in 2013, while traditional voice calls grew by 7%. During that same period, *Skype* calls amounted to a total of 214 billion minutes whereas traditional voice calls reached a total of 547 billion minutes.[80]

Based on these numbers, ETNO conclude that the OTT market presence and substitution of traditional telecommunication services can no longer be ignored.[81] While, this is certainly true, it is still questionable as to whether the presence for OTT service providers offering alternative services is the only cause for EU users changing their communication means as per figures above.

A recent study on behalf of the EC examines not only the rise of OTT services but also possible effects of changes in technology, the regulatory environment and economic growth.[82] Using the development of *WhatsApp* messages as an indicator, the rise of OTT displays no significant effect on the development of revenue, costs and profits for fixed line calls (rather changes in technology and regulation seem to have fostered competition and driven down prices).

In the mobile communications market, on the other hand, the rise of OTTs seems to have had a significant influence in reducing revenues and profits of ECS. Thus, while it is tempting to conclude that decreasing revenues and profits from mobile calls and SMSs are solely driven by the rise of OTTs, some of the developments had already been foreshadowed by increases in competition through the rise of broadband internet and smartphones, triggering changes in consumer behaviour and ensuing updates in business models (e.g. flat rate pricing).[83]

Yet ECS so far compete in one ecosystem that is owned and operated by a large number of providers bound by standards of interoperability, serving an interconnected subgroup of end-users (i.e. services based on the E.164 numbering plan). OTT providers, on the other hand, compete between ecosystems and for subscribers using multiple similar services of competitors and without the need to follow standards of interoperability.[84]

- The EU and US advertising markets

In this section, we present some information on the EU and US advertising markets. The two markets differ with regard to the presence of regulation: In the U.S. case, there are no strict laws explicitly aimed at Online Behavioural Advertisement (OBA) and

[80] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 13.
[81] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 13.
[82] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology.
[83] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 66.
[84] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 100.

transparency towards users. In the European Union, several laws and regulations apply to the OBA industry. The ePD has an indirect link to both markets through its provisions concerning the tracking of consumers and their online behaviour by means of cookies on websites (e.g. for the purpose of targeted online advertising), as well as – subsequently – sending consumers commercial communications containing marketing material. The purpose of the section is to give the reader a high-level overview of the relevance of online tracking and targeted advertisement for the sector and the size of both markets. Article 5(3) of the ePD affects the advertisement market via its rules on cookies.

ANNEX 5: BASICS OF THE ONLINE ADVERTISING MARKET (TECHNICAL AND ECONOMIC)

5.1. Snapshot of behavioural advertising practices with an impact on individual's privacy[85]

What is behavioural advertisement? A number of technologies and techniques exist to observe the website browsing behaviour of individuals over time (e.g., the pages that they have visited or searched). From this observation, a profile is made of each user (e.g. male v female, age, interests, likes and dislikes, wealth), which is used to show him/her advertisement that match this profile. This type of advertisement is often called 'behavioural advertisement' or targeted advertisement.

To be able to build profiles and send targeted advertisement, it is necessary to identify individuals when they move from a website to another. There are a number of technologies and techniques available. The use of cookies is the most widespread. A cookie is a small file sent from a website and stored in the users' web browser while he or she is browsing the Internet. However, other techniques are increasingly being used, such as for example, browser fingerprinting.

Companies and players involved. Many companies/players are involved in delivering behavioural advertising, including: (a) *Publishers*: are the website owners looking for revenues by selling space to display ads on their website (e.g. an online newspaper)*;* (b) *Advertisers* who want to promote a product or service to a specific audience (company X producer of shoes) and *(c) Advertising networks providers (also referred to as "ad network providers" and "ad exchanges"),* they are technology companies which connect publishers with advertisers. They place advertisements in publishers websites (they decide that a given add will be shown in a given website). Ad networks are becoming ad exchangers and increasingly act as real time marketplaces for the purchase and the sale of advertising space. In addition, companies that conduct market analysis of users' data are also active in this space.

How does it work? The following is based on the use of cookies as tracking technology**.** A publisher reserves space on its website to display an ad. The ad network provider places a tracking cookie on the data subject's' browser, when he/she first accesses a website serving an ad of its network. The cookie will enable the ad network provider to recognise a former visitor who returns to that website or visits any other website that is a partner of the advertising network. Such repeated visits will enable the ad network provider to build a profile of the visitor which will be used to deliver personalised advertising. Because these tracking cookies are placed by a third party that is distinct from the web server that displays the main content of the webpage (i.e. the publisher) they are often referred to as "third party cookies".

[85] This summary is based on Article 29 Working Party Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010 and on a report of the Norwegian Data Protection Authority entitled '*The Great Data Race, how commercial utilisation of personal data challenges privacy*", November 2015. It also based on a report **produced by IHS and sponsored by IAB Europe, "Paving the way: online advertising in the European economy,** November 2015. We have included an excerpt from the JRC Contribution to the revision of the ePrivacy Directive, of 5.5.2016.

The larger the advertising network, the more resources it has to monitor users and "track" their behaviour.

What are the economic implications? Online advertising in general and more specifically behavioural advertising is a driver of the digital economy that promotes business and economic growth. The most important players are Google (DoubleClick) and Facebook. According to newspapers report, in the second quarter of 2016 the two companies together made $13.1 billion profits[86]. However, many more companies are active in the ad ecosystem. For example, according to **HIS/ IAB Europe report, publishers** active in Europe generated revenues of €30.7 billion from online advertising (this is not exclusively behavioural advertisement as it may include other contextual advertisement), this represents 30.4% of all advertising revenue. The same report estimates that 0.9 million European jobs (or 0.4% of the EU-28 total) are directly supported by online advertising.

[86] *Four days that shook the digital ad world, available at:* http://www.ft.com/cms/s/0/a7b36494-5546-11e6-9664-e0bdc13c3bef.html#ixzz4IG8JgHEk, *TV Ad Growth Overshadowed by Surge of Digital Giants Like Facebook, Google,* available at: http://variety.com/2016/voices/columns/facebook-google-ad-growth-1201839746/.

ANNEX 6: DRAFT DG-JRC CONTRIBUTION TO THE REVISION OF THE EPRIVACY DIRECTIVE

European Commission

JRC TECHNICAL REPORTS

Privacy in Mobile Devices and Web-Applications

A DG-JRC Contribution to the revision of the ePrivacy Directive

Neisse Ricardo, Kounelis Ioannis, Steri Gary, Nai Fovino Igor

Distribution List: EU Commission Staff

2016

Joint Research Centre

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

Contact information
Name: Igor Nai Fovino
Address: Via E. Fermi 1, Ispra, 21027, VA, Italy
E-mail: igor.nai-fovino@jrc.ec.europa.eu
Tel.: +39 0332785809

JRC Science Hub
https://ec.europa.eu/jrc

JRC103740

Luxembourg: Publications Office of the European Union, 2016

How to cite: Author(s); title;

Table of contents

ABSTRACT

Scope of this report is that of supporting DG-CNECT during the early stages of the ePrivacy revision with evidences and technological options for what concerns cyber-security and privacy of mobile and web services.

The report analyses the main privacy threats rising from the use of new communication services, mobile technologies and web-applications.

The major concern emerged in the study, when speaking of privacy of telecommunication/online services is related to the lack of end-users' free will with regards to their sensitive information.

If we take as an example the cookies, we can undoubtedly claim that the previous implementation of the ePrivacy directive failed in promoting transparency and privacy awareness in digital services. Hence, the identification of a new, efficient, and effective way to give back the control of personal information to the end-user is needed, and the review of the ePrivacy directive is the best occasion to elaborate on this challenge.

The problem is in a way not trivial due to the fact that even if formally the concept of privacy has a clear definition, in practice, it is often in contraposition to the need of certain information to enable the delivery of a service.

The adoption of very prescriptive and stringent measures forbidding access to all possibly sensitive information of an individual has been proved to be a bad option, as modern datamining and inference techniques can easily be used to infer from explicit, completely depersonalized information, implicit sensitive information, circumventing in this way every type of legislative limitation.

If we look to the roadmap of the Digital Single Market, it is evident that the digital privacy will have to coexist with the more and more pressing need of opening up the free flow of data in the DSM, to boost innovation and new economic opportunities.

The key to allow the coexistence of these two needs (or principles) lays on the ability of the ePrivacy revision to ensure two key principles:

1) Trust in the services provided
2) Full knowledge about which data is shared with whom

Under this perspective the report presents several technical recommendations which could be taken into consideration to enable a more privacy friendly digital space.

1 Introduction

In the past years, the Commission has started a major modernisation process of the data protection framework; as part of this reform, the Digital Single Market Strategy prescribes that the Commission should also review the rules on ePrivacy directive and deliver a legislation that is fit for the digital age.

The objectives of the review are:

1. Ensuring consistency between the ePrivacy rules and the new General Data Protection Regulation
2. Updating the scope of the ePrivacy Directive in light of the new market and technological reality
3. Enhancing security and confidentiality of communications

Scope of this report is that of supporting DG-CNECT during the early stages of the ePrivacy revision with evidences and technological options for what concerns objectives 2 and 3 in the area of mobile devices and web-applications.

The report analyses the main privacy threats rising from the use of new communication services, mobile technologies and web-applications.

In particular, after having set the scene for what concerns the technological elements involved in modern digital interactions, the report presents a description of the Mobile App ecosystem with a particular emphasis on Android and iOS systems (which together account for the majority of the Mobile Operating Systems market).

An analysis of the relevant threats to which the end-users are exposed in the mobile world is provided, together with a set of guidelines which should be streamlined in the mobile app life cycle to enhance the level of privacy and security of the digital ecosystem.

The report addresses also the “web-application” environment, with a strong emphasis on the so called cookies (one of the targets of the old ePrivacy directive) and tracking, analysing how they evolved in the last years, identifying some technical solutions today in place and putting in evidence how a new policy package would be needed to enforce the privacy of the end-user.

Finally, technological and policy options are proposed in the conclusions of this document.

2 Setting the Scene

The scope of this section is that of "Setting the Scene" with regard to the possible source of "privacy" weaknesses for what concerns the ecosystem which should be taken into consideration in reviewing the ePrivacy directive (2002/58 amended with Directive 2009/136). The potential surface of analysis of the digital privacy domain is extremely wide, it is therefore important to set the boundaries which can be considered pertinent to the ePrivacy directive, to avoid dispersion of resources and efforts (for a definition of the terms used in this document, please refer to Appendix A).

Figure 3 depicts a reference architecture diagram to assist the definition of the boundaries of the ePrivacy Directive study. The lines represent interactions between components and the dashed lines indirect interactions, which may be carried out using a supporting networking mechanism (e.g., telecom network). This figure shows a scenario where a user accesses an application running in the end-user device, and an Internet of Things (IoT) device that monitors the user environment and exchanges data with and IoT hub located in the user vicinity. Both application and IoT hub communicate with backend services through a telecom network. Both end-user device and server may be implemented using a virtualization infrastructure.

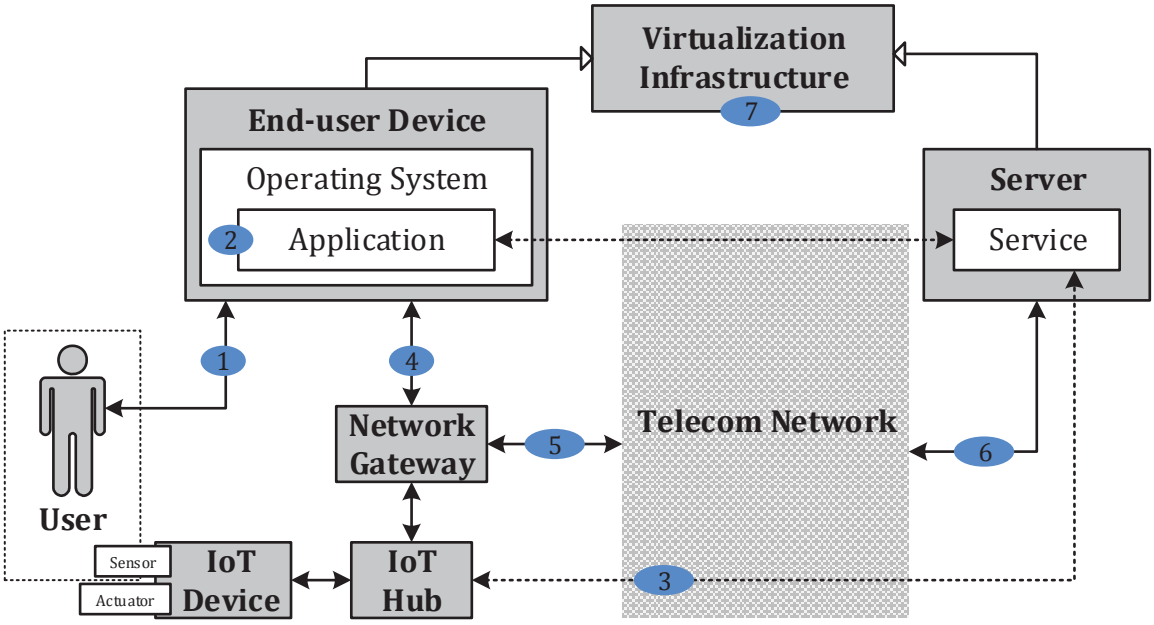


Figure 3 – Abstract architecture diagram

In order to clarify the focus of the study a set of blue ellipses numbered from 1 to 8 representing **security and privacy mechanisms** are depicted in Figure 3, with the following meaning:

1) **User-centric**: user-centric security and privacy mechanisms accessible through their devices that inform users about their privacy settings including preferences (e.g., cookies) and information regarding the collected data about them by the different entities such as native apps, web browsers, and web applications. The study should detail the mechanisms considering the scope chosen, for example, if the focus is decided to be on Android apps then user-centric privacy mechanisms should be included.
2) **Application Runtime Environment**: mechanisms provided by the operating system to control rights and obligations of native applications, for example, which resources can be accessed and how the stored application data is managed.

3) **IoT communication with Cloud**: mechanisms to enable control over the flow of information between IoT hub devices and server-side components that may retrieve/store IoT device data, and maybe also include firmware updates.
4) **Device Network Gateway**: mechanisms available for users to evaluate their connection to the network, for example, to use restricted configurations for public/private access network hotspots (e.g., open WiFi networks).
5) **Telecom Network User Access**: mechanisms to prevent user tracking/traffic monitoring by telecom network providers (e.g., Tor). This should also include a security and privacy analysis of different protocols used, for example, for VoIP (Voice Over IP), instant messaging, etc.
6) **Telecom Network Server Access**: same as 5, but from a server-side infrastructure point of view, for example, cloud computing platform providers (e.g., Amazon cloud) could also monitor users.
7) **User/server-side Virtualization**: mechanisms implemented using virtualization that could offer an advantage from a security/privacy perspective, for example, client-side sandboxing of apps. From a server-side it is unclear if any virtualization approach could offer an advantage.

Figure 4 describes instead the different interactions between applications and services running respectively in the end-user device and server. More in details, we consider any type of applications that run directly under control of the respective operating system including those particular types of applications that use a runtime environment inside of a web browser, namely web apps (a.k.a. websites). Web browsers typically also support an extension mechanism based on add-ons or plugins that allow any 3rd party to extend their functionalities, for example, to allow visualization of particular types of content (e.g., Flash) or to include extended security management functionality (e.g., cookie management). In the server side we depict software distribution and management platforms to distributed applications including updates (e.g., Google Play for Android mobile devices) and the backend components of web apps. We distinguish between the end-user and server side components of web apps since they have different implications in the user privacy: the end-user side may include executable code to collect user information that is further communicated to the server side part for processing. Similarly to Figure 3, the set of blue ellipses to Figure 4 represents **security and privacy mechanisms** with the following meaning (the list of examples in the yellow boxes is indicative and not exhaustive):

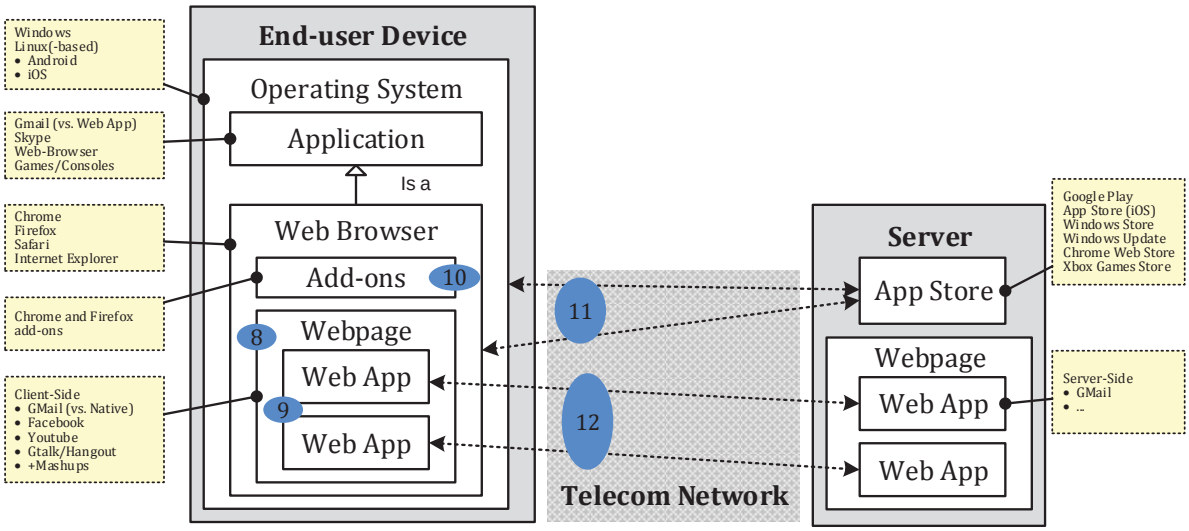


Figure 4 – User Applications and Server Services

8) **Web Applications (end-user side)**: mechanisms provided by the web browser in order to protect users from data collection on the client side, for example,

private browsing modes and cookie management. It also includes mechanisms to enable control of the resources and local cached data of web applications.

9) **Mashups of Web Apps**: mechanisms used to manage the flow of data between complex web apps that are in fact a composition of many apps. For example, some apps may embed social networking functionalities (Facebook/LinkedIn like buttons) in their pages, use external services (embedded Google Maps) that enable flow of sensitive user data, or even use a single-sign-on mechanism (Facebook/Google account) to access different web applications. The focus is on the analysis of permissions and security mechanisms that allow users to control their flow of data, as well as information about this flow for a scenario like the ones described above.
10) **Web Browser Add-ons:** mechanisms used by browsers to control the permissions of add-ons that can be installed by users in their web browsers. Add-ons are particularly dangerous since they may allow the installation of executable code that may indiscriminately have access to all user sessions and web app data.
11) **Web Applications (server-side)**: mechanisms used to control flows and management of user data by the server-side part of web applications, including privacy preferences that regulate the access and future use of this information. Detailed user tracking data stored for advertisement and analytics purposes should also be covered.
12) **Software Installation and Updates**: represent mechanisms that support users in the installation or update of software including native apps, web browsers and their add-ons, operating system components, etc. A main point of interest is app markets currently deployed for different platforms, which may be able to track users since they are aware of the precise software stack configuration and can be used for device fingerprinting.

From this list of security and privacy mechanisms, points 1, 5, and 8 are already addressed in the current Directive, but the advent of new technologies requires revising them together with further investigation on all other points.

As claimed before, the surface composed by these elements is too wide and a prioritization is needed to allow an effective support to the ePrivacy revision process.

With reference to the previous domains, here below is a prioritization list of the areas addressed in this document:

1) **Operating Systems**
2) **Privacy settings including preferences (e.g., cookies)** of modern Internet services.
3) **Web Applications (end-user side)**
4) **Web Applications (server-side)**
5) **Software Installation and Updates**

In the following sections we develop these topics starting from the ground (operating systems).

3 User Applications

User applications refer to applications that are installed on the users' device. They provide all possible functionalities to the users, boosting their experience with their device and allowing them to personalize it in order to meet their demands. Applications are usually downloaded from the associated application market of the device but, especially on desktop computers, can also be downloaded freely from any source.

3.1 Malicious Applications

The aim of malware found on applications is mainly to steal personal user information that could be later used on the advantage of the attacker. Such information can be for example, credit card numbers, user biographic information, user activities, etc. The most common way that malware reaches the users' device is through an infected application. In the next sections we explain the appearance of malware in different platforms and the reasons for the diversity between different operating systems.

While analysing the privacy issues of malicious applications, it is in any case important, especially in the context of this document, to take into consideration that the same problems, are valid also for perfectly licit applications, which might fall somehow on the "malicious side" due to their invasiveness in term of privacy. What we mean with that is that privacy breaches are not the exclusive domain of software developed by hackers, but also of applications downloaded through licit channels which pay little attention to the privacy rights of the citizens and that gather more information than what they indeed need to operate, without asking the consent to end users.

3.1.1 Android (Google)

The vast majority of the malware written for mobile devices is targeting Android, reaching 97% [1]. The main reason for this is the very big market share of Android (around 80% [2]), which makes it the preferable target, as well as the business model that Android uses. Android gives the users the possibility to download applications from any market, even if they do recommend using the official download channel of Google Play. Moreover, as Android is open source, it is used by many different manufacturers, each of which implements and maintains it in a different way. For example, if a security vulnerability is found and Google fixes it with a patch, a new update will have to be downloaded on the Android devices with the same OS version. This happens almost directly for the Google devices (i.e. all Nexus/Pixel devices) but for the rest, the manufacturer (e.g., Samsung, HTC, Motorola, etc.) will have to first receive the update, integrate it with their customized OS and then release it to the users. This procedure takes usually a lot of time, and sometimes does not happen at all, thus leaving users vulnerable to known threats. Moreover, the customized OS that each manufacturer provides, may be vulnerable to even more threats compared to the native Android OS as it has more services built on top of it (a detailed description of Android's update model is given in 4.1.1).

3.1.2 iOS (Apple)

iOS on the other hand is a closed environment and Apple is the only manufacturer. The procedure of "publishing" an application on the App store goes through an extended review which among others controls the application for malicious content. Even with these measures in place, there have been cases where malware applications have reached the App store [3].

Moreover, in contrast with Android, if a user wants to install an application from another market he/she will have to jailbreak his/her device. That means that he/she will voluntarily remove security measures from the device in order to give access to other markets. Of course by doing so, the risk of being infected with malware is highly increased. Apple is trying to prevent this from happening and after each release of iOS jailbreaking is becoming more and more difficult. Furthermore, users that jailbreak their

device automatically void the phone guarantee and cannot download and install any OS updates.

3.1.3 Mobile Apps (General)

In 2015, the Kaspersky Lab detected almost 3.000.000 malicious installation packages, 900.000 new malicious mobile applications, and 7000 mobile banking trojans. In general, there is an increase of malware compared to the last years [3].The most common malware categories are Trojans, Adware and PUA (Potentially Unwanted Applications) [1].

According to OWASP (Open Web Application Security Project), the top 10 Mobile Risks are the following [4]:

1) **Weak Server Side Controls:** Refers to vulnerabilities found on the backend of the application, e.g., backend API service, web server, etc. Even if this risk is not specific to mobile applications, it is also very relevant in a mobile environment.
2) **Insecure Data Storage**: Most of the applications that handle data input save data locally on the device. It is important to keep such data protected and prohibit access from unauthorized actors. This is even more important with sensitive data such as passwords, credit cards, etc.
3) **Insufficient Transport Layer Protection:** Many of the applications communicate with a service over the Internet. It is thus very important to control if the connection is properly encrypted, if the certificates used are valid and make sure that the connection is made towards the intended party.
4) **Unintended Data Leakage**: Unintended data leakage refers to data leaking due to vulnerabilities that are external to the application itself. For example, data that leak because of vulnerabilities of the underlying operating system, of the hardware, of frameworks that interact with the application, etc. In such cases, it is important that the developers of the application have sufficient documentation to all the services that interact with the application in order to limit such leakage.
5) **Poor Authorization and Authentication:** The applications that require authentication, should make sure that the authentication is equivalent to the one used when browsing from a computer. It is also important to avoid authenticating on the mobile device but instead perform authentication on the server side.
6) **Broken Cryptography:** This risk underlines the dangers of using cryptography in an insecure way. This may mean that either a process is using well-known cryptographic algorithms in an improper way that make them insecure or that the cryptographic algorithms are not secure themselves or are outdated.
7) **Client Side Injection:** Client side injection occurs when a source of the application's input has been tampered with and is used to insert malicious code inside the application. Such inputs can be the data found on the local storage of the device, e.g., though a database or local files, user sessions on the browser, etc. All the inputs of a mobile application should be well known and protected accordingly.
8) **Security Decisions Via Untrusted Inputs:** An application exchanges data with many different actors through a process called Inter Process Communication (IPC). This risk concerns the implications of handling in an insecure way such communications. All input received should undergo validation and the use of IPC should be in general restricted to the only absolutely necessary cases.
9) **Improper Session Handling:** This risk refers to handling in an insecure way a session once a user has been authenticated. Several attacks can take place at a session level, and it is therefore important to take the appropriate precautions in order to avoid them.
10) **Lack of Binary Protections:** Binary executions refer to alterations of the original application after it has been released. These can happen at the mobile device, for example, if an attacker modifies on purpose a part of the app in order to misbehave for his/her own benefit. Secure coding techniques are the most common countermeasure for this threat.

As it can be concluded from the threats above, most of them (2, 3, 5, 6, 7, 8, 9, 10) can be dealt with during the development phase. **Introducing security and privacy by design** is a key factor in reducing such risks. In general it should be pointed out that software security is a system-wide issue that takes into account both security mechanisms and security design [5]. It is therefore important to remind developers of this, since security design is neglected (usually in the favour of functionality) as there is the belief that its lack can be later replaced by using security mechanisms.

Risks found on the backend and not on the user device (1, 4, 5, 9) should also be considered starting from the design phase of the application's architecture. As these interactions occur outside the mobile device, they may often be neglected or left to be considered in a later stage. Dealing with them is sometimes not the application's developer role, since third party services are mostly used for the backend. Nonetheless, the developers should adhere to the codes of practice for secure programming and minimize potentials risks by paying attention to common and well-known security issues. Finally, some of the threats (4, 10) cannot be completely controlled by the application. In such case developers should make sure that they have used all possible mitigations and security mechanisms on their side and should monitor the application dependencies for any new security updates and patches in order to ensure that any new threats will be dealt with immediately.

3.1.4 Desktop Operating Systems

In principle, desktop operating systems traditionally designed to run on desktop machines and servers should not be taken into consideration in the context of the ePrivacy directive, which deals with telecommunication services and the security of terminal devices. However, two new elements recently emerged which might change this statement:

1) **Operating system convergence**: terminal devices are becoming more and more as powerful as desktops. Operating systems producers, in an attempt, on one side, to provide a homogeneous user experience, and on the other to optimize the resource investments, are pushing for a fast convergence in operating systems. The last version of Windows 10 running on Windows phones for example, is the same that today runs on every desktop, notebook in the market. The same is happening for the Linux world, where new raising distributions are able to work both on mobile phones and on desktops.
2) **Telecommunication layer convergence**: with the advent of VOIP, and the delivery of application layer communication services, the definition of "terminal device" most probably needs to be updated and expanded to the domain of portable devices and desktop.

New services providing similar functionalities available previously only by means of dedicated telecommunication services in portable devices and desktops are now available including:

- Instant messaging services like Hangouts, WhatsApp, Facebook Messenger, and Skype.
- Mashups of social networking and advertisement networks that are able to track fine-grain users' activities and collect information about their preferences for marketing purposes. For example, some web pages and mobile apps introduce advertisement banners and embed their own code (e.g., Facebook like button or comment box) in all different locations in order to track users and provide personalized content/ads.
- Video Broadcasting: service providers broadcasting video and collecting preferences, traffic, and location data of end users such as YouTube, Netflix, SkyGo. In these services users are also able to manage their own channels and provide their own customized content in partnership with advertisement services.

For these reasons we also include in the following sections some reflections on the security of desktop operating systems, without pretending to be exhaustive, but with the intention to remark the fact that the distinction between the desktop world and the mobile world is quickly fading and blurring.

3.1.4.1 Windows

Windows is the most common target of malware in the domain of desktop operating systems. There are many different reasons for this.

First of all, and probably most importantly, Windows is by far the most used operating system. So, as a natural consequence, most of the malware are specifically targeted for Windows, reaching directly the vast majority of desktop users, trying to exploit known vulnerabilities of the different Windows versions.

Moreover, the first versions of Windows (i.e. 3x, 95, 98) did not distinguish between users. All users had the same privileges on the system, which actually meant that all users were administrators. As a result, a malicious application once executed could immediately gain permission to sensitive data and functions. Moreover, there was neither an antivirus nor a firewall installed by default. The majority of the Windows users had no interest or knowledge of the need of such applications and the OS was left without any protection. In general, Windows was initially developed without having security in mind and this affected largely its future versions.

With the latest versions of Windows the situation changed, as Microsoft introduced UAC (User Account Control), which prompted the user for permission when an application was requesting admin rights. Moreover, by default the users where not set directly with admin rights and they were asked every time an application requested admin access. Additionally, an antivirus program and a firewall came preinstalled with Windows.

Another important reason for Windows to be a common target of malware is the fact that there is no central store where users can download applications. The users can download an executable from any place on the internet and execute it on their computer. As a result, many websites contain malicious applications and trick users in downloading them. Another popular approach is to infect the operating system through a third application. For example, use a malicious PDF or MS Word document that will exploit a security vulnerability on Acrobat Reader or MS Office and then affect the operating system.

3.1.4.2 Linux\Unix

Few malwares exist for Linux (Ubuntu, Debian, Fedora, Red Hat, CentOS, etc.) and Unix (OS X, BSD, Solaris, etc.) systems, compared to the quantity of malware for Windows. One of the main reasons for this is that unlike Windows, you download software from trusted software repositories (something similar to the App Store and Play Google for mobile devices). As a result, the software found in such repositories has been checked and can be trusted.

Moreover, users on Linux and Unix are given only the basic user rights. They perform most of their actions as normal users and only when a sensitive action that requires more rights is needed, they temporarily switch to becoming root.

Finally, Linux and Unix have a very limited share on the computer market and consequentially attract less attackers. Even more, most of the users of such operating systems are advanced users and are well familiar with the system they are using and with the consequences of their actions.

OS X, the operating system that Apple computers use, is a Unix distribution. It has the same and in some cases enhanced security features compared to other Unix OS. Moreover, like iOS, it has a dedicated App Store and mechanisms that control that the applications installed come from verified producers and do not include malware.

4 Mobile App Ecosystem (a detailed look)

The key element for the security of any IT device is the operating system controlling the way in which hardware operate. In this section we review the Android and iOS mobile operating systems (the two dominating OS of the market). We discuss the operating system structure, the app execution environment, the permission management model, the app distribution and code protection approaches, the app data protection model, and threats for users of both operating systems.

In Android and iOS app permissions are requested when specific resources and information found at the operating system/device level are needed for the app to function. These requests are handled differently on each OS and it is the user that in the end decides whether to grant or reject the access. Permission management plays an extremely relevant role when speaking of privacy, since it is only because of the granted permissions that an application is allowed to gather a certain type and amount of information from a terminal device. Until the version 6.0 of Android, Android and iOS had a quite different approach for handling application permissions, but this situation has now changed as it will be discussed in the following subsections.

The final goal of this chapter is to have an overview of the structure and security mechanisms of the two most common mobile operating systems.

4.1 Android

Android is the dominant operating system for mobile devices; it currently has the largest installed base mainly because it is supported by many different mobile phone manufacturers. Moreover, it supports a huge variety of different devices such as watches, tablets, TV sets, etc.

Due to its large adoption and everyday use to perform on-line tasks, malicious developers/hackers are increasingly targeting this operating system. Even if the Google Bouncer [6] security service scrutinizes applications before allowing them to be published in Google Play, there are evidences [7] showing that malicious software (malware) can be found among legitimate applications as well. In most cases, the main goal of these malware apps is to access sensitive phone resources e.g., personal data, the phone billing system, geo-location information, home banking info, etc.

4.1.1 Operating System Structure

The security of the Android OS is mainly achieved by its subdivision into layers, which provide platform flexibility and separation of resources at the same time. This separation is reflected in the whole software implementation, shown in Figure 5. Each level of the stack assumes that the level below is secured. In this section we focus on the security of apps, which run in the Dalvik Virtual Machine (DVM), and have their own security environment and dedicated file system (every mobile app runs into a completely separated virtual environment, emulating the underlying real hardware). The DVM has been completely replaced by the new Android Runtime (ART) from Android version 5.0 (Lollipop) on.

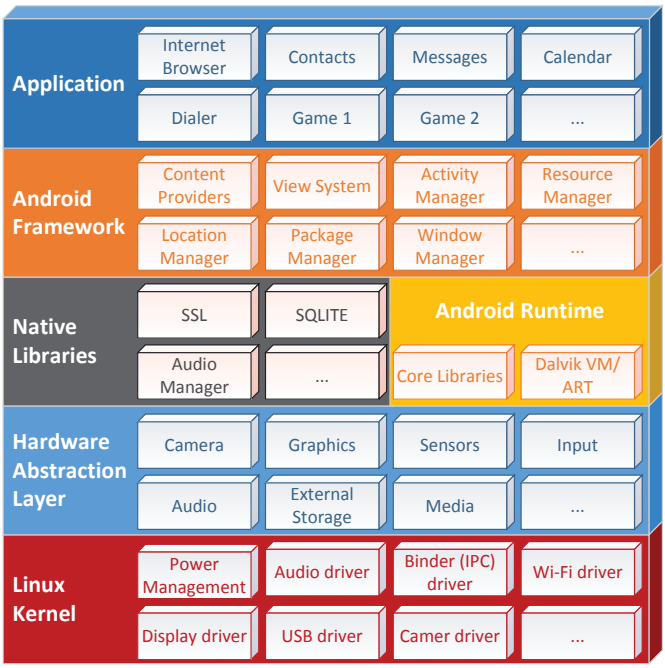


Figure 5 – Android software stack

One of the aspects which characterized the Android OS since its first deployment is the possibility given to Original Equipment Manufacturers (OEMs) to perform "heavy" customisations. This has an effect on the chain mechanism to deliver the security patches related to the operating system:

- When a vulnerability is identified, Google releases a patch for the stock version of Android (i.e. the version released by Google without any type of skin, bloatware etc.) to the OEMs;
- The OEMs, if needed, work on the patch to adapt it to their phones. Moreover, they release the new version to the telecommunication carriers for the cases where the update is performed through the carrier and not the OEM (i.e. SIM-locked devices, carrier specific devices, etc.);
- The carriers, if needed, work on the patch to adapt it to their branded phones, and release it to the end-users.

This approach has two negative effects on the security of the OS:

1) The time between the moment in which the vulnerability/problem is discovered and the moment in which all the systems are patched can be considerably long;
2) The OEM can decide to stop the support to a given OS version at any time, making virtually impossible to those terminals mounting this OS version to get the update.

The second point is indeed extremely critical from a security point of view, since it leaves a huge portion of the active smartphones in the world un-protected against the last discovered threats.

4.1.2 App Execution Environment

The security mechanism for app isolation, which is also in place for native code invoked by the apps[87] is called the Android Application Sandbox. This sandbox is set up in the

[87] Libraries and classes usually written in C/C++ and compiled for a specific hardware platform, which can be called by the app bytecode

kernel, thus propagating the isolation on all the layers above and on all kinds of applications. All apps running in the Android OS are assigned a low-privilege user ID, are only allowed access to their own files, cannot directly interact with each other, and have a limited access to the OS resources. The isolation is a protection against inter-process security flaws, meaning that a security problem in a given app will not interfere with the resources of other apps.

4.1.3 Permission Management

In the Android Software Development Kit (SDK), the functionalities an application can use are categorized and grouped in APIs that give access to resources normally accessible only by the OS. For example, among the protected APIs there are functions for SMS and MMS management, access to location information, camera control, network access, etc. The access to the protected APIs is regulated by a *permission mechanism*, in which a specific permission should be granted to an app at installation time in order to allow access to a particular API. Unprotected APIs do not require any special permission to be executed by the app.

More specifically, permissions in the Android OS are grouped in four different levels considering the risk level introduced to the user: *normal*, *dangerous*, *signature*, and *signature-or-system*. Normal permissions are considered of low risk to other apps, the system, or the end-user [8]. Dangerous permissions have a high risk of negative consequences for the users' personal data and experience. Signature permissions are used to protect exported interfaces accessible only by apps signed with the same developer key. Signature-or-system permissions are used to protect core resources available only to trusted system apps signed with the firmware key. When installing an app users are notified only about the dangerous permissions required by an app; normal permissions are granted by default.

The mapping of permissions to methods in the Android APIs is one to many, a characteristic that contributes to make less clear/deterministic which kind of and the actual functionalities an app actually uses. All permissions required by an app are declared in the app *Manifest file*. Previous to Android version 6.0 (Marshmallow), when installing an app the user was notified about the permissions needed by the application itself and then he/she had to decide if the permissions should be granted or not. In case the user did not agree to grant one or more permissions, the app could not be installed. Instead, only if the user agreed on granting all the requested permissions the app could be installed, and as a consequence would be allowed to use of all the APIs and functionalities related to those permissions.

In the Android version 6.0 (Marshmallow) release runtime or time-of-use permissions were included as well [9], in addition to install-time permissions, which were already supported in the previous versions. Time-of-use permissions give users the possibility of denying a permission request at runtime, or permanently revoking an install-time permission already granted. This new privacy feature shows that the Android community recognizes the need for more advanced privacy and anonymity control for end-users.

Even though time-of-use permissions allow end-users to better control over the restricted resources, one drawback introduced is the additional overhead for end-users because they may be asked multiple times to decide about an app permission request during runtime. However, this usually occurs during the first time the app is executed, or if the user manually changes the permission from the device’s settings. If he/she does not want to be asked all the time, it is possible to select the option to never ask again about the same permission. Nevertheless, the lack of protection of many sensitive API functions, the possibility of manipulating apps' features and services, as well as the lack of a restrictive policy-based approach that allows end-users to automate decisions with respect to the protection of their data, privacy, and anonymity, indicate that complementary research work is needed in the Android platform.

In Android, upon selecting the application you wanted to download and install from Play Google, you were shown with a comprehensive list of all the permissions that the application requested. There was no choice to select some of them; you either had to accept them all or simply not install the application (Figure 6). However, from version 6.0, after the installation you are prompted to grant access each time a special permission is required by the application (Figure 7). Moreover, you can manually change all the applications' permissions after installation from the App Permission settings (Figure 8). A more detailed description of the permission model is given in 4.1.3.

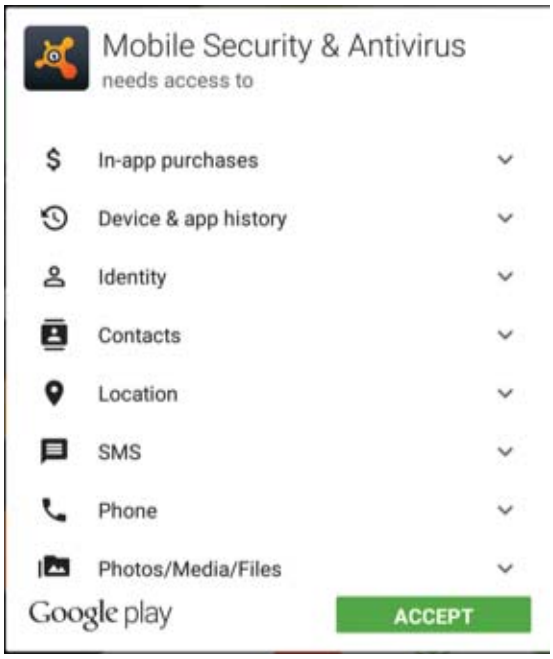


Figure 6 – Permissions on Android prior to version 6.0.

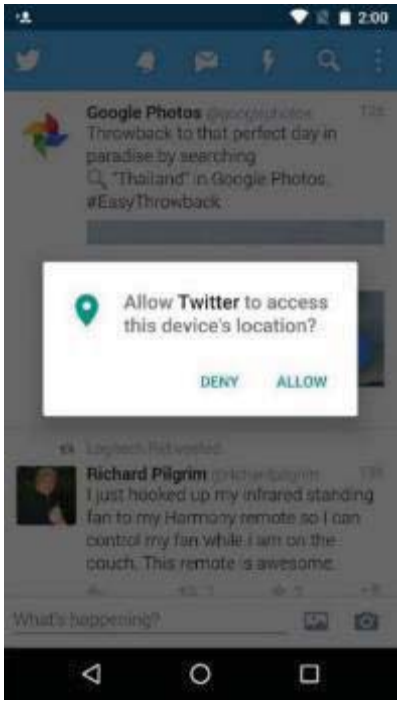


Figure 7 – An app is asking for a permission to use the device's location (Android 6.0)

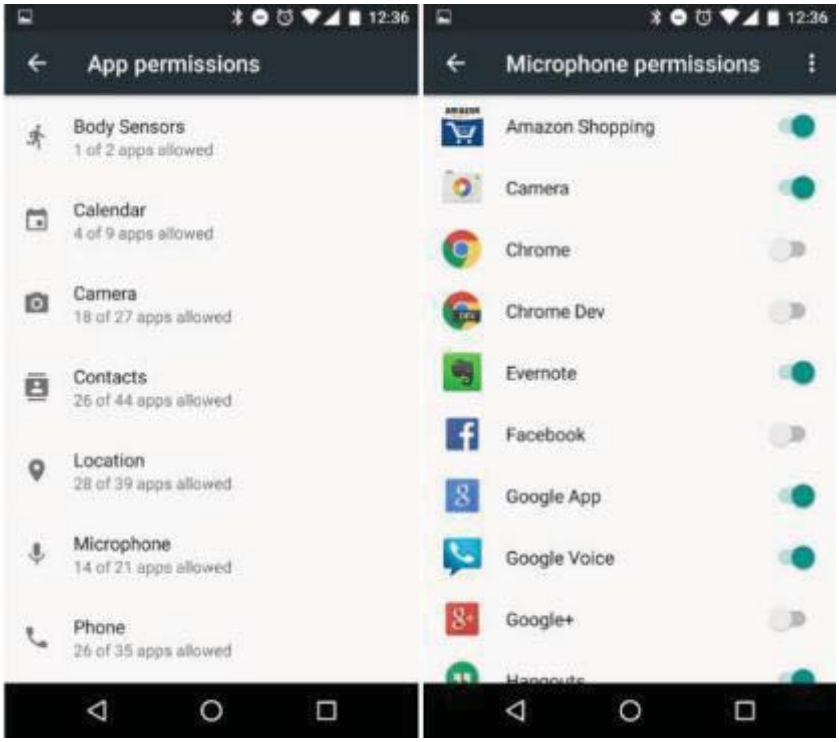


Figure 8 – The user can manually change the permissions of all apps (Android 6.0)

4.1.4 App Distribution and Code Protection

All Android apps should be signed by the developer using his/her private key. In their default configuration Android phones only allow the installation of apps from the Google Play, but this security setting can be changed in order to allow the installation of apps from any sources. Other sources of app distribution are e-mail or any arbitrary website, however, updates of apps that are not installed from the official app store are not automatically managed by the phone, so users need to update the apps manually.

4.1.5 App Data Protection

Android apps have a default directory in the internal memory file system of the mobile device to store their data (i.e. any data that the application needs in order to operate, as well as user data relative the app that is created during the app use), identified by their package name under the folder "*/data/data/<name>*". This folder contains all the app data including created databases, settings, libraries, cached data, etc. An alternative directory in external memory (e.g., SD card) is also available under the folder "*/Android/data/<name>*", which can be used in case the app expects to store a relatively large amount of data that may not fit in the internal memory space. The external memory can in fact be used indiscriminately by all apps, and they are allowed to create their own folder structure. System or root apps are allowed to read and store data anywhere in the device's internal memory as well, including access to the default directory of all installed apps. By default, the app data is stored in plain unencrypted format and is only protected by the OS standard file permissions.

Android supports also full disk encryption using the "dm-crypt" kernel feature that is available to all block devices including SD cards. If supported by the specific device the encryption key can be stored using a hardware Trusted Execution Environment (TEE).

4.2 iOS

iOS is a mobile operating system developed by Apple to be run exclusively in hardware also developed by Apple including iPhone, iPod, and iPad devices. Since the hardware of the devices is designed in parallel to the software there is a high level of optimization and customization as no other hardware manufacturers need to be supported. In this regard, this section summarizes many low level details about the iOS design and implementation considering the integration between hardware and software, which in Android would be only possible by analysing hardware details of many manufacturers.

4.2.1 Operating System Structure

Figure 9 depicts the iOS security architecture[10]. In the bottom of the picture the kernel, crypto engine, and boot ROM are part of the hardware and firmware parts providing secret and tamper proof storage of security keys, dedicated crypto engine, and kernel with secure enclaves and elements. The upper part shows the software deployment including the file system, the OS partition, and the user partition that contain the app sandboxes assigned to specific data protection classes. Both OS and file system partitions are also encrypted in the device flash memory.

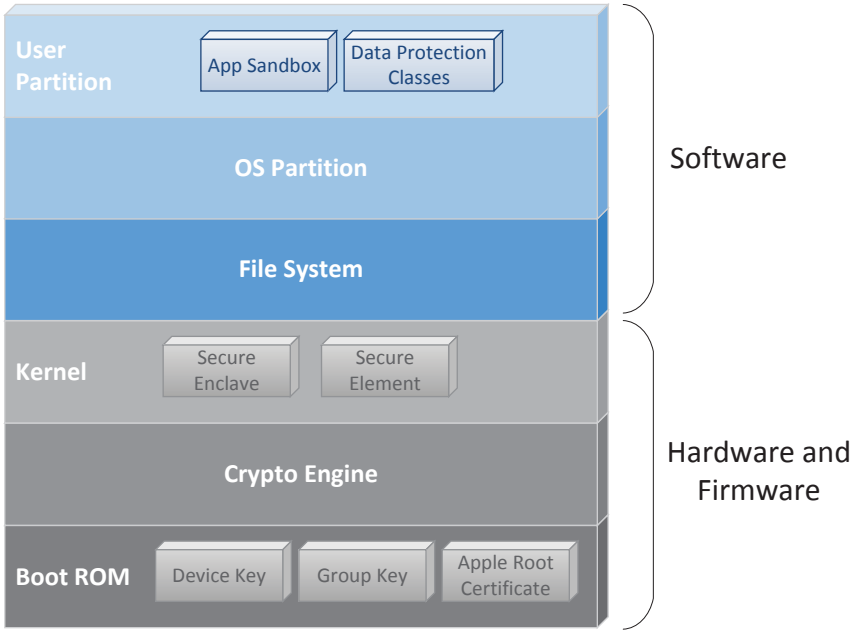


Figure 9 – iOS Security Architecture

iOS devices implement a **secure/trusted boot chain** where only code signed by Apple is allowed to be loaded and executed. The secure boot starts with the boot ROM, which is the first executable immutable code written in the hardware during chip manufacturing and contains the Apple root CA public key. This codes verifies the Low-level Bootloader (LLB) is signed by Apple and only passes execution control to it in case the signature is verified. The LLB executes, performs the device initialization, and only passes control to the next-stage bootloader if the signature matches again. This chain of trusted starting by the boot ROM, acting as the hardware root of trust, guarantees that only signed code by Apple executes in the devices running iOS.

By default, iOS is a **stripped down** OS as it does not include many binaries found in standard unix distributions (e.g., /bin/sh shell), and other utilities such as ls, rm, ps, etc. Therefore, attackers cannot use these utilities to perform analysis of the running system and in case an exploit is found for code execution no shell code can be launched and there is a limited number of activities that can be run by an attacker.

In the same way as Android, iOS implements **privilege separation** and most processes run as a “mobile” user, for example, “MobileSafari”, etc. Access to many system

resources requires superuser/root privileges, and in some cases even the superuser is not allowed to perform some tasks (for example to modify the OS executables without breaking the signature).

All iOS devices include a dedicated AES 256 **crypto engine** built into the Direct Memory Access (DMA) path between the flash storage and the main memory, allowing for highly efficient data encryption at runtime. The encryption keys are generated using a device unique ID and group ID created during manufacturing and are not visible to Apple or to any other system component. All data is therefore protected in memory using these tamper proof encryption keys. Files in the device's flash storage are also protected using encryption by assigning each file a class, where the accessibility is determined by the unlocking of a particular data protection class by any given application.

Vulnerabilities have been found in iOS allowing users to overwrite the OS code allowing the execution of code not signed by Apple. These vulnerabilities allowed users to ***jailbreak*** their devices, usually in untethered or tethered mode. An untethered jailbreak allows permanent violation of the chain of trust, while a tethered jailbreak required the phone to be plugged to a computer and the exploit has to be re-applied every time the phone is restarted to keep the device jailbroken. iOS also enforces a system software authorization process preventing users from downgrading their iOS devices, after a newer or updated version is installed it is impossible to roll back to the older and possibly vulnerable version.

Jailbreaking an iOS device essentially breaks all the security architecture since it disables code signing requirements, disables many memory protection mechanisms, usually adds user shell and remote shell access (sshd server), and adds many other user utilities with the objective of increasing the system's functionality and customization. On one hand users benefit significantly of jailbreaking their devices, however, on the other hand they also increase significantly the attack surface of their devices.

4.2.2 App Execution Environment

All apps are signed and only signed code may be executed at runtime. This feature prevents the introduction of arbitrary code and any change to the executable, allowing only code that has been reviewed by Apple to run in the mobile device.

The runtime data areas of an iOS app (e.g., stack and heap) are marked **non-executable** and at runtime no writable memory area can become executable. This low-level protection scheme prevents attackers from writing executable code in the memory and exploiting vulnerabilities in order to make the processor execute this code.

When loading an app the iOS execution environment implements **Address Space Layout Randomization** (ASLR) for the app execution artefacts including binary, libraries, dynamic loader, heap, stack, etc. Furthermore, it also supports Position Independent Executable (PIE) code, meaning that the app execution artefacts can be randomly positioned in the memory in order to prevent certain attacks, for example, a buffer overflow that could allow an attacker to selectively redirect the program to specific instructions in memory since their memory location would always be the same.

All user-installed apps run in a **sandbox** with a limited set of permissions and restricted file system access. Apple-developed applications have a less restrictive sandbox since they are compiled in the kernel and can, for instance, open the SMS database but are not allowed to fork their process or send SMS messages.

4.2.3 Permission Management Model

The list of permissions associated with an app are called "entitlements" in iOS. iOS apps may also set specific entitlements representing specific capabilities or security permissions. Entitlements may be set for iCloud data storage or push notifications to alert the user even when the app is not running. In iOS, when you download and install an application you are not shown a list of the permissions it requires. Instead, all

applications by default are granted the basic permissions as defined by iOS. Later on, when the application is running and a special/sensitive permission is required by the app, the user is prompted in order to grant or deny the permission request (see Figure 10). Moreover, from the settings and the privacy tab the user can see a list of all the permissions, the applications that use them, and can change the desired settings directly from there by granting/denying the permission for each respective app (see Figure 11).

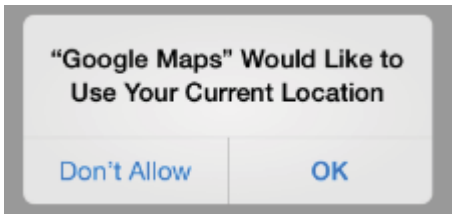


Figure 10 – An app is asking to access the location data in iOS

Figure 11 – Just as on Android 6.0, the user can manually change all permissions in iOS

4.2.4 App Distribution and Code Protection

In iOS apps can only be downloaded and installed through the App Store, which acts as an anti-virus against malicious developers. Apple verifies the real-world identities of all developers that are allowed to publish apps in the App Store. All apps are reviewed by Apple before they are made available and only **apps signed** by Apple are allowed to be installed in iOS devices.

Apps can also be packaged and provisioned to be installed on specific devices without going through the App Store. In order to be installed these apps must include the list of all device IDs they will be provisioned to, which may be a solution for enterprise apps that should not go through the App Store.

4.2.5 App Data Protection

For every new file created a data protection class is assigned to it by the respective app. If a file is not assigned a data protection class, it is still stored in encrypted form (as is all data on an iOS device). Each class has a different policy with respect to key generation and security, which is summarized in the following list:

- **Complete Protection**: The encryption key for this class of data protection is derived from the user passcode and the device UID, and is removed from the memory when the device is locked so all data is inaccessible until the user unlocks the device by entering the passcode or using fingerprint authentication (Touch ID);
- **Protected Until First User Authentication (default)**: the same as Complete Protection, except that the decrypted class key is not removed from memory when the device is locked. The data is not accessible when the device boots before the user unlocks the device for the first time;
- **Protected Unless Open**: Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background. This behaviour is achieved by using asymmetric elliptic curve cryptography (ECDH over Curve25519) that generates a per-file key wiped from memory when the file is closed. To open the file again, the shared secret is re-created using this same class;

- **No Protection**: This class key is protected only with the device Unique ID (UID), and is kept in a short time volatile memory called Effaceable Storage. Since all the keys needed to decrypt files in this class are stored on the device, the encryption only affords the benefit of fast remote wipe.

The iOS SDK provides a full suite of APIs to support 3rd party apps in the implementation of data protection primitives for data encryption of files, configuration data, and databases. In case an app does not choose an encryption scheme, the "Protect Until First User Authentication" data protection class is chosen by default for all installed user apps.

4.3 Threats to Users

The goal of the iOS and Android permission models is to protect system resources from indiscriminate and unauthorized use by apps. However, this model has some inherent problems that might affect end-users' privacy and anonymity. The following paragraphs describe the types of threats we have identified targeting the permission model for both operating systems, i.e. threats related to: pre-installed apps, permission management, permission granularity, permission notification, unused permissions, and lack of security.

First of all, pre-installed or OEM apps in Android are automatically granted all required permissions and are considered trusted since they are part of the OS firmware. Therefore, users are not informed about the required permissions of these apps, since consent is normally granted by users for an app's required permissions during the installation process. This means that end-users do not have any indication which resources are accessed by these apps, and are vulnerable to privacy invasive behaviour by them. In the case of Android 6.0 and iOS, however, the permissions are granted at runtime when the app is used for the first time and the user can check and change these permissions from the permission settings later on to revoke a specific permission.

The second important point is the way permissions are managed and granted during the app's life-cycle. As described previously, if an end-user would like to successfully install and use an app, he/she is obliged to grant all the requested permissions. As a result, a common end-user behaviour while installing an app is just to accept all permission requests to reach the end of the installation process as soon as possible. This approach is not adopted in iOS and on Android from 6.0, where the user is prompted for special permissions during the use of the app. However, also in the latter case, a reluctant user will simply grant the permissions in order to proceed and use the app. Besides, most of the end-users do not have knowledge about possible risks the requested permissions introduce towards their personal data, while the information prompted during the installation process are not really informative about the real functionalities the app is going to access and with what frequency (e.g., fine grain location tracking, access to microphone when app is executing in background, etc.).

More knowledgeable end-users might try to evaluate the list of requested permissions, but even for experts it is often unclear how permissions are used. This is a consequence of the fact that permissions are not a one-to-one mapping scheme with the corresponding method calls to Android framework API that implements the actual functionality. Indeed, their granularity is quite coarse, and, considering the 197 permissions of Android version 4.2 associated to the 1310 methods, one permission is associated on average to 7 API methods. For instance, a mobile app granted the CAMERA permission is allowed to take pictures or to capture videos using the *takePicture* and *MediaRecorder* methods respectively. This means that an end-user after grating this permission is not aware of the precise action performed by the app at any specific time since it can give access to a wider group of more or less sensitive functionalities. In iOS this is also the case, since the number of permissions is much smaller, for example, in the privacy settings users can grant/deny 11 permission groups and also additional permissions to specific functionalities introduced by 3rd party apps (e.g., post in Facebook timeline). The main issue for iOS and Android is the lack of personalized

control and customization from the user perspective since permissions can only be managed using a restricted set of options.

When revoking permissions to an app users have no guarantees that the application will function in a normal way. Some of these permissions may be crucial to the functionality of the application and disabling them may lead to malfunctioning or not being able to execute at all the application. Android developers until now were not concerned about permissions being denied since their assumption was always that all permissions needed were granted at install time, however, with the change in the permission management model from Android version 6.0 on, the recommendation now is for developers to account for the situation where not all permissions are granted in order to prevent their apps from malfunctioning or stop working in this case.

Another threat to users are the normal level permissions in Android or default entitlements in iOS, which are considered of lower risk and are automatically granted to apps without asking end-users explicitly for consent. Even if end-users have the possibility to review this automatic granting, this a priori categorization as low risk may not be perceived by all users in the same way. As a result, though the permission granting mechanism is in place, from the end-user perspective this approach may be wrongly understood as if the apps are not accessing sensitive resources at all. For example, in iOS all apps are granted access to the network by default and there is no mechanism for users to revoke the access after the app is installed.

Some apps may also request permissions that are not used in the app implementation, and that are not actually needed for accomplishing their task (unused permissions). These apps are usually labelled as over-privileged, and could lead to privilege escalation problems in terms of sensitive resources they can access after an update. Privilege escalation may also lead to confused deputy attacks, when an app that has been granted a specific permission is exploited by other apps that do not have this permission in order to perform sensitive tasks. A classic example is an app that is allowed to send SMS messages and allows other apps to use its interfaces to send SMS messages as well. Previous studies of JRC [11] [12] [13] demonstrated that the majority of the existing mobile applications can be considered today over-privileged. The reason is in general not linked to malicious purposes, but rather due to bad software development habits: the design of mobile apps with the largest set of permission is indeed a way to ensure the largest space of options when developing future software updates. Unfortunately, this behaviour even if licit, exposes the end-user to several risks. In iOS unused permissions are not an issue since permissions are only granted the first time the app tries to use it.

Finally, some methods in the Android API are still not protected by specific permissions and introduce a lack of security with respect to the sensitive resources they may allow access to. For instance, an app might use the *exec(String prog)* method to execute the process *prog* passed as parameter. This means any app could silently execute unprotected system commands in order to read system information from the *proc* filesystem, retrieve the list of installed and running apps, read the SD card contents, etc.

4.3.1 Threats to Users' Privacy

Threats to users' privacy may be posed not only by malware apps but also by legitimate apps. Many legitimate apps are characterized by a certain degree of privacy invasiveness, which is related to the permissions they request and to which use they make out of the protected methods. In this direction, TaintDroid for Android as well as other papers in the literature demonstrate the type of end-users' personal data manipulation performed by mobile apps.

Examples of privacy-invasive behaviour apps are, for instance, games that request access to unique identifiers or user location that are not needed by the app to function. Ultimately, it is up to each mobile device’s user to judge if an app’s behaviour is privacy-invasive according to his/her personal perceptions. In this direction, the Android OS and

iOS provides security services that verify apps distributed in the respective app stores before installation, and in Android also to periodically scan the OS for harmful apps.

Unfortunately, these services themselves are also privacy-invasive because, according to the Android documentation, the device "*may send information to Google identifying the app, including log information, URLs related to the app, device ID, your OS version, and IP address*"[88]. Therefore, the user-desired functionality is bound to a privacy-invasive behaviour, and users have no choice when using these services to control or restrict the personal data shared with Google. Furthermore, Google, in the Android developers documentation[89], suggests as apps distribution options alternative to the Google Play Store, e-mail and websites, thus exposing packages to the risk of malicious code injection. As a consequence, the existing features aimed at protecting end-users from privacy-invasive applications is quite limited. On the other hand, in iOS all apps must be distributed through the certified Apple app store and only jailbroken devices can install apps from other sources.

4.3.2 Threats to the OS Update Model

As every operating system, Android is not immune to software vulnerabilities. From time to time, new vulnerabilities are discovered and a patch needs to be released to fix the problem. However, as already described, the update model used by Android is quite complicated; indeed, the patch might require to be handled by several "hands" (Google, OEM, Network Carries) before reaching the end-user device.

On top of this, even if a patch is released by Google (which we remind here is the "owner" of Android), it is not automatically said that it will reach the final destination since OEMs could decide that it is not "economically" viable to invest in the re-engineering effort required to adapt the patch to their customized version of Android for each model smart-phone model they produce. For the same reason when an entirely new version of Android is released, not all the devices will be able to receive it.

Typically, low-end smart-phones "die" with the same Android OS version which was originally installed on them while high-end smart-phones receive updates for a couple of years in average. The net effect is that a huge amount of smart-phones is today using a version of Android not maintained anymore, hence potentially exposed to newly discovered vulnerabilities without any possibility of being patched.

In iOS the update model is much more agile considering that hardware and software are all produced by the same manufacturer. Therefore, updates can be released and pushed in devices in a matter of days, therefore efficiently maintaining older devices with fixed security vulnerabilities.

4.4 Comparison of iOS and Android Security Features

The following table summarizes some of the important differences between iOS and Android devices mostly with respect to the available security features.

Table 1 – Differences between iOS and Android

Feature	iOS	Android	Comment

[88] https://support.google.com/accounts/answer/2812853?hl=en
[89] http://developer.android.com/distribute/tools/open-distribution.html

Feature	iOS	Android	Comment
Device hardware manufacturer	Single hardware optimized for software	Multi-vendors and custom network carriers	iOS is capable of providing a higher-level of optimization and more agile update model since there is one single hardware and software manufacturer.
Trusted boot	Trusted boot chain in all devices from low level Boot ROM up to app/firmware level	Vendor-specific security features with different levels of assurance depending on the manufacturer and versions	iOS with a single manufacturer for hardware and software provides a higher level of assurance on average. Android in most cases can be rooted without many issues.
Roll back to previous versions	System software authorization prevents users to downgrade their systems	Users are allowed to downgrade most of Android devices without many issues	
OS customization	Single version for all device models and configurations.	Multi custom OEM versions	iOS is capable of reacting much faster to bugs since there is no need for porting the fixes to multiple vendors/carriers/etc.
App distribution and installation	Apple signs all apps and users cannot install from alternative sources, unless the device is jailbroken	Google distributes apps but users are free to install apps signed and distributed even by e-mail directly by the developers	Android users have a higher risk since they may inadvertently install malicious apps from any source
Jailbreak and rooting	Users can in some cases jailbreak their devices to run custom software not distributed through the Apple Store and have admin rights	Users in most of the cases can root their devices to have admin rights	

Feature	iOS	Android	Comment
Custom ROMs	iOS is closed source and there are no custom ROMs available. The bootloader cannot be unlocked since it relies on the signature of the firmware using Apple's private key.	Android allows custom ROMs and makes it possible because the system is open source and the bootloader can be unlocked	
Default system apps	Apple controls all default installed system apps, which are the same for all different types of devices.	Each OEM manufacturer and region may add to their devices their own custom system and pre-installed apps.	Due to the higher number of possible customizations in Android there is a bigger attack surface or opportunity for vulnerabilities to be exploited.
Memory and file system encryption	Available by default with different classes of encryption to protect against direct flash storage access using forensic tools. Relies always on tamper-proof hardware support for storage of encryption keys and execution of encryption functions.	Flash storage encryption is supported but depends on the device manufacturer. In most cases the storage of encryption keys is not tamper proof and secured by hardware.	Android is far more vulnerable to attacks using forensic tools to read data even in devices with encryption enabled. iOS implements a level of security that even Apple in some cases is not able to circumvent.
OS features	Stripped down from basic commands, utilities, and shell.	Most standard utilities are available and some are not protected by permissions.	In Android an app can run a "ps" command to get the list of running processes and infer the installed app by the users without requiring any specific permission.

4.5 General User Guidelines for Applications

From our overall experience, the below are some suggested practices in order to avoid malicious or insecure applications:

- Download applications from the original market store. Applications are controlled both before and during their availability on the market. Moreover, in case a central store is not available or the user needs to download an application outside

of the store, the origin of the application should be checked with precautions and not be blindly trusted.

- Once an application has been installed in the system, the user should make sure to update it regularly. Vulnerabilities are found during the lifecycle of applications and updates are released in order to fix them. By having an up to date application, the exposure to known vulnerabilities is decreased.
- When installing and using an application the permissions should be carefully checked. Many of the applications are over-privileged and the user should control what permissions are granted to each application.
- Avoid removing the built in security mechanisms of the operating system, e.g., jailbreak.

4.6 Considerations on privacy vs mobile OS

On the light of what described in the previous sections it is possible to identify three main sources of threats against the end-user privacy related to mobile operating systems:

1) Threats related to the permission model and to the opacity of permission granting with respect to the information surface accessed.
2) Threats related to the way in which apps get access to and treat personal information hence impacting directly the privacy of the end-user
3) Threats related to the update model adopted by Android. Indeed, the fact that Google implemented in its last version of Android (6.0) a more refined permission model allowing at run time to disable permissions previously granted to mobile applications, is a clear sign that our evaluation of the problem mentioned in point (i) is correct. However, the permission model and its implications are still complex and do not allow end-users to fully understand the implications of granting or not a permission to a mobile application.

There is here a big gap between the typical understanding of the end-user about the actions performed by the applications he/she installs and the real potential they have when granted with the full set of permissions specified in the manifest. The security update model of Android is indeed another relevant source of possible risks, since:

- it slows down the response to the discovery of new vulnerabilities;
- it leaves completely unsupported a huge portion of the installed Android systems, since the maintenance is guaranteed only for a very limited amount of time and it is completely left to the willingness of the OEMs.

This last point is the most critical since it leaves every year millions of devices prone to vulnerabilities. A survey on existing solutions allowing to deploy a more privacy and security friendly smart-phone ecosystem shows that technical solutions exist, however they are all at an academic level, hence demonstrating how, still, the industry has not yet perceived the security and privacy principles as mandatory. Indeed, this is the point where policy actions might be needed:

- **Privacy Aware Mobile Code Platform**: mobile applications need to be developed from the beginning with privacy and security in mind. Unfortunately, as mentioned in the introduction, privacy and security represent often an additional cost to software developers which can be hardly covered by the revenues generated by mobile applications downloads. In this context, a series of initiatives could be developed at European level to stimulate the creation of a new **privacy by design** development framework for mobile applications. Under this name should go a development platform putting at disposal of mobile developers pre-packaged and configured libraries already integrating privacy friendly features. In this way, the mobile-app developers would not have to invest a lot of their time in rethinking from scratch privacy enhancing solutions for their applications. A similar initiative obviously could be successfully exploited bringing

on board at the same time the big actors on the mobile app scene together with the open-source community.

- **Code Development Best Practices**: the previous initiative could have success only if accompanied by a set of parallel initiatives to foster a new generation of mobile application developers conscious of the means in which smart-phone services should be developed in a secure and privacy friendly way.
- **Certification and Labelling**: certification and labelling are two powerful mechanisms helping the end-user to discriminate between privacy respectful and privacy invasive mobile applications. It is true that the mobile application ecosystem is so vastly populated that it would be almost impossible to certify and label everything. However, certification and labelling could be requested for those applications dealing with sensitive information (e.g., mobile banking, e-government, social networks, e-health applications). The presence of a certification and labelling scheme would surely increase the level of trust of end-users in critical mobile applications and, at the same time, it could be used as rewarding mechanism for virtuous European companies, in the sense that their certification as privacy-friendly, should incentive the end-users to use their services.
- **Smart-Phone Operating Systems and Cyber Security Industry**: Europe is today in a weak position when speaking of Operating System and Cyber Security Industry. Initiatives should be taken in this area on a side to promote the design of more privacy-friendly operating systems for mobile devices, and on the other to stimulate the development of a vibrant and active Cyber-security industry in the mobile device domain. A good vehicle to stimulate developments in this area could be a set of ad-hoc crafted H2020 initiatives.
- **Data protection impact assessment:** introduction of prescriptive and sectorial rules making mandatory the execution of a data-protection impact assessment analysis for apps and OS (similar to that introduced by DG-ENER in the smart-grid and smart-metering areas).

However, the most advanced techniques to improve the privacy level of mobile-devices objects are useless if the end-user does not have any perception of the risks to which he/she is exposed. In this sense, ad-hoc initiatives should be taken to raise the awareness of the citizen toward privacy threats in mobile devices. In this area, apart from usual informational campaigns, initiatives in the educational sector (primary and secondary schools) could be a good way to forge the new generation of digital citizens with more developed privacy awareness.

5 Web Applications

Web applications can be understood as client-server application where the client runs in a web browser. The distinction between simple “web-pages” and “web-applications” is today becoming very blurry as web-pages are today rarely static and often offer several application services.

In this section we describe privacy invasive approaches used to track users including user and server-side mechanisms currently adopted by web app providers that may impact on the security of users. We also describe existing user-centric security and privacy tools/mechanisms that inform users about their privacy preferences (e.g., allowed/blocked cookies) and about the data collected about them by web apps. Tools and mechanisms include, for example, private browsing modes, cookie management tools, mechanisms to enable control of the managed resources and local cached data of web applications, privacy preferences that regulate the access and future use of this information, and detailed user tracking data stored for advertisement and analytics purposes.

Web applications usually track users [14] in order to collect data that is needed to (1) improve/adapt/customize the service provided or to (2) build user profiles that are used for personalized advertisement purposes. Examples of both categories are cookies set in order to keep track of the user session and to remember the items selected in a web-shop for later acquisition in the user shopping basket, or cookies set in order to keep track of all browsing history of users to learn their interests, preferences, and all possible information about the users in order to suggest items for them to buy.

The following subsections describe the different types of privacy intrusive approaches (e.g., user tracking), the technical aspects involved, existing tools that put the problem in evidence, and technical recommendations from the JRC or the community on how to address this problem.

5.1 Web Cookies and Trackers

Cookies are name-value pairs of strings that can be written and read by a web app in the user’s computer and are managed by the web browser (a.k.a. **web cookies**) or by the Adobe Flash Player (AFP) (a.k.a. **flash cookies**). Since flash cookies do not appear in the standard cookie management setting in the web browsers users are usually unaware of them and may not even configure any restrictions on their use simply because they do not know about this option.

Cookies are commonly used to store the user session identifier in order to allow the web app to remember the user while he/she navigates through the different parts/pages of the app. For example, if users access a webshop and add items to their shopping baskets the app is able to remember the added items and display the list later on to the users without requiring the user to explicitly login with a username and password. Cookies are also used for analytics purpose to make a complete profile of the user navigation and preferences.

The management of access rights to cookies follows a *same-origin policy*, meaning that cookies written by a specific domain URL (e.g., www.website.com) can be only accessed by web apps in the same domain. Figure 12 illustrates the scenario when a user accesses the page “showBikes” from the server with domain name “website.com”. The access consists of an HTTP request for the page, and an HTTP response by the server with the requested content. Any cookies saved in the web browser to this domain are also sent together in the HTTP request, and the server may decide to overwrite or create new cookies by embedding them in the response sent to the web browser. Cookies are simply name/value pairs, for example, the website may create a cookie to contain the user e-mail with the name/value: “e-mail=bob@website.com”.

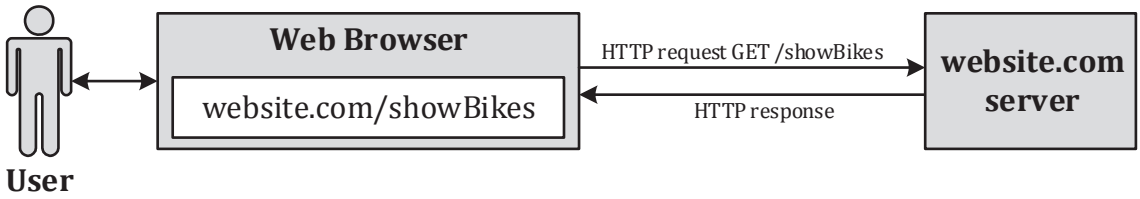


Figure 12 – Access to page in server website.com

Cookies are also sent to a website in case of a cross site request, for example, if a particular website includes a script or image hosted in www.google.com, the cookies of google are sent together in the request and may even be available to client-side scripting languages to the website that issued the request to www.google.com. Figure 13 shows an example scenario of cookie and data flow when a website hosted at "website.com" embedded content from another website "tracking.com". In this example the user is accessing the page "showBikes", and when the web browser requests the page from the server it sends in the request all the stored cookies for this domain. In the retrieved page, "website.com/showBikes" includes an embedded content for the content "banner", which is also loaded by the web browser, and the server "tracking.com" receives in the request the argument "interest=bicycles", the stored cookies for the domain, and also is able to know that the request originated from "website.com/showBikes". The cookies sent in this type of scenario to tracking.com are called 3rd party cookies, while the cookies sent to website.com are called 1st party cookies. Both website.com and tracking.com may have an agreement on the exchanged information, for example, website.com may send other arguments in addition to "interest" such as the user e-mail, location, etc. The cookies set for both websites may include any type of information encoded in strings, including encrypted information that is opaque for end-users.

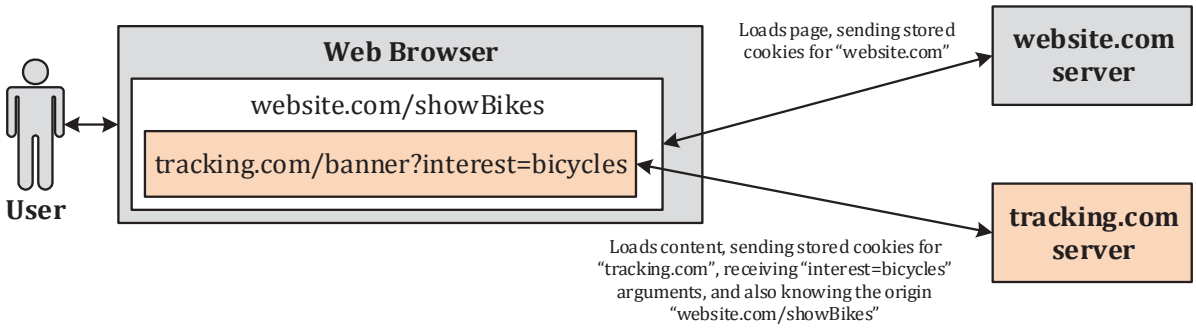


Figure 13 – Example of cookie and data flow in websites with embedded content

There are different types of cookies:

1) Cookies that manage user sessions across web pages and across browsing sessions (remember me functionality). These sessions are used to store user login information, preferences, screen and configurations to improve user experience, etc. This type of cookies should be allowed in an anonymous way for users that have no accounts in the website, and can be enabled in an identifiable way to users that choose explicitly to create an account and login in the service. Anonymous and authenticated sessions should never be linked to each other, meaning that after login or logout all associated information to the session should be deleted. All information including user input cookies associated with the sessions to that domain should be deleted as well when the user logs out and only reset when the user logs in again.
2) User input cookies: name, address, to autofill forms;
3) Authentication cookies: session identifiers, secure cookies for failed login counts;
4) User profile cookies: information about the user such as address, birthdate, etc;

5) Load balancing cookies: server cookies to redirect users to specific server farms in order to balance the load;
6) 3rd party Cookies for analytics: not a problem if IP is anonymized.
7) Social networking cookies such as twitter, etc. require consent, and are not necessary for the page, only if users really would like to use social networking functionality**.** This type of cookies could be enabled on demand if needed when users request the functionality.
8) 3rd party cookies for advertisement.

Figure 14 shows the typical content of cookies for three websites. It is rather difficult to understand what information is being stored, however, it can be seen that the user location (dy_df_geo=Europe), search queries (tc_ad_category=bicycle), and user ids (x-wl-uid=…) are stored in this case.

Figure 14 – Typical cookie format stored for news and e-commerce websites

In order to minimize privacy risks, cookies can be set for a web session only or may persist across sessions, for example, to remember the user after the browser or tab is closed. Furthermore, secure cookies only transmitted over an encrypted (HTTPS) connections, and HttpOnly cookies that are not accessible through client-side scripting

languages such as Javascript can also be defined. The Google Chrome web browser also introduced a particular type of cookie called “SameSite”, which is not sent in requests for scripts included in a website that do not share the same origin to prevent specific attacks where cookie information could be leaked. Finally, supercookies can also be defined respectively for websites that do not share the same origin and would like to share a cookie, or for websites that share a top-level domain name. For example, a cookie could be defined for the .eu domain and it would be accessed by all websites under this domain such as “www.website.eu” or “www.europa.eu” etc.

Users can configure in their web browsers the allowed cookies and domains using the standard privacy/security settings. The Vanilla Cookie Manager[90] is an example of an additional tool that improves user control over the installed cookies. Figure 15 shows the main configuration options of this tool displaying logging, a list of suggestions for unwanted cookies, the option to delete the cookies, and the option of adding a website/domain to a whitelist that allows all cookies of this domain. For less knowledgeable users a suggestion of unwanted cookies is a desirable feature since simply deleting all cookies may result in closing all user sessions and requiring the user to login again in all open web applications with possible loss of session data such as the shopping basket.

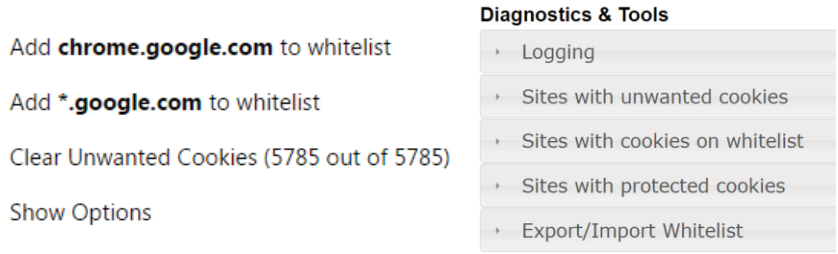


Figure 15 – Vanilla Cookie Manager options

Web trackers are complete online platforms dedicated to collect user browsing information for advertisement purposes including all the visited websites, duration of the visit, outgoing visited links, and origin/source of link. This tracking can be done using **web or flash cookies** by embedding links, hidden images, or any other type of content from third party locations. Users are mostly unware of web trackers since no user consent is asked in websites given the users the choice of allowing or preventing tracking of their online activities. In standard web browsers third party cookies related to trackers are also not explicitly shown to users.

Lightbeam[91] (formally known as Collusion) is a web browser add-on only available for the Firefox web browser that shows tracker information, including a history showing how trackers connect to each other. Figure 16 shows the Lightbeam user interface after accessing two well-known news websites, and as can be seen from the picture a series of trackers are connected to both websites, meaning that all user activities in both websites can be identified by these trackers.

[90] https://github.com/laktak/vanilla-chrome
[91] https://addons.mozilla.org/en-US/firefox/addon/lightbeam/

Figure 16 – Lightbeam add-on showing the tracker connection between two news websites

Disconnect.me is another web browser add-on[92] that monitors for every web app all visited connections (network requests) made to other web apps, which could be potentially trackers as well. All these connections are categorized into different groups (Google, Facebook, Twitter, Advertising, Analytics, Social and Content) and are blocked by default, except from requests for content that are unblocked in order to prevent the correct functioning of the web app. The user is able to decide to block or unblock any category. The add-on also shows details for each category, including the specific known trackers that may also be (un)blocked by the user. Trusted sites may be added to a whitelist and when visited all categories are unblocked. The add-on is available for Chrome, Firefox, Safari, and Opera web browsers. Ghostery[93] and Privacy Badger[94] provide similar functionality to Disconnect.me, while Privacy Badger has been conceived to work without the need for any manual configuration or expertise from the user side.

Figure 17 shows the Chrome add-on displaying network request information for a major news website. In this example there are 5 connections related to advertising, 8 to analysis, and 5 to content requests. The add-on also shows in the top of the user interface if Facebook, Google, or Twitter trackers are included in the page, which may indicate also another number of indirect trackers as well.

[92] https://disconnect.me/disconnect
[93] http://www.ghostery.com/
[94] https://www.eff.org/privacybadger

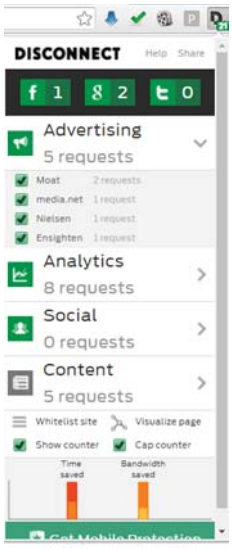


Figure 17 – Disconnect.me plugin showing advertising trackers

Existing websites request consent from users to use cookies but do not provide enough details about the purpose of the cookies they set and the 3rd party cookies included in their content as illustrated by the Lightbeam tool. The following text was extracted from a website explaining their use of cookies:

> *This website uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.*

From this description of the use of cookies the problem of user misinformation about the necessity of using cookies is very explicit. The website claims that it may not be able to provide the functionality if cookies are not enabled, while Google Analytics is simply a tool for helping the website providers to analyse the access logs, it is not related to the website functionality. The disclaimer information is also vague in the sense that is uses the expression "may", therefore the precise information that is provided in the cookies is unclear. Browsing this specific website without enabling cookies had not effect whatsoever in the functionality, in many cases cookies are only required when users need to login and establish an authenticated session with the server.

The Do Not Track (DNT) policy [15] is an opt-out approach for users to notify web servers about their web tracking preferences. It is opt-out since users have to explicitly

state they do not want to be tracked by the website. The DNT policy is implemented technically using an HTTP header field binary option where 1 means the user does not want to be tracked and 0 (default) means the user allows tracking in the website. Web servers can also communicate their tracking status [16], for example, they only track users with consent, they track users anyway, they disregard the DNT header, etc.

The "Do Not Track" option was enabled by default in Windows version 8 and Internet Explorer 10 in their express install mode, and was criticized by US advertising companies claiming that this option should be an opt-in choice by users and should not be automatically enabled. Their claim is that this choice of Microsoft was even criticized by Roy Fielding, one of the authors of the DNT standard, and was later removed from Windows version 10 express install mode.

The discussion about enabling DNT or not is inconclusive and based on the following arguments:

- Privacy protection should be set by default, and users should opt-out from it in order to protect users that are not knowledgeable and may not even be able to opt-in for the DNT option;
- Setting DNT by default violates the standard specification since it will not be respected if the recipient does not believe this field was explicitly set by a person that favours privacy in detriment of website personalization;

The following list summarizes a list of technical **recommendations** that could be adopted in order to mitigate the major issues discussed above:

1) **Transparent and specific cookie consent over cookie information flow:** simply asking for user consent to authorize a website to use of cookies is not enough, users should be alerted about the specific **reason or purpose** for setting each cookie (e.g., persistent login, shopping basket, etc.) and **who can read and write these cookies**, including possible third parties and also the **specific reason or purpose for the information flow**. Instead of alerting the user saying "we use cookies to improve the service" the website should say: "we set one cookie X in order to remember the items you added to your shopping cart", or "to remember the order and items you have browsed in our website and to make suggestions for you", or "this cookie is set to be read by third parties XYZ in order to display advertisements to you", etc;
2) **Users should also be given the chance to oppose/control or to opt-out from specific cookies:** when cookies are read and content is displayed to users it should be clear the source of the adaptation or personalized information, for example, "the user is seeing this ad because website XYZ says he is interested in car parts, mobile devices, baby items, sport equipment, etc." Furthermore, users should also be allowed to opt out from their consent. Plugins mechanisms should be also provided by websites or a standard add-on to web browsers to allow user control over the cookies, and different levels of control considering the expertise of the users. Mechanisms for consent from the user should be transparent and selective, in the sense that the user should be allowed to know which data are going to be collected and why, and selectively choose if granting this collection or not. The mechanism should be similar to the new permission control implemented in Android 6. Of course, in order to make the browsing not too difficult and continuously interrupted by the consent mechanism, it should be possible to define profiles to apply to all the websites by default but still with the possibility to tune them for every single website;
3) **Explicit information regarding 3rd party cookies/data:** when accessing a website all 3rd party communication should be blocked by default, and only allowed if users explicitly opt-in for it. Furthermore, a control mechanism should be in place to automatically whitelist the allowed 3rd party communication, in a way that users can be easily made aware of it. For example, when accessing a

website, users should be informed about all 3rd parties providing content, storing cookies, etc;

4) **Trust on browser extensions and solutions:** many solutions exist to improve the user privacy and to avoid tracking, cookies, etc. One major issue for users is how to trust these solutions, and to be sure that they are not in fact tracking users even more or that malware software is embedded in benign solutions to empower and protect end users. For this reason, those extensions should be certified or integrated as default functionalities of the browsers, easily accessible by users rather than hidden in the settings.
5) **Easier management of cookies stored by every website:** in some of the most popular browsers, it is not so easy for a user to find where the list of the stored cookies is. Facilitating those things, would increase user's awareness and active participation in privacy settings, rather than always trust in default configurations or previously given consents that would never be revised.

5.2 Redirection to Unencrypted Content

In some cases, users access a secure/encrypted web app (HTTPS) and some of the content or links displayed may redirect the user to unsecure/unencrypted websites (HTTP). Users may unnoticeably access these unsecure links and change from secure to unsecure. This problem has been addressed by the HTTPS everywhere [95] browser extension, which is available for Firefox for desktop/Android, and Opera. This extension automatically replaces all unsecure links in a secure website to secure versions, which may solve the problem. However, some websites may not offer all the unsecure content over a secure version as well, which may result in broken links/content. Cookies that are transmitted over insecure connections may also be leaked in case the user connection is monitored. From this perspective a technical **recommendation** should be for users to always use secure/encrypted connections in order to prevent possible tracking risks and to have web browsers to enforce the same behaviour as the HTTPS everywhere extension by default.

5.3 Private Browsing Modes

All top used web browsers[96] include a private/incognito browsing mode where some measures are taken to prevent tracking of the user web activities. For example, in the Chrome browser the incognito mode will not save the user browsing history, and will not transmit any saved cookies to the web apps accessed by the user. All cookies created during incognito mode are only available during the incognito mode session and are immediately deleted as soon as the user closes the session.

The Tor project also provides a web browser that in addition to a private browsing mode also allows direct access to the Tor relay network without the need to install any client software. By using the Tor browser users are protected against network layer tracking from their Internet Service Provider (ISP) and Web Application Providers (WAP), meaning that the ISP is not able to identify the web applications accessed by the user and WAPs are not able to distinguish multiple visits of a user to their web apps simply by looking at their source IP address. Every visit by the users will appear to be originating from a different IP address.

JonDonym[97] is a solution for anonymous and secure web browsing, and it is available for Windows, MacOS, and for Linux/BSD. JonDonym establishes an encrypted connection between the user's web browser and anonymization servers. An anonymization server is

[95] https://www.eff.org/https-everywhere
[96] The top 98% used web browsers are: Internet Explorer, Firefox, Chrome, Safari, Opera, and Android Browser [17]
[97] https://anonymous-proxy-servers.net/en/jondofox.html

called in the JonDonym terminology a Mix, and works in a different way than Tor or I2P[98] since a Mix operator must be certified.

Private browsing is a useful feature to enable privacy protection among users that share a computer but it **is not a solution to mitigate user tracking and privacy** since it is unfeasible from a usability perspective for users to use private browsing all the time considering the reduction in the usability, for example, multiple login requests for commonly used web apps and impossibility to remember previous activity/sessions. However, for occasional use, private browsing significantly improves the privacy protection of users in the specific browsing session.

5.4 Reputation and Certification of Websites

In many cases users are unaware about a website reputation when browsing and allowing the collection of their data. The Web Of Trust (WOT)[99] is a web browser add-on that allows users to rate and get recommendations about websites. Figure 18 shows the results for the same news website we analysed previously, observe that it is rated as a good site, even though the Lightbeam solution shows that many trackers are actually used. Social network websites are rated as an **online tracking** websites, but it can be doubtful whether the news website is also tracking their users in the same way Facebook does since users are not informed about the tracking performed in the background.

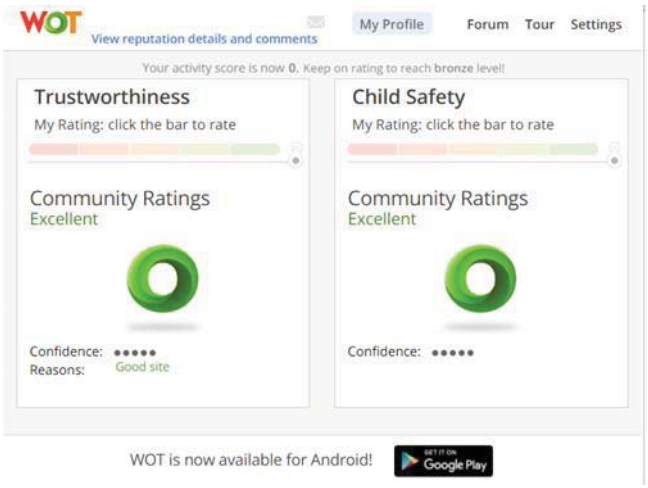


Figure 18 – WOT plugin results for the a news website

5.5 Tracking User Location using IP Addresses

IP addresses can be used to infer information about the geographical position of the user. This can allow (a raw) tracking and proposal of commercial offers based on geographical information, leading to discriminatory conducts. Cases were reported and discussed in [18]. A web-based tool called IP Leak[100] showing information about your specific IP address shows also the precise source network of the machine accessing the page.

Location tracking is the indirect determination of the user geographical location based on the web-browser language, IP address, or user provided information (e.g, geolocation tags in web posts). The location information can reveal not only where the user is at the moment and their moving history, but the combined analysis of geolocation data of a

[98] Invisible Internet Project (I2P) is an overlay network that allows applications to send messages to each other pseudonymously and securely.
[99] https://www.mywot.com
[100] https://ipleak.net/

user could reveal privacy sensitive information including the users home and workplace, as recently shown by [19].

Location tracking can only be prevented by network-layer IP anonymization techniques, or by users explicitly preventing web apps from receiving location information about them. The simple tracking of user activity could also reveal their time zone and possibly details about their location as well, since users have clear patterns of activity during the day and night time, for example, late night activity in general is less likely.

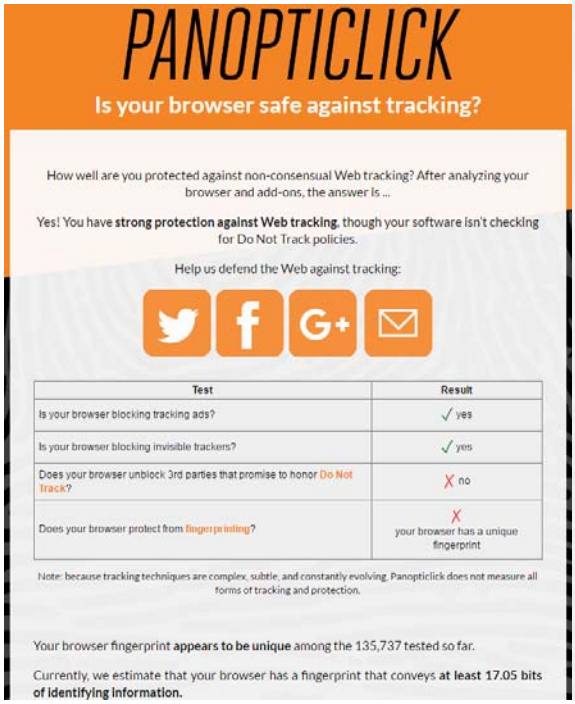
5.6 Software/Browser Metadata Fingerprinting

The user web browser, when accessing a web app, provides by default many detailed information to the server about the client-side configuration, for example, using the HTTP header string *User-Agent*, the supported language, the list of system fonts, the platform, the screen size, the time zone, etc. For example, the information encoded in the User-Agent string reveals the web browser and version like "*Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36*". By analysing all this information it has been shown that users can be uniquely identified since very few users share the same exact set of configurations.

Panopticlick [101] is an online tool that illustrates browser metadata fingerprinting capabilities and shows all the detailed metadata that is available about the web browser and maintains a database showing how unique this configuration is. A sample analysis provided by this tool is displayed in Figure 19 on the left side, while the right side shows detailed web browser metadata that in this case uniquely identifies the browser among around 130 thousand web browsers tested. Furthermore, it also tests the resilience of the web browser against tracking ads and provides a web browser plug-in Privacy Badger[102] to protect users from four tracking approaches used, namely: tracking ads, invisible trackers, unblock 3rd parties that promise Do Not Track, and metadata fingerprinting.

[101] https://panopticlick.eff.org

[102] https://www.eff.org/privacybadger



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.48	1.39	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	7.17	144.25	a8bbc4155e16ca433555bb2f381a6dda
Screen Size and Color Depth	2.41	5.31	1920x1080x24
Browser Plugin Details	2.07	4.19	undefined
Time Zone	1.84	3.57	-120
DNT Header Enabled?	1.05	2.07	False
HTTP_ACCEPT Headers	3.14	8.84	text/html, */*; q=0.01 gzip, deflate en-US,en;q=0.8
Hash of WebGL fingerprint	8.35	327.08	a314cf83e99bebc15def2c24dd2c8d48
Language	1.02	2.03	en-US
System Fonts	5.82	56.56	Arial, Arial Black, Arial Narrow, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	1.25	2.37	Win32
User Agent	6.77	108.85	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36
Touch Support	0.51	1.42	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.25	1.19	Yes

Figure 19 – Web-browser tracking and metadata analysis

5.7 Device Hardware Fingerprinting

Browser fingerprinting is based on characteristics and settings of a software component. However, mobile devices embed several hardware components that present unique characteristics, so that it is possible to extract from them hardware fingerprints, which allow distinguishing a device from another, even of the same model. Those built-in components are typically the digital camera, radiofrequency transceivers, microelectromechanical sensors (MEMS) like accelerometers and gyroscopes, microphone and speaker, and clock.

This means that the analysis of the output of these sensors (i.e. a picture, a radio transmission, the acceleration measured for a certain position/movement, a recorded audio or the clock skew) can lead to the identification of a unique pattern (fingerprint) that can be used to identify a particular sensor and then the device that contains it. The way to extract these fingerprints in order to classify and identify the device are basically two:

- the output of the component is captured outside the device, without the need to install any software or hardware component on it (e.g., a radiofrequency emission is recorded by an external receiver and then processed in order to extract the fingerprint);
- the output of the component is captured on the device by an application (or a malware) that gains access to the component. Here the extraction of the fingerprint can be done on the device or by an external system that receives the data read by the application.

Evidences of the (unique) noise introduced by digital video cameras in the tapes were already discussed and published in 1999 [20] while more recent studies on smartphone identification based on photo camera pictures are published for example in [21] and

[22]. For what concerns MEMS, microphones and speakers, evidences are published in [23] and [24]. At the JRC, we conducted a successful experiment on smartphone accelerometers and gyroscopes fingerprints in [25], and also on radiofrequency and camera identification.

From a technical perspective hardware fingerprinting is very difficult to avoid, since it considers intrinsic features of the device that cannot be easily changed or masqueraded. Therefore, from a regulatory perspective a possible **recommendation** is to legally prevent companies from collecting, storing, and using this type of information about the devices unless the information is anonymized and the chances of distinguishing one device from another are statistically equivalent to blindly guessing.

5.8 Locally and Remotely Saved Web Browser User Data

A potential privacy risk for users is the information saved about them by the web browser in the disk/memory of their device, which may also be synchronized with a remote cloud server if the user creates an account and agrees to do so. For example, the Chrome web browser saves:

- Browsing history information containing all the URLs of pages the user has visited, cache files of all text and images, list of some IP addresses linked to the visited pages;
- A searchable index of all pages visited by the users optimized for quick search, excluding pages visited using HTTPs;
- Thumbnail-sized screenshots of most pages you visit;
- Cookies or web storage data deposited on your system by websites you visit;
- Locally-stored data saved by add-ons;
- A record of downloads you have made from websites;
- List of active user tabs;
- Passwords and auto complete form data including credit card information, mobile phone numbers, e-mails, etc.

The storage of this information by the web browser locally or remotely implies a huge risk for users since any security vulnerability in the local machine or in the remove cloud server could imply a complete exposure of all web apps and data. Therefore, from a technical perspective this information should always be stored remotely in an encrypted format with the encryption keys being only available to the end-user.

5.9 Data Leaks due to breaches in server's or client's policy settings

Some private information, especially in social networks, can be indirectly or unintentionally disclosed due to privacy insensitive policy settings. An example of personal information that got outed on Facebook was reported in [26]. In this case, some information about joining a discussing group of a specific sexual preference was disclosed, thus revealing a private information to users that were not supposed to know about it.

More in general, wrong or not up to date security and privacy settings both in client and server systems can lead to unauthorized access and theft of private data and sensitive information. According to Gartner 75% percent of the mobile security breaches depend on application misconfigurations [27]. OWASP, apart from the top ten web application security flaws proposes a set of **recommendations** that constitute a good guideline and helping tool for safe web applications development and systems configuration [28].

The Platform for Privacy Preferences Project (P3P) is a language and protocol to support users and web app providers in the exchange of user privacy preferences and website privacy policies. The specification of user privacy preferences is done using the P3P policy language, while the web app providers specify their internal privacy policies using the Enterprise Privacy Authorization Language (EPAL) language. A web browser add-on

is used to verify if the EPAL policy provided by the web application matches the P3P requirements specified by the end users. In case there is a match and users believe the web app provider is following their privacy requirements the user data is automatically provided [29]. The P3P and EPAL languages have been criticized for their complexity and lack of precise semantics since many of the policy assertions were strings open to interpretation.

Users should be always in control of the information released about them by the web app to other users and should be made aware by the specific web app provider about the possible privacy implications of using the app. This could be implemented as a **user-centric risk analysis** requirement for all web apps that handle potentially sensitive user information. A concrete approach could include for each web app a list of the collected information, where the information is stored, what is the purpose of the collection, a list of potential negative consequences for users if the information is leaked in a data breach, and a plan of action for users in case a data breach occurs in the future. Users are then more informed to decide if they would like to provide the information or not considering the possible negative consequences.

5.10 Information Leakage to Third party components

In order to provide their services/functionalities, some web applications run third party components and applications that get access to user's personal data. This is the case, for example, of some Facebook's third-party apps (online games) reported in [30], which were able to retrieve the Facebook user ID (useful to identify the user along with some private information) and send it to tracking and ad companies.

Some frameworks and architectures mostly based on information flow control have been proposed in literature. The *Logical attestation* framework [31] (implemented in an operating system called Nexus) allows to specify security policies that all the server-side components have to follow. *Hails* [32] is a framework designed to build web applications where untrusted components are used.

The studies mentioned above represent a good example on how to protect from the leakage of information to third parties. However, our **recommendation**, as already suggested in section 5.1, is that communications with third partied should initially be blocked by default and, according to the sensitiveness of the information requested, the user, properly informed, can choose if accessing the external service and release this information or not. Moreover, the use of certain information should be justified (e.g., an online game might not really need a strong identifier like the Facebook user ID).

5.11 Data Mining and Correlation

The collection of user's data done using the different tools and techniques mentioned in the previous subsections (e.g., ad trackers, cookies, etc.) produces a huge amount of information. In order to make use of them, mainly for commercial purposes, companies apply data mining techniques to discover useful or hidden patterns and to predict user's behaviour. The use of these tools, which is actually the data processing part, can allow to infer sensitive information even from data that apparently do not contain any private fact, especially when those are correlated. The purpose of this section then, is to show how powerful these tools are, putting the accent on the importance of limiting the collection of data that can lead to privacy invasions.

Actually, there are companies like for instance the ones cited in [33], which are specialized on data mining for digital marketing and provide third party services for analysing those data. Data mining for e-commerce mainly targets the following two points:

- Customer profiling: based on the purchases done, e-commerce platforms try to predict the future needs of the customer and propose targeted offers;

- Customer behaviour analysis; to make the e-commerce platform more usable and then successful, users' path traversals are analysed in order to predict future traversal and load the appropriated content in advance, resulting in faster browsing;

The result of these activities is a personalization of the platform for each customer and a recommendation system that targets individual needs and preferences. Although most of this information could be processed in an anonymized form, threats for user's privacy come when information are intentionally or unintentionally linked to real identities instead of being just a summary of habits or statistics. For example, the correlation of information coming from different sources, allows to progressively reduce the set of possibilities and, potentially, to infer the identity of a real person (e.g., gender, age, zip code, owned car and so on). On the other side, some of the companies specialized on these activities, have been criticized about intentional link of information and persons [34], leading to individual dossiers containing any kind of personal information ready to be sold to other companies or individuals interested in it.

A study published in [35] showed that using some data mining techniques it was even possible to differentiate users with the same usernames (alias-disambiguation) across different online platforms in more than 46% of the cases. This means that the correlation between user's data left in various platforms can allow distinguishing different identities even if the same alias was used. Consequently, the use of pseudonyms is not always effective to protect against advanced data mining.

Correlation and link to real identities becomes easier or automatic when collection of data and tracking are done using a platform in which identities are unequivocally established. For example, Facebook in 2012 bought the data mining company Datalogix [36], which tries to associate data coming from shopping loyalty cards to Facebook users in order to establish if a certain product was purchased after it's advertisement on a Facebook page. The association is made quite easy and almost error free thanks to the decision of Facebook to allow advertisers to match email addresses and phone numbers collected by them with Facebook profile's data [37]. Similarly, Twitter started a partnership with the WPP company to allow the analysis of Twitter data for better real time consumers behaviour monitoring [38].

The most dangerous and invasive behaviour related to data mining activities is the link to real identities, which allows to say exactly what a certain person has done, bought and expressed in a certain period of time. This practice goes behind a simple market analysis, especially if it results in individual dossiers which are themselves put in the market. Our **recommendation** in this case is to forbid this kind of link and associations and to only allow analysis of anonymized and obfuscated data.

6 Conclusion

All the cases analysed so far show that the major concern when speaking of privacy of telecommunication/online services is related to the lack of free will give to the users with regards to their sensitive information.

If we take as an example the cookies, we can undoubtedly claim that the previous implementation of the ePrivacy directive failed in promoting transparency and privacy awareness in digital services. The disclaimer users have to review and accept every time they visit a web-site or use a web-service, is an uninformative *take-all or nothing* text which (1) doesn't give any real choice to the end-user and (2) doesn't provide any effective information about the type and the use of information that is gathered. In practical means, a good informative initiative has been transformed into a useless and cumbersome additional clicking step without any real benefit for the end-user.

Hence, the identification of a new, efficient, and effective way to give back the control of personal information to the end-user is needed, and the review of the ePrivacy directive is the best occasion to elaborate on this challenge.

The problem is in a way not trivial due to the fact that even if formally the concept of privacy has a clear definition, in practice, it is completely subjective, linked to the cultural background, to the moment in time when we're accessing a service, to the mood, the place and many other variables. For example, is the ID on my phone sensitive information which shouldn't be disclosed? According to the general definition of privacy and to an opinion of article 29 working party every ID is sensitive information hence falling under privacy regulations. However, it is also true that some services, to be delivered, need this information perhaps as an easy way to identify the device from session to session but it is evident that a privacy friendlier option with pseudo-ids could be used instead to prevent tracking across different services. Is the position of the mobile phone a sensitive information? Again, the access to the GPS sensor could give to an application the possibility to track the movements of an end-user, infringing its privacy. On the other side, if the application is providing a navigation service, the GPS position becomes essential information needed to allow the delivery of the service that the end-user is expecting. It would be possible to make thousands of similar illustrative examples, just to demonstrate how the question of what can be shared without consent is indeed very subjective and related to the needs and feelings of the end-user.

Moreover, even with the adoption of very prescriptive and stringent measures forbidding the access to all possibly sensitive information of an individual, modern datamining and inference techniques can easily be used to infer from explicit, completely depersonalized information, implicit sensitive information, circumventing in this way every type of legislative limitation.

If we look to the roadmap of the Digital Single Market, it is evident that the digital privacy will have to coexist with the more and more pressing need of opening up the free flow of data in the DSM, to boost innovation and new economic opportunities.

However, the coexistence of these two needs (or principles) is not new as it has been already experienced in several countries where digital and e-government services have been already rolled-out. In these countries in general privacy and data-sharing where made possible thanks to three main pillars:

3) Digital identity
4) Trust in the services provided
5) Full knowledge about who is accessing which personal information for what reason

While “digital identity” falls out of the domain of the ePrivacy directive, the second and the third points (which are indeed strongly linked) could provide inspiration to identify a viable way to solve the “cookies and information gathering problem”.

The embryonic proposal would be that of introducing a legislative measure obliging the providers of online services to put at disposal of digital users of an online platform where it is clearly showed:

1) The type of information collected
2) The information stored so far
3) The network of organisations with which this information is shared
4) The identity of the persons/organisations accessing this information

The same platform should be able to give to the end-user the possibility to:

1) Revoke the permission to access to a certain type of data
2) Erase the information stored so far
3) Monitor the data flows related to his/her sensitive information between the service provider and other third parties, giving the possibility to revoke, if needed, the access of the information to these additional parties
4) Impose the degree of anonymity which should be applied to the information gathered before being shared with third parties

A similar approach, even if ensuring to end user a high control on his/her sensitive data, might not be economically viable to all the digital companies.

A complementary, less expensive approach could be the following:

1) The end-user is given the possibility to define locally on his/her digital device a set of “privacy profiles” stating which category of data can be shared with which category of digital service
2) When the user accesses a web-service, through an automated trust-negotiation, the web-service will obtain by the browser of the end-user a digital token containing the privacy profile settings previously defined
3) The content of this profile will have to be taken as the willing of the end-user and hence respected mandatorily by the web-service

This approach would be a huge advance with respect to the actual “cookie consent” mechanism, guaranteeing at the same time better Internet experience (everything can be automated, hence, no more need for clicks on consent forms), higher granularity and control by the citizen with a limited economic impact. A similar approach already exist in the IoT domain [39].

An additional element to be taken into consideration obviously is the fact that several digital companies have built a business on the access to users’ data. Therefore, a too stringent set of measures could impact on the development of new digital markets and services. For that reason, in the presented approach the concept of “data value” could also be inserted, where an end-user could be encouraged to share a bigger amount of information through a negotiation where, in change he can get some benefit (money, additional services etc.). The net effect of a similar additional initiative would be two-fold: on a side the citizen would increase his/her awareness on the value of his/her personal information, while on the other, it would be possible to finally boost the information market (as foreseen by the DSM), but on the basis of a fair and balanced approach, where each party (business and citizen) has something to offer and something to gain.

Technically speaking the scenario is feasible (JRC already developed something similar for what concerns IoT devices), and could be easily extended to web-services, mobile applications etc.

From a legislative perspective it would be needed to clearly put down the definition of the previously mentioned principles (revocation, monitoring, access to data, anonymity

etc.), and the definition of the measures which the data controller should adopt to allow the end-user to be informed and evaluate the disclosure options at his disposal.

Additional inspiration can be taken by the W3C best practices for web application published in 2012[40]. They are based on 13 principles:

1) Follow "Privacy By Design" principles.
2) Enable the user to make informed decisions about sharing their personal information with a service.
3) Enable the user to make decisions at the appropriate time with the correct contextual information.
4) When learning user privacy decisions and providing defaults, allow the user to easily view and change their previous decisions.
5) Focus on usability and avoid needless prompting.
6) Active consent should be freely given, for specific data, and be informed.
7) Be clear and transparent to users regarding potential privacy concerns.
8) Be clear as to whether information is needed on a one-time basis or if it is necessary for a period of time and for how long.
9) Request the minimum number of data items at the minimum level of detail needed to provide a service.
10) Retain the minimum amount of data at the minimum level of detail for the minimum amount of time needed. Consider potential misuses of retained data and possible countermeasures.
11) Maintain the confidentiality of user data in transmission, for example using HTTPS for transport rather than HTTP.
12) Maintain the confidentiality of user data in storage.
13) Control and log access to data.

Although in some cases these are mainly general recommendations, there are important references to the specificity of the consent (best practice 6) and the minimum set of data to be disclosed (best practices 9 and 10). These best practices are already followed by many of the tools described in this document and are in line with the **recommendations** introduced throughout this document.

Finally, for what concerns mobile platforms and applications, stakeholders can have a key role in “guiding” software and service development towards a privacy-preserving approach. The example is given again by the last version of Android, which significantly improved the permission mechanism. In the same way, the granularity of the permissions can be increased (thus avoiding that unnecessary permissions are granted only because they depend/are linked to others) and the use of sensitive functionalities could be reserved only to certain kind of applications or even developers. This would create a sort of categories/levels of application, giving to users a more a clear perception on the potential risks. Moreover, a labelling/certification scheme could help in identifying sources/developers according to their privacy friendliness and compliance to privacy principles. The user would be more aware that untrusted or unknown sources could hide more risks. More in general, the role of stakeholders would be fundamental to enforce some privacy rules at the OS and browser level.

From a legislative point of view, what already proposed in section 4.3 can easily find application in the mobile application domain. However, here, since the ePrivacy directive addresses also the aspects related to the “security of terminal devices”, the prescriptiveness should be broader.

Differently from the old “terminal devices”, smart-phones are in continuous evolution and much more open to external interactions. Newly discovered vulnerabilities might put in serious danger the security of the terminal device. The directive should address this issue, introducing the principle of mandatory and timely application of patches when a

cyber-security issue is discovered. Looking at the Android phone market, with the exception of brand flagships, the OS support life of a smart-phone is very limited, in several cases the smart-phones never receive the update to the following release of OS. Especially when a vulnerability involves kernel level or low level library issues, this is an extreme weakness, leaving exposed to cyber-attacks millions of devices in the world (as it happened for example last year for the vulnerability discovered in Stagefright, leaving for months over 1 billion of Android devices exposed to cyber-threats) [41].

A revision of the ePrivacy directive should take this aspect into consideration, by asking to OS developers, smart-phone producers and telecom operators, to ensure the availability of cyber-security patches for all the life time of all the released smart-phone.

The timeliness release of these patches is also a key point that the revision should take into consideration. In fact in several cases, it happened in the past that some producers released a patch for some low-level models even one year after its discovery, leaving the end-user exposed to privacy leakages and security risks for all that time.

Here, incentives to facilitate also proactive vulnerability information sharing and cooperation among the sector operators could be seen as a set of accompanying measures to the ePrivacy directive revision.

References

[1] "2015 Mobile Threat Report | Pulse Secure Mobile Threat Center." [Online]. Available: https://www.pulsesecure.net/lp/mobile-threat-report-2014/. [Accessed: 25-Jul-2016].

[2] "IDC: Smartphone OS Market Share," *www.idc.com*. [Online]. Available: http://www.idc.com/prodserv/smartphone-os-market-share.jsp. [Accessed: 25-Jul-2016].

[3] "Mobile malware evolution 2015 - Securelist." [Online]. Available: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/. [Accessed: 25-Jul-2016].

[4] "OWASP Mobile Security Project - OWASP." [Online]. Available: https://www.owasp.org/index.php/Mobile#tab=Top_10_Mobile_Risks. [Accessed: 25-Jul-2016].

[5] G. McGraw, *Software security: building security in*. Upper Saddle River, NJ: Addison-Wesley, 2006.

[6] "Android and Security - Official Google Mobile Blog." .

[7] "Report: Malware-infected Android apps spike in the Google Play store," *PCWorld*, 19-Feb-2014. [Online]. Available: http://www.pcworld.com/article/2099421/report-malwareinfected-android-apps-spike-in-the-google-play-store.html. [Accessed: 22-Jul-2016].

[8] "<permission> | Android Developers." [Online]. Available: https://developer.android.com/guide/topics/manifest/permission-element.html. [Accessed: 22-Jul-2016].

[9] "Working with System Permissions | Android Developers." [Online]. Available: https://developer.android.com/training/permissions/index.html. [Accessed: 22-Jul-2016].

[10] Apple, "iOS Security (iOS 9.3 or later)." [Online]. Available: https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[11] I. Nai Fovino, R. Neisse, D. Geneiatakis, and I. Kounelis, "Mobile Applications Privacy, Towards a methodology to identify over-privileged applications," Publications Office of the European Union, EUR - Scientific and Technical Research Reports, 2014.

[12] D. Geneiatakis, R. Satta, I. N. Fovino, and R. Neisse, "On the Efficacy of Static Features to Detect Malicious Applications in Android," in *Trust, Privacy and Security in Digital Business*, S. Fischer-Hübner, C. Lambrinoudakis, and J. López, Eds. Springer International Publishing, 2015, pp. 87–98.

[13] D. Geneiatakis, I. N. Fovino, I. Kounelis, and P. Stirparo, "A Permission Verification Approach for Android Mobile Applications," *Comput. Secur.*, Nov. 2014.

[14] "Do Not Track," *Do Not Track*. [Online]. Available: https://donottrack-doc.com/en/. [Accessed: 31-Oct-2016].

[15] "A privacy-friendly Do Not Track (DNT) Policy," *Electronic Frontier Foundation*, 24-Apr-2014. [Online]. Available: https://www.eff.org/dnt-policy. [Accessed: 25-Jul-2016].

[16] "Tracking Preference Expression (DNT)." [Online]. Available: https://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html. [Accessed: 25-Jul-2016].

[17] “Browser Statistics.” [Online]. Available: http://www.w3schools.com/browsers/browsers_stats.asp. [Accessed: 25-Jul-2016].

[18] J. Valentino-DeVries, J. Singer-Vine, and A. Soltani, “Websites Vary Prices, Deals Based on Users’ Information,” *Wall Street Journal*, 24-Dec-2012.

[19] “We know where you live,” *MIT News*. [Online]. Available: http://news.mit.edu/2016/twitter-location-data-homes-workplaces-0517. [Accessed: 25-Jul-2016].

[20] K. Kurosawa, K. Kuroki, and N. Saitoh, “CCD fingerprint method-identification of a video camera from videotaped images,” in *1999 International Conference on Image Processing, 1999. ICIP 99. Proceedings*, 1999, vol. 3, pp. 537–540 vol.3.

[21] Q. Liu *et al.*, “Identification of Smartphone-Image Source and Manipulation,” in *Advanced Research in Applied Artificial Intelligence*, H. Jiang, W. Ding, M. Ali, and X. Wu, Eds. Springer Berlin Heidelberg, 2012, pp. 262–271.

[22] R. Satta and P. Stirparo, “Picture-to-Identity linking of social network accounts based on Sensor Pattern Noise,” presented at the 5th International Conference on Imaging for Crime Detection and Prevention (ICDP 2013), London, UK, 2013.

[23] H. Bojinov, D. Boneh, Y. Michalevsky, and G. Nakibly, “Mobile Device Identification via Sensor Fingerprinting,” 2014.

[24] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, “AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable,” 2014.

[25] G. Baldini, G. Steri, F. Dimc, R. Giuliani, and R. Kamnik, “Experimental Identification of Smartphones Using Fingerprints of Built-In Micro-Electro Mechanical Systems (MEMS),” *Sensors*, vol. 16, no. 6, p. 818, Jun. 2016.

[26] G. A. Fowler, “When the Most Personal Secrets Get Outed on Facebook,” *Wall Street Journal*, 13-Oct-2012.

[27] “Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration.” [Online]. Available: http://www.gartner.com/newsroom/id/2753017. [Accessed: 25-Jul-2016].

[28] “OWASP Product Requirement Recommendations Library - OWASP.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Product_Requirement_Recommendations_Library. [Accessed: 25-Jul-2016].

[29] W. H. Stufflebeam, A. I. Antón, Q. He, and N. Jain, “Specifying Privacy Policies with P3P and EPAL: Lessons Learned,” in *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*, New York, NY, USA, 2004, pp. 35–35.

[30] E. S. A. G. A. Fowler, “Facebook in Privacy Breach,” *Wall Street Journal*, 18-Oct-2010.

[31] E. G. Sirer *et al.*, “Logical Attestation: An Authorization Architecture for Trustworthy Computing,” in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, New York, NY, USA, 2011, pp. 249–264.

[32] D. B. Giffin *et al.*, “Hails: Protecting Data Privacy in Untrusted Web Applications,” in *Proceedings of the 10th USENIX Conference on Operating Systems Design and Implementation*, Berkeley, CA, USA, 2012, pp. 47–60.

[33] J. Stein, “Data Mining: How Companies Now Know Everything About You,” *Time*, 10-Mar-2011.

[34] “The Data Brokers: Selling your personal information.” [Online]. Available: http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/. [Accessed: 25-Jul-2016].

[35] J. Liu, F. Zhang, X. Song, Y.-I. Song, C.-Y. Lin, and H.-W. Hon, “What’s in a Name?: An Unsupervised Approach to Link Users Across Communities,” in *Proceedings of the Sixth ACM International Conference on Web Search and Data Mining*, New York, NY, USA, 2013, pp. 495–504.

[36] T. Wasserman, “Facebook Now Tracks Consumers’ Retail Purchases,” *Mashable*. [Online]. Available: http://mashable.com/2012/09/24/facebook-tracking-retail-purchases/. [Accessed: 25-Jul-2016].

[37] “In Pursuit of Revenue, Social Networks Ramp Up Ad Targeting.” [Online]. Available: http://adage.com/article/digital/pursuit-revenue-social-networks-ramp-ad-targeting/237096/. [Accessed: 25-Jul-2016].

[38] “Twitter and WPP announce global strategic partnership - WPP.” [Online]. Available: http://www.wpp.com/wpp/press/2013/jun/06/twitter-and-wpp-announce-global-strategic-partnership/. [Accessed: 25-Jul-2016].

[39] “SecKit: A Model-based Security Toolkit for the Internet of Things.” [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815000887. [Accessed: 05-Aug-2016].

[40] “Web Application Privacy Best Practices.” [Online]. Available: https://www.w3.org/TR/app-privacy-bp/. [Accessed: 25-Jul-2016].

[41] “The ‘Stagefright’ exploit: What you need to know,” *Android Central*, 17-Aug-2015. [Online]. Available: http://www.androidcentral.com/stagefright. [Accessed: 05-Aug-2016].

[42] “What is a Mashup? - Definition from Techopedia,” *Techopedia.com*. [Online]. Available: https://www.techopedia.com/definition/5373/mashup. [Accessed: 07-Jul-2016].

[43] “Virtual machine,” *Wikipedia, the free encyclopedia*. 21-Jul-2016.

[44] “Web application,” *Wikipedia*. 17-Oct-2016.

APPENDIX A. LIST OF DEFINITIONS

Invisible Internet Project (I2P). An overlay network that allows applications to send messages to each other pseudonymously and securely.

IoT Hub. A hub where IoT devices connect and through which they exchange information and/or connect to the Internet.

Mashups of Web Apps. A mashup is a technique by which a website or Web application uses data, presentation or functionality from two or more sources to create a new service. [42]

Mobile Applications. Application running on a mobile device, such as a smart phone or a tablet.

Pre-installed applications. Applications that are already installed on the device when the user operates it for the first time.

Terminal device. Any computer device of the end user including mobile phones, laptop, and desktop computers used to access websites or services.

User Applications. User applications refer to applications that are installed on the users' device either mobile or desktop computer.

Virtualization Infrastructure. Emulation of a given computer system based on the computer architecture and functions of a real or hypothetical computer, and their implementation may involve specialized hardware, software, or a combination of both. [43]

Webpage. A HTML interface displayed in the client web browsers that may include links or embed web applications. A webpage may also display content using other technologies such as Javascript, Scable Vector Grap*hic*s (SVG), PHP, etc.

Web Application. A client-server application where the client runs in a web browser [44].

Website. A domain accessible through a HTTP protocol (e.g., www.google.com) that hosts a set of webpages and web applications.

Web browser add-ons. Program utilities that extend the capabilities of a browser.

Web browser plugins. See Web browser add-ons.

Web trackers. Online platforms dedicated to collect user browsing information for advertisement purposes including all the visited websites, duration of the visit, outgoing visited links, and origin/source of link.

APPENDIX B. LIST OF ABBREVIATIONS

AFP – Adobe Flash Player
API – Application Programming Interfaces
ART – Android Runtime
ASLR – Address Space Layout Randomization
CA – Certificate Authority
DMA – Direct Memory Access
DNT – Do Not Track
DSM – Digital Single Market
DVM – Dalvik Virtual Machine
EPAL – Enterprise Privacy Authorization Language
GPS – Global Positioning System
HTTP – Hypertext Transfer Protocol
I2P – Invisible Internet Project
ID – Identity Document
IMEI – International Mobile Station Equipment Identity
IoT – Internet of Things
IP – Internet Protocol
IPC – Inter Process Communication
ISP – Internet Service Provider
LLB – Low-level Bootloader
MEMS – MicroelEctroMechanical Sensors
MMS – Multimedia Messaging Service
MS – Microsoft
OEM – Original Equipment Manufacturers
OS – Operating System
OWASP – Open Web Application Security Project
P3P – Privacy Preferences Project
PDF – Portable Document Format
PHP – PHP: Hypertext Preprocessor
PIE – Position Independent Executable
PUA – Potentially Unwanted Applications
ROM – Read Only Memory
SD – Secure Digital
SDK – Software Development Kit
SIM – Subscriber Identity Module
SMS – Short Message Service
SVG – Scalable Vector Graphics
TEE – Trusted Execution Environment
UAC – User Account Control
UID – Unique Identifier
VOIP – Voice Over IP
WAP – Web Application Provider
WOT – Web Of Trust

LIST OF FIGURES

LIST OF TABLES

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

ANNEX 7: WHO IS AFFECTED BY THE INITIATIVE AND HOW

This annex describes the practical implications of the preferred option identified in the Impact Assessment for the Review of the ePrivacy Directive (ePD) for representative groups likely to be directly or indirectly affected by the legislation including electronic communication service providers, Over-the-Top players, SMEs, national authorities and consumers. Moreover, it includes a specific section on SMEs ("SMEs Test") and a section on impact on international trade.

For each stakeholder group, the relevant impacts of the preferred option, the key obligations that will need to be fulfilled and when these might need to be fulfilled in order to comply with obligations under the revised ePrivacy rules will be discussed. Wherever possible, potential costs that may be incurred in meeting those obligations will be indicated.

1. Impact on categories of stakeholders

- **Citizens** (both individuals and legal persons) will benefit from this option in terms of more effective, consistent and efficient privacy protection. The extension of the scope by legislative change to OTT entities providing communications, to publicly available private networks (WiFi) and to IoT devices would fill considerable gaps or uncertainty related to the scope of the current ePD. Citizens will hold equivalent rights for equivalent services, which is not the case today.

  Since the new provisions will be value-based, rather than tehcnology-based, the citizens' protection would be less likely to become unfit for purpose in light of future technological developments.

  By mandating specific software providers to set-up privacy friendly settings to reinforce user's control, this option would greatly simplify the management of their privacy preferences and allow citizens to set their preferences in a centralised way. This is expected to reduce the problems caused by cookie banners and the related cookie-consent fatigue.

  The introduction of a special prefix and the consequent banning of unsolicited calls by anonymous numbers, together with the extention of the rigths to block calls, are expected to increase transparency and effective enforcement.

  Finally, by reinforcing and streamlining enforcement, including by providing for deterrent penalties, this option would ensure independence and significantly reinforce the powers of the national authorities, thus creating the conditions for a more effective and consistent enforcement.

- **Businesses:** the following main cateogories of undertakings would be affected by the new rules in the following way:

  - ✓ **ECS**: would benefit from the increased harmonisation and legal certainty stemming from the clarification of the scope and content of a number of provisions. Greater harmonisation and clarity would reduce their costs, especially when they operate in several Member States. ECS would benefit considerably from the level playing field. Competing services will be subject to the same rules, thus putting an end to the asymmetric regulation. Moreover, these entities will be able to use the additional flexibility introduced under this option and have the opportunity to engage in the data economy. The repeal of outdated or unnecessary

provisions will simplify the regulatory framework and ensure consistency with other pieces of legislation, such as the GDPR.

- ✓ **OTTs** will have to comply with the ePrivacy rules. They will face some additional compliance costs 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 will no longer be able to rely on all legal grounds for processing personal data under the GDPR and could process communication data only with the consent of the users. The same would apply to publicly available private Wi-Fi operators and IoT players engaging in forms of tracking previously not covered by the rules. OTTs 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, in proportion, particularly high for big/medium enterprises, which have consolidated experience in the application of privacy rules. Moreover, these changes would not substantially affect those OTTs 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 cost stemming from administrative burden) is expected to be fairly contained at least in relative terms.

  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. 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 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.

  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[103]; 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.

- ✓ As concerns the new rules relating to tracking, all **website operators** and **online advertisers** would face some additional costs stemming from the new obligations/restrictions. In particular, 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 statistical cookies. 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 indeed clarify that consent to 'third party cookies'/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 pre-set 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 cumbersome cookie messages. 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)[104], with more than 3.4 million websites potentially affected in 2030[105]. 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[106]. 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[107]). The magnitude of the total savings potentially stemming from exemption from consent is therefore significant.

---

[103] 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.

[104] Castro, D. and Mcquinn, A. (2014), *The Economic Costs of the European Union's Cookie Notification Policy*, ITIF, p. 5.

[105] 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.

[106] SMART 2016/0080, cited above.

[107] Article 29 Working Party, Opinion 04/2012 on *Cookie Consent Exemption*, WP 194.

While the impact on compliance costs is expected to be significantly positive, a large number of businesses would potentially incur opportunity costs to the extent that OBA tracking would become more difficult. From a rather extreme perspective, the "reject third party cookies"/do-not-track by default 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, a breakdown of the OBA / ad-network market might turn out to be less likely considering that:

First, OBA tracking solutions not relying on storing information on the users' devices are already existent and used; they are part of the toolboxes related to tracking and thereby to some extent available to customers using these toolbox solutions.

Second, 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[108].

- ✓ Additional costs would ensue for the limited number of **providers of browsers** 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, operating systems and app stores cannot 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[109]. On this basis, an overall moderate increase for browsers may be expected for all three solutions.

- ✓ **Direct marketers (for voice-to-voice telephony)** will have to review their business models and comply with the new rules on mandatory identification, e.g. via a prefix. This is expected to raise the costs of a marketing campaign (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.

[108] This assessment of opportunity costs is the result of SMART 2016/0080, cited above.
[109] Data for geographic Europe only, based on visitors of a sample of 3 million websites globally accessible on http://gs.statcounter.com/

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.[110]

The impact on **SMEs** of this option is on balance expected to be positive. SMEs would benefit from increased harmonisation and legal certainty which would reduce their costs, in particular costs for seeking legal advice when operating in several Member States. More concretely, SMEs would benefit from clearer rules, more streamlined and harmonised enforcement mechanisms across the Member States. Some of the SMEs that responded to the public consultation emphasized the positive impact of the harmonisation role.

Furthermore, the changes in browser settings and limited need for cookie banners would lead to reduction of the compliance costs with regard to the cookie consent requirement. Moreover, the broadening of the exceptions to the current consent rule would allow SMEs which are operating in the advertising business to benefit from these exceptions. SMEs in the ECS business will also benefit, as bigger companies, of exceptions to process communications data.

SMEs which are OTTs would be faced with new obligations due to the broadened scope of the ePrivacy rules and could thus face additional compliance costs, in particular in so far as they currently process communications data on legal bases other than consent. While these costs may impact competitiveness of smaller OTT players as well as newcomers, more generally, these costs may be offset by the benefits associated to simplification and clarifications, including with respect to website management, the increase of consumer trust in the digital economy, and from the greater harmonising effects of more consistent enforcement.

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 European Charter. 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 could potentially cause the same harm as one caused by a larger player. Fundamental rights, therefore, shall be respected by every operators and no fully-fledged derogation is therefore possible for micro-enterprises. However, see below for other measures envisaged in the SMEs test section.

- The costs for the **Commission** are low and essentially coinciding with the conduct of the legislative process. However, the Commission will not have to finance the WP29 body for the ePD rules. Costs for the Commission to oversee the functioning of the new instrument would not change significantly compared to the current situation.

- MS would have to bear the costs relating to the transposition of the legal instrument, if the new instrument is a directive. Should the new instrument be a regulation, implementation costs would be more limited. The consistency mechanism would entail additional costs for **MS** authorities. In particular, they would need to spend additional time and resources, including for cooperating and exchanging information among competent authorities (running cost). The main costs for competent authorities would relate to the changes needed to allocate competence of all the provisions of the proposed Regulation to DPAs (one-off cost) and the extension of the consistency

[110] SMART 2016/0080, cited above.

mechanism to aspects relating to the ePD (running cost). In this respect, Member States have followed very different approaches as regards the allocation of competence of the various provisions of the ePD. 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[111], including in addition to DPAs and NRAs e.g. consumer protection authorities. Therefore, the entailing costs will vary according to the extent to which these provisions are already under the responsibility of the DPA. The table included in **Annex 11** presents an overview of the situation in each Member State[112].

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)[113].

2. SME test

Consultation of SME stakeholders: A number of SMEs have responded to the public consultation. In total, 18 respondents to the public consultation qualified themselves as SMEs. These companies are active in various economic sectors, such as software, marketing and subscriber directory companies. As such they have normally put forward their views as stakeholders active in a particular area rather than as companies of a particular size. The main views gathered are summarised below:

- Some SMEs stressed that the GDPR is a better framework than the ePD and that at the moment, the level of protection depends on MS' implementation;

[111] 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.
[112] SMART 2016/0080, cited above.
[113] Commission Staff Working Paper on *Impact Assessment on the General Data Protection Regulation proposal*, 25.01.2012, SEC 2012(72), p 103.

- Some SMEs report difficulties in relation to compliance with the rules on cookies, which are covered by different rules at national level, making it difficult to operate websites in different countries.

- SMEs also identify differences in national interpretation and enforcement as a special problem.

- The costs for complying are considered by some as disproportionate, especially in light of the fragmented national landscape. The costs to check Robinson lists are reported as significant costs, together with technical and legal advice costs, lengthy and disproportionate litigation procedures for cookies and marketing rules. In relation to the cookie consent provision, some respondents reported quite significant costs (over EUR 200,000), while other considerably lower (EUR 1,000).

- Some respondents have expressed concerns regarding the excessive costs of compliance for SMEs and start-ups. They argue that large "fixed cost" of compliance should not become a barrier for new businesses.

- One SME points out that many SMEs are leading on privacy by design and are using this as a unique selling point.

Identification of affected businesses: As the ePD provisions have a different scope, it is possible to identify at least three categories of affected SMEs. ***First***, SMEs that are ECS providers are affected by all provisions concerning confidentiality of communications and related traffic data as well as the rules on calling line identification, automated call forwarding and directories of subscribers. According to Eurostat, around 44.7 thousand enterprises are active in this market, accounting for a share of 0.2% of all businesses active in the EU. Around 90% of these enterprises are micro-enterprises, 99% are SMEs. Overall, approx. one million citizens are employed in the telecommunications sector of which roughly 20% are active in SMEs.[114]

Second, all SMEs that use cookies or similar techniques are affected by the provisions concerning confidentiality of terminal equipment. These will be primarily all SMEs that have a website using cookies. The study supporting the impact assessment estimated that that – per year between 2016 and 2030 – around 3.7 million businesses will be affected by the ePD rules in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (3.3 million). Around 260,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with around 10,000 per year. Also, SMEs that have developed mobile apps interfering with the confidentiality of terminal equipment are also affected by these rules. It can be presumed that a very high proportion of these businesses are SMEs and mostly microenterprises.

Third, SMEs who engage in marketing campaigns are affected by the rules on unsolicited communications. Although only very limited quantitative information is available in relation to costs associated with the provisions on unsolicited communications, the external study supporting this impact assessment provided quantitative estimates – mostly based on a set of assumptions and expert judgment. In

[114] SMART 2016/0080, cited above.

general, the study assumed that compliance costs are incurred not by all businesses that provide for unsolicited communication but only by those that also have a website and use cookies because collecting the consent of users over the counter does not produce costs.[115] Therefore, the compliance costs associated with Art. 13 are only incurred by businesses that also incur costs in relation to Art. 5(3).

The preferred option will increase the number of businesses subject to the ePD provisions, as the scope of these provisions will be extended to OTTs. While no precise data are available, a more or less significant fraction of these businesses are indeed SMEs. With regard to the provisions on unsolicited communications, the preferred option would extend the applicability of the rules to marketing campaigns over OTT platforms. As regards businesses subject to the rules on confidentiality of terminal equipment, Option 3 has the potential of reducing the number of affected SMEs thanks to the introduction of centrally managed privacy settings. The study supporting the impact assessment estimated that under policy option 3 in the "browser solution" implementation scenario, per year, between 2016 and 2030, around 190,000 businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (170,000). In the "tracking company" and "publisher implementation" scenarios, figures would be respectively 740,000 (660,000 microenterprises) and 2.22 million (1.99 million microenterprises).

Measurement of the impact on SMEs: The impact on **SMEs** of the preferred option is to be expected to be positive on balance. SMEs would benefit from clearer rules and increased harmonisation. Furthermore, the changes in browser settings and limited need for cookie banners would lead to reduction of the compliance costs with regard to the cookie consent requirement. Moreover, the broadening of the exceptions to the current consent rule would allow SMEs which are operating in the advertising business to benefit from these exceptions. SMEs in the ECS business will also benefit from the exceptions to process communications data.

SMEs which are OTTs would be faced with new obligations due to the broadened scope of the ePrivacy rules and could thus face additional compliance costs, in particular in so far as they currently process communications data on legal bases other than consent. These would be, however, offset by the benefits associated to the increase of consumer trust in the digital economy and from greater harmonisation. SMEs active in the OBA are expected to face opportunity costs as a result of the extension of the confidentiality rules and the rules on browser settings. These costs may not be quantified, but some mitigating elements have been identified above on the basis of which such costs would be contained.

---

[115] The study submits that there are two reasons for which this can be reasonably assumed: (1) All businesses can, potentially, make use of unsolicited communications by electronic communication means– either in a B2B or B2C context. However, it is only those businesses that provide for a website that are actually able to collect users' consent, either by an opt-in or opt-out solution. Furthermore, such businesses are generally expected to make also use of cookies in order to understand better "who their customers are" with a view to providing targeted unsolicited communication by electronic communication means. (2) Businesses that provide for unsolicited communication by electronic communication means but do not make use of a website are not able to collect the consent of their customers – both from a B2B and B2C perspective. Therefore, such businesses are expected to simply provide for unsolicited communication – even though this may not necessarily be compliant with national law. In any event, though, the compliance costs incurred by such businesses (e.g. related to legal advice) are (1) expected to be insignificant in view of the overall amount of costs; and (2) even though businesses may have costs related to legal advice, they could still make use of unsolicited communication as the chances of being detected of non-compliance are close to zero.

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 study estimated savings in compliance cost by 70% compared to the baseline (equal to an average of around EUR 261 per company)[116]. Costs related to administrative burden would also decrease even if less substantially (by a 10%). Far from being a precise figure, this gives however a rough idea of what the magnitude of the impact on SMEs could be. On the basis of these qualitative arguments and the external study quantitative estimated, it is concluded that the impact on costs for SMEs of this option would essentially be moderately positive.

Assessment of alternative mechanisms and mitigating measures: 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 European Charter. 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 may potentially cause the same harm as one caused by a larger player. Fundamental rights, therefore, shall be respected by every operators and no fully-fledged derogation is therefore possible for micro-enterprises.

While the general protection of communications should be afforded irrespective of the size of the enterprise concerned, it is however possible to identify some mitigating measures with specific regard to micro-enterprises in relation to the entry into force of the new rules and the applicability of some specific obligations. In particular, the proposed instrument will take action to avoid rules to be too prescriptive or specific, thus giving ample margin of manoeuvre to small enterprises to choose the most efficient implementation. For example, the proposal would not prescribe specific means to request consent, does not contain specific prescriptions concerning the information obligations vis-à-vis users and supervisory authorities. All provisions are technology neutral and purpose, rather than technology, driven.

Generally speaking, the preferred option does not include provisions implying any significant costs deriving from administrative burden. A provision including specific security and a reporting obligation, i.e. the data breach notification obligation, would be removed. Moreover, the introduction of software enabled general privacy settings as a way to provide consent and the expansion of the exceptions to the cookie-consent rule would allow savings for all SMEs running a website. With regard to setting of administrative fines, the new instrument will take into account the economic size of the undertaking (worldwide consolidated turnover) as an element for setting the maximum value of an administrative fine. The new ePrivacy legal instrument will further encourage (in a recital) Member States and their supervisory authorities, to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

3. Impact on international trade

While the IA certainly does not constitute a legal assessment of the WTO compliance of regulatory measures, it is important to take account of the broad legal obligations

[116] SMART 2016/0080, cited above.

associated with trading regimes in the formulation of policy options. **Option 3** extends the scope of the ePD and, in particular of confidentiality rules, to OTTs, i.e. online services. These services are more or less frequently totally financed by means of OBA, rather than direct payments, as they are normally provided free of charge. In this respect, the extension of the confidentiality and other ePD rules to these services may be considered as a barrier to trade.

However, this measure is considered to be a justified and proportionate measure to ensure the effective protection of fundamental right to privacy and data protection. In light of the particular sensitivity of the data relating to electronic communications, browser setting are considered as a necessary tool to make sure that users retain effective control over the tracking of their communications and thus to ensure compliance with the protection of the privacy of individuals in relation to the processing and dissemination of personal data. In the online world, users are increasingly overloaded with notices and requests for consent. Given people's limited time and the increasing complexity of online interactions, users are less and less capable of coping with the growing amount of notices and requests. A centralised system governing by means of mandatory general settings the users' privacy choices with regard to all third party interactions with their terminal equipment would greatly simply and make more effective the level of protection.

In particular, this system would have the following main advantages:

- Users would be able to set (and adjust) their privacy preferences only once, in a way that is valid and binding for all websites or services they interact with;

- Users would not be overwhelmed with banners and requests for consent every time they visit a website;

- If a user opts for strong privacy settings (e.g. do-not-track or "reject third party cookies"), tracking websites may still send individual requests to users (possibly through the browser) asking to be authorised to place cookies as a condition to access the website or the service. As these individual requests will be less frequent that it is the case today, users would be prompted to pay attention and make a conscious choice about whether or not they want to consent.

- Significant savings in terms of compliance costs may be envisaged per individual websites, given that the dialogue with the user, today performed by the websites, would be guaranteed centrally by general applications like banners.

- Moreover, it has to be considered that "reject third party cookies"/do-not-track software already exist in the market and are widely used. The main difference and added value of the present measures is (a) to clarify that these settings, as long as they correspond to certain conditions, can be considered as a valid and legally binding form of consent; (b) to ensure that these settings are made available by default in terminal equipment, by prompting users to regulate such settings at the first utilisation of the device to set their privacy preferences.

In light of the above, it is considered that the measure in question is indeed necessary and proportionate to achieve the underlying objective of ensuring effective protection of privacy and confidentiality of terminal equipment.

Summary stakeholder impacts

	Opportunities	Challenges
Citizens (both physical and legal persons)	☑ Comprehensive protection of confidentiality, irrespective of technology ☑ Clearer and more consistent rules, filling existing gaps and clarifying relationship with related legislation (e.g., GDPR) ☑ More consistent protection across the all EU ☑ Greater and better control of their choices thorugh privacy settings ☑ Enhanced transparency (publicly available Wi-Fi) ☑ Reduction of cookie consent fatigue ☑ Greater transparency of phone calls for marketing purposes ☑ More consistent and effective enforcement	☒ If cookies are blocked and privacy settings are set on "do-not-track", citizens may still be requested to give individual consent to "tracking". Websites may require consent to cookies to access specific websites/online services
Traditional fixed and mobile electronic communication services operators (ECS)	☑ One directly applicable regulation across 28 MS ☑ Clearer and more consistent rules, filling existing gaps and clarifying relationship with related legislation (e.g., GDPR) ☑ Savings from one-stop shop and consistency mechanism ☑ Level playing field with competing providers offering functionally equivalent services (OTTs) ☑ Greater opportunity to invest, with the user's consent, in the OBA market ☑ Removal of redundant or unnecessary obligations ☑ Savings from one-stop shop and consistency mechanism	☒ Higher fines in case of privacy breaches ☒ No removal of the ePrivacy rules
Over-the-top (OTTs), IoT and publicly available	☑ One directly applicable regulation across 28 MS ☑ Clearer and more consistent rules, filling existing gaps and clarifying relationship with related legislation (e.g., GDPR)	☒ New requirements/obligations become applicable (compliance costs) ☒ Potentially increased competition from ECSs in the

private Wi-Fi providers	☑ Opportunity to differentiate their offers on the basis of privacy features	OBA markets ☒ Opportunity costs
Website and OBA operators	☑ One directly applicable regulation across 28 MS ☑ Clearer and more consistent rules, filling existing gaps and clarifying relationship with related legislation (e.g., GDPR) ☑ Savings from one-stop shop and consistency mechanism ☑ Simplification measures proposed in relation to tracking (introduction of additional exceptions, derogations)	☒ Privacy sensitive citizens may decide not to use certain services, following the introduction of the rules on browser settings ☒ Opportunity costs
Web browser/Operating System	☑ Increased importance in the privacy ecosystem ☑ Opportunity to differentiate their offers on the basis of privacy features ☑ Increased market competitiveness on non-price factors	☒ Additional costs deriving from new obligations ☒ Higher fines for privacy breaches
Direct marketers	☑ One directly applicable regulation across 28 MS (with possible exceptions for voice-to-voice live calls) ☑ Clearer and more consistent rules, filling existing gaps and clarifying relationship with related legislation (e.g., GDPR) ☑ Savings from one-stop shop and consistency mechanism	☒ Increased costs for marketing campaigns ☒ Additional costs for the use of the prefix ☒ Higher fines for privacy breaches
SMEs	☑ The same opportunities identified for the various business categories above ☑ Smaller businesses will benefit from the increased harmonisation, legal certainty and consistency across 28 MS ☑ Smaller businesses will benefit from the simplification of the legal framework and the related reduced costs ☑ Lower costs in relation to the cookie consent provision	☒ The same identified for the various business categories above ☒ While the adjustment and opportunity cost required by the new rules is expected to be low, it may felt more by smaller businesses
Member States	☑ Streamlining of regulatory approaches and governance at national and EU level should drive synergies and may enable	☒ Ministries will need to ensure adequate resourcing and empowerment of supervisory authorities (where

	cost savings	not already the case), and governance changes may require re-organisation in some Member States

EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 3 final

PART 3/3

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}

ANNEX 8: DRAFT ECONOMIC ANALYSIS REPORT BY DELOITTE (SMART 2016/0080)

Economic Analysis

Introduction

This Annex, provided by the Commission's contractor of the external study supporting the impact assessment (Deloitte)[117], serves to achieve two objectives:

- To outline the overall model used for the projections, incl. a transparent discussion of its strengths and areas of further improvement ideally necessary[118];
- To present and explain the qualitative and quantitative data and assumptions used for the projections (incl. the specific approach used to translate qualitative reasoning concerning the assessment of the impacts of the policy options into tangible, quantitative assumptions).

A separate section is devoted to each of these objectives.

The overall model used for the projections

This section outlines the key procedural / analytical steps of the model developed for the assessment of the problem assessment, the establishment of the baseline scenario, as well as the assessment of the policy options and their comparison with the baseline scenario.

In addition, the section identifies key strengths and weaknesses of the model.

Overall, the model serves to provide quantitative projections as of 2002 until today. This can both be used for the REFIT exercise, as well as for the assessment of the problems. In addition, the model serves to provide quantitative projections for the expected development until 2030. These projections inform the establishment of the baseline scenario, and the quantitative assessment of the impacts of the options compared to the baseline scenario (status quo).

Key procedural / analytical steps of the model

Based on a number of assumptions that are further elaborated below (section 4), the model is used to project:

- The number of citizens affected by the ePD in the EU and per Member State between 2002 and 2030;
- The number of businesses (per size class) affected by the ePD in the EU and per Member State between 2002 and 2030;

[117] Deloitte, Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080).

[118] As will also be shown below, the projections should not be regarded as "exact calculations" but rather as projections based on (very) limited quantitative data in relation to what the situation is today, what it was before, and what it will be in the future.

- The magnitude of compliance costs for these businesses per year and Member State, as well as per size class; and
- The magnitude of costs stemming from administrative burden for businesses per year and Member State, as well as per size class.

Within the model, each of the above is projected based on distinct steps. These steps are presented in the table below.

Table 1 – Quantitative assumptions used for the projections

	Number of citizens affected	Number of businesses affected	Magnitude of compliance costs	Magnitude of costs from admin. burden
Preparatory tasks				
Step 1	Identification of relevant Eurostat data and evidence concerning the current usage rate of the services covered.	Identification of relevant Eurostat data	Identification of relevant quantitative economic data needed for the projections (see "basic assumptions" above). *[Eurostat data on the number of businesses is re-used]*	
Step 2	Projection of Eurostat data back to 2002 and until 2030 based on the CAGR of the identified data set (incl. completion of gaps in the initial Eurostat data set). Projection of the available evidence on usage rates of services back to 2002 and until 2030 based on the respective CAGRs	Projection of Eurostat available data back to 2002 and until 2030 based on the CAGR of the identified data set (incl. completion of gaps in the initial Eurostat data set).		
Step 3	Definition of qualitative assumptions regarding the development of the number of citizens and businesses affected, as well as compliance costs and costs related to administrative burden under the policy options and translation of these assumptions into quantitative proxies concerning the increase / decrease in the figures (in % per Article of the ePD) in the baseline scenario under each policy option.			
Milestone 1: Preparatory tasks are completed				
Assessment of the problem and establishment of the baseline scenario				
Step 3	Multiplication of Eurostat data concerning the number of citizens per year and Member State with the projected usage rates for each type of service.	Multiplication of the number of businesses per year, Member State, and size class with the share of businesses that have a website per size class.	*Cannot start before Step 4 concerning the number of businesses is completed because this is used as the relevant statistical basis.* Multiplication of the number of affected businesses per year, Member State, and size class with the share of websites that use cookies and that comply with legislation (e.g. because the websites are not inactive). Projection of a minimum, medium, and maximum scenario.	*Cannot start before Step 4 concerning the number of businesses is completed because this is used as the relevant statistical basis.* Multiplication of the number of affected businesses per year, Member State, and size class with the frequency of information obligations per year and with the hours of work of respective tasks.
Step 4	n/a	Multiplication of the number of businesses per year, Member State, and size class with the share of businesses that use cookies. Projection of a minimum, medium, and maximum scenario.	Multiplication of the number of websites that comply per year, Member State, and size class of business with the costs for websites to be compliant in EUR. The costs for websites to be compliant include costs related to Art. 5(3) and Art. 13. Costs related to Art. 4, as well as Arts. 5(1) and 5(2) have also been / are / will be incurred but cannot be estimated due to a lack of data.[119] Therefore, the estimates are very	Multiplication of the number of hours per year, Member State, and size class of business with the average salary in the EU in EUR. *Simultaneously:* Calculation of the Present Value of these costs in 2016.

[119] Costs concerning other Articles, are expected to be comparatively insignificant today and/or have already been written off since the adoption of the ePD in 2002.

	Number of citizens affected	Number of businesses affected	Magnitude of compliance costs	Magnitude of costs from admin. burden
			likely to underestimate the actual value of compliance costs. *Simultaneously:* Calculation of the Present Value of these costs in 2016.	
Milestone 2: Both the problem assessment (2002-2015) and the baseline scenario (2016-2030) are established.				
Projection of figures under the policy options and quantitative assessment of policy options				
Step 7	Multiplication of the baseline scenario figures per year and Member State with the expected increase / decrease of the number of affected citizens in % in relation to provision of the ePD, and each type of service per policy option.	Multiplication of the baseline scenario figures per year, Member State, and size class of business with the expected increase / decrease of the number of affected businesses in % in relation to each provision of the ePD per policy option.	Multiplication of the costs per year, Member State, and size class of business in the baseline scenario with the expected increase / decrease in % under the policy options based on a qualitative assessment of the impacts of each element of the policy options (see above).	
Step 8	Comparison of the policy options with the baseline scenario to identify a preferred policy option.			
Milestone 3: The quantitative assessment of the policy options and their comparison with the baseline scenario is completed.				

Source: Deloitte

Strengths and areas for improvement of the model

As part of this study, a pragmatic approach based on a model has been taken, compared to, for example, a regression analysis. The purpose of this section is to outline why this decision has been taken by addressing – in an open and transparent manner – strengths and areas that could be improved in case better data would be available.

Overall, the development and application of a certain type of economic model always depends on the types, granularity, and usefulness of the data available. Hence, economic modelling is always a trade-off between three factors: (1) The level of detail and accurateness of the model; (2) The accessibility of the model for outsiders and non-experts; and (3) The proportionality of the efforts to gather the relevant data, and to develop and implement the model in view of its usefulness for the analysis.[120] This means that modelling is always about striking the right balance between these factors.

Strengths of the model:

- The model is constructed in such a way that projections are "reasonable based on the information available and the assumptions made" – even though it has not been possible to gather comprehensive quantitative data (e.g. relating to *all* provisions), in particular with regard to any types of micro- and macro-economic costs.
- The model provides a pragmatic approach of projecting quantitative (economic) data that would otherwise not be available into both past and future.
- The model uses only a limited number of clearly defined assumptions, which makes it easy to adjust the projections in case better data becomes available. Given the lack of quantitative data, the assumptions made are considered to be fairly robust, given that

[120] According to the Better Regulation Guidelines (see section 2.5.3, page 27), only the most significant impacts should be quantified if possible, i.e. if they are susceptible of being quantitatively estimated through a sound methodology and if the required data exists and can be collected at a proportionate cost.

minimum, medium, and maximum scenarios have been used to project ranges where appropriate.

- The limited number of assumptions also makes the model more understandable to outsiders. This makes the model's results traceable also for non-experts.
- The model allows for a quantitative comparison of the policy options with the baseline scenario based on clear and traceable assumptions on how the policy options have an impact on the quantitative data.

Areas in which improvements could be made in case better data was available:

- In relation to costs for businesses, the model only projects the available data on compliance costs and costs stemming from administrative burden": (1) This means that, although efforts have been undertaken to obtain more and better data from businesses and business associations, the data used in the model is the best data available. (2) This means that opportunity costs (e.g. from lost business opportunities) are not in scope of the model, although they are assessed qualitatively. This has two reasons: (1) Only illustrative quantitative evidence is available; and (2) A sound quantification of future opportunity costs (e.g. until 2030) is hardly feasible because they depend on the market success of future technologies and business models that are not yet developed (or even conceived) today. What is possible, however, is the qualitative illustration of current opportunity costs.[121]
- Feedback received from businesses shows that after the adoption of the ePD, businesses incurred significant capital expenditure (CAPEX) to develop and implement the technical measures needed to comply with the legislation. The model implicitly assumes that such historical capital expenditures to comply with the ePD (CAPEX) in particular for technologies and services outdated today have been written off already by the businesses and have amortised themselves over the years. This concerns, for instance, costs regarding the presentation and restriction of calling line identification which is already built-in by design in modern devices today. Recurring operating expenditures (OPEX) are assumed to have decreased over time with only insignificant recurring costs occurring today. Due to the lack of data on such historical costs, however, they cannot be projected. The result is that the compliance costs for businesses projected for the time period directly after the adoption of the ePD are likely to be underestimated.
- With regard to some of its elements, the model does not apply dynamically, i.e. accounting for evolving variables over time, but rather static assumptions regarding the quantitative value of the variables. This means that, due to a lack of data, the model assumes that the following variables included in the model are stable over time (2002-2030):
    - The share of businesses that have a website;
    - The share of websites that use cookies;

[121] A 2016 study by the Open Rights Group, for instance,[REFERS TO ANOTHER STUDY WHICH] estimates that that by 2016 UK mobile operators could be making over half a billion pounds a year just from monetising the location of their customers. In terms of opportunity costs, this means that if such direct monetisation would depend on the prior consent of consumers, UK mobile operators alone (i.e. not the retailers who could monetise location data of their customers) could miss roughly 600 million Euro per year in revenue. See: https://www.openrightsgroup.org/assets/files/pdfs/reports/mobile-report-2016.pdf

- Similar average wages across the EU in relation to information obligations; and
- The number of working hours per task in relation to information obligations, as well as the frequency of obligations.

Ideally, the model should apply dynamic quantitative figures (i.e. evolving over time) for all these elements and, in addition, account for inflation in relation to pricing developments. With the Net Present Value, we have however used a measure that allows to project values in 2002 (e.g. the costs related to administrative burden) based on constant prices of 2016.

A similar point is valid for the assessment of the policy options. The model assumes consistent impacts of the policy options over time (i.e. percentages of increases / decreases of the number of citizens and businesses affected, as well as the costs for businesses).

Overall, the use of such a *pragmatic* model is reasonable both in view of the given data limitations and the focus of the analysis as such. Finally, the based on the model it is possible to project at least some quantitative data and thus add value to the overall analysis.

The qualitative and quantitative data and assumptions used for the projections

This section presents the available quantitative data, as well as the underlying quantitative and qualitative assumptions with regard to the REFIT exercise, the assessment of the problem and the establishment of the baseline scenario. The assumptions concerning their impact of the policy options on the quantitative elements identified in the bullet points above are presented in a separate table below.

Basic assumptions for the problem assessment and the establishment of the baseline scenario

In general terms, quantitative economic data as concerns most aspects surrounding the ePrivacy Directive are scarce. Feedback from businesses received as part of the online survey and the interviews carried out shows that:

- The vast majority of the organisations consulted do not hold quantitative information concerning the impacts of the ePD, e.g. as concerns the relevant costs (meaning compliance costs, costs stemming from administrative burden, and opportunity costs); and
- In case quantitative information is available, it is patchy, mostly anecdotal (i.e. not available in a structured sense), inconsistent, inhomogeneous, and inconclusive (meaning that information from one stakeholder can be contradictory to information from another stakeholder).

In order to mitigate this challenge, a pragmatic, quantitative model that is based on a limited set of quantitative building blocks has been developed. More specifically, the model is based on two types of data:

- Publicly available Eurostat statistics on the number of citizens (2002-2015) and businesses (mostly 2010-2014) per year and Member State; and
- Quantitative data obtained by means of desk research, the online survey, and the interviews carried out. As indicated above, the available data is scarce.

While the Eurostat statistics have been used as the primary building block for the projections, the data gathered as part of the desk research, the online survey, and the interviews have been used to develop the assumptions on which the projections have been carried out.

Table 2 provides an overview of the quantitative assumptions used for the projections. Table 4 provides more detailed explanations of these assumptions, as well as qualitative reasoning.

Table 2 – Quantitative assumptions used for the projections

Information need for which a quantitative assumption has been made	Quantification
Number of citizens affected	
Compound Annual Growth Rate (CAGR) for services (2016-2030)	%
Internet to browse online	3.4%
Online social networks	3.4%
E-Mail	4.0%
Instant messaging	7.9%
VoIP	9.7%
Mobile phone to make calls or send texts	3%
Fixed phone line	-4%
Number of businesses affected	
Constant shares of businesses that have a website by size over time	
0 to 9 persons employed (micro-enterprises)	60%
10 to 19 persons employed (SMEs)	75%
20 to 49 persons employed (SMEs)	75%
50 to 249 persons employed (SMEs)	85%
250 persons employed or more (large enterprises)	95%
Share of non-EU businesses that have a website[122]	99%
Share of websites using cookies	
Maximum scenario	55%
Medium scenario	50%
Minimum scenario	45%
Compliance costs	
Share of websites that would need to comply	
Maximum scenario	47%
Medium scenario	42%
Minimum scenario	37%
Costs for websites to be compliant	900 EUR
Average useful life time of a website in years	3 years
Costs (EUR) per website to be compliant (one-off)	300 EUR
Share of businesses that have a website and use cookies and potentially provide for unsolicited communication using publicly available electronic communications services in public communications networks	90.0%

[122] Non-EU businesses that are active in the EU and have websites fall under the ePD. Therefore, it is important not to discard them as part of the quantitative assessments.

Information need for which a quantitative assumption has been made	Quantification
Additional share of annual costs for websites to be compliant	25.0%
Additional annual costs for websites to be compliant	75 €
Frequency of checking the Robinson list (per year)	26.0
Duration of checking Robinson list	15 minutes
Social discount rate for Net Present Value	4%
Administrative burden	
Average salary per hour	18 EUR
Number of hours consumed with an information obligation	
Maximum scenario	16 hours
Medium scenario	8 hours
Minimum scenario	4 hours
Frequency of information obligations per annum	
Maximum scenario	Once every two years
Medium scenario	Once every four years
Minimum scenario	Once every eight years

Source: Deloitte

In addition, below a mapping is provided in relation to the types of businesses (i.e. only businesses active in the telecommunications sector or potentially businesses in all sector) covered by the analysis in relation to each of the ePD's provisions as part of the REFIT exercise, the problem assessment and establishment of the baseline scenario, as well as the assessment of the impacts of the policy options compared to the baseline scenario.

Table 3 – Mapping of types of businesses covered by each provision of the ePD

Article	REFIT exercise	Problem Assessment	Baseline scenario	Assessment of policy options
4.1 & 4.2	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector with emphasis on additional OTTs
4.3 & 4.4	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
5.1 & 5.2	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector with emphasis on additional OTTs
5.3	All businesses that store or access information in the users' terminal equipment (e.g. based on cookies)	All businesses that store or access information in the users' terminal equipment (e.g. based on cookies)	All businesses that store or access information in the users' terminal equipment (e.g. based on cookies)	All businesses as above with emphasis on additional browser providers, app store providers, and operating system providers
6 & 9	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector with emphasis on additional OTTs
7	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
8 & 10	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
11	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
12	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector	Businesses in the telecom sector
13	All businesses that provide for unsolicited communications by means of electronic communications	All businesses that provide for unsolicited communications by using publicly available electronic communications services in public communications networks	All businesses that provide for unsolicited communications by means of electronic communications	All businesses that provide for unsolicited communications by means of electronic communications

Source: Deloitte

Table 4 – Qualitative and quantitative assumptions used for the projections

Broad area of assumption	Assumption and brief explanation
Number of citizens affected	
General assumption on the future growth of the population	The past and future growth of the population follows the growth rate of the years for which data is available, e.g. 2002 to 2015 (per Member State, based on Eurostat data). This is a common assumption for models projecting future scenarios. However, it is a rather static assumption that does not take account of e.g. national population policies (in particular regarding fertility and ageing). It should be kept in mind that, under certain conditions such as no *jump* in fertility rates occurs in the future, the population growth might not only be slowing down, but also turn into a decline at some point. Similarly, past population growth could have also been different from in the years for which data is available. However, as no specific data is available, this assumption seems most pragmatic. We have used Compound Annual Growth Rates (CAGR) to project the development of the population into the future. The CAGR represents the year-over-year growth rate (in %) for a specific type of statistics and is used as a multiplicative factor in order to project the figures identified in the problem assessment until 2030 as a cumulative figure, or in 2030 as an annual figure. In order to project a figure in 2030 the following formula has been applied: $y_t = y_{2016} \times (1 + CAGR)^{(t-2016)}$ Whereas y_t is the value of the number of citizens affected in year t, The CAGR can be used to project figures both into the future, as well as into the past in case no relevant public statistics from Eurostat are available.
General assumption concerning the number of citizens affected based on usage rates of services	The number of citizens affected is linked to the (projected) usage rates for each service covered by the ePD. The projections are based on Eurobarometer data[123] regarding the share of citizens that make use of a service "at least a few times per month".[124] This means that only citizens that make use of a specific service are affected – either positively (e.g. benefitting from higher privacy standards) or negatively (e.g. if companies are not compliant), while others not making use of a service are not affected. In practice, however, it could be argued that also citizens that do not make use of a service could be affected. This argument has two components. On the one hand, citizens could use services on behalf of others, e.g. buying products online for elderly, transferring cash online to a regular bank account for which data could be hacked, communication not *with* but *concerning* a third person etc. On the other hand, there is also a societal component, in that e.g. in case of a security breach or data hack, not only the person who has been subject to the security breach or being hacked is affected, but quite naturally also the citizens in the social environment of this person. Such argumentation is, however, not reflected in our projections. We have used Compound Annual Growth Rates (CAGR) to project the development of the usage rates in the future (see also below).
Compound Annual Growth Rate for services reflected in Flash Eurobarometer 443	
Internet to browse online	We have used a **CAGR of 3.36%** for this service. This assumption is based on evidence regarding the increase of global consumer Internet traffic (2015 to 2020), which is estimated to be 18%.[125] Assuming an

[123] Flash Eurobarometer Survey 443 on ePrivacy.
[124] In addition, account has been taken of the approx. years in which major OTTs (WhatsApp, Facebook, and Skype etc.) were introduced in the EU markets. This means that usage rates increase by a larger margin since then.

Broad area of assumption	Assumption and brief explanation
	unchanged growth rate for the time frame of 2020 to 2030, the respective CAGR can be calculated.
Online social networks	See *Internet to browse online*
Email	We have used a **CAGR of 4%** for this service. This assumption is based on evidence regarding the increase in mobile email traffic by 32.8% from 2010 to 2015.[126] As this is the best data available, it is assumed that this forecast also applies to the timeframe of 2015 to 2030. However, it is assumed that the actual CAGR is likely to be lower. The reason for this is that emails are expected to be gradually replaced / complemented by other forms of communication such as instant messaging – in particular in the private sphere but also more and more in a business environment. Therefore, the projected development can be considered as a maximum projection.
Instant messaging	We have used a **CAGR of 7.92%** for this service. This assumption is based on evidence regarding the increase in mobile IM traffic by 46.3% from 2010 to 2015.[127] As this is the best data available, it is assumed that this forecast also applies to the timeframe of 2015 to 2030. However, it is assumed that the actual CAGR is likely to be lower because of new future market developments that might evolve further from instant messaging. Therefore, the projected development can be considered as a maximum projection.
VoIP	The global VoIP volume is expected to **grow by 9.7%** between 2014 and 2020 by Transparency Market Research.[128] It is assumed that this estimate to be applicable as a CAGR for the number of VoIP users.
Mobile phone to make calls or send texts	No evidence could be found on the CAGR in relation to this service. However, it is assumed that, in line with general market trends such as the increased use of mobile devices and mobile internet, the use of mobile phones to make calls or send texts will increase by a **CAGR of 3%.**
Fixed phone line	In 2010, IBM calculated a voice traffic **decline in minutes by 4%** between 2003 and 2008. This information is used to project the development until 2030, keeping in mind that the decline could be even stronger based on the take-up and development of other services.
Number of affected businesses	
General assumption on the future growth of the number of businesses	Similar to the number of citizens, the past and future growth of the number of businesses (micro, SMEs, large, and foreign enterprises) is expected to follow the growth rate (overall) of the previous years (per Member State, based on Eurostat data). We have also used Compound Annual Growth Rates (CAGR) to project the development of the number of businesses in the future based on available public data from Eurostat.
General assumption concerning the number of businesses affected by the ePD	For the calculation of the compliance costs of the ePD, it is assumed that the ePD potentially affects all businesses that run a website and use cookies based on Article 5(3). The number of businesses affected by other provisions of the ePD is expected to be significantly lower as they refer to the telecom market only (e.g. Art. 4, 5(1), 5(2)) or only to a sub-group of businesses (i.e. those providing for unsolicited communication using publicly available electronic communications services in public communications networks under Art. 13 – this means that not all businesses that you "some sort of communication B2B or B2C" are covered but only those that make actual use of "unsolicited communication".)

[125] See: http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf, page 14.
[126] See: http://www.telecomsmarketresearch.com/reports/itm_Mobile_Messaging_extract_LR.pdf
[127] See: http://www.telecomsmarketresearch.com/reports/itm_Mobile_Messaging_extract_LR.pdf
[128] See: https://www.linkedin.com/pulse/20140911043449-339157087-voip-services-market-is-growing-at-a-cagr-of-9-7-from-2014-to-2020

Broad area of assumption	Assumption and brief explanation
	).[129] Overall Article 5(3) extends the scope of the ePD also to businesses active in other industries than the telecom sector.[130] Keeping this in mind, alternative projections have been carried out for businesses that Eurostat strictly defines as being part of the "Telecommunications sector", i.e. businesses providing telecommunications and related service activities, such as transmitting voice, data, text, sound and video. While the former projections concerning "businesses overall" can be regarded as projections of the absolute maximum values, projections referring to the "telecommunications sector only" should be seen as minimum projections.
General assumption concerning the application of Art.5(3) to potentially all businesses	We assume that Article 5(3) generally applies to all businesses that operate a company website, as cookies can be stored and information can, in principle, be tracked on every website. However, there are two important restrictions to this assumption: (1) Not all businesses run a website; and (2) Not all company websites use cookies (i.e. "no cookies" vs. "some sort of cookie"; If a website does not use any cookies, they do not need to comply. If they are using any sort of cookies, they indeed need to comply). Hence, it can reasonably be assumed that the maximum number of businesses in the EU affected by the ePD has a strong correlation to the number of company websites operated by: (1) Businesses that have their primary place of establishment within the 28 EU Member States; and (2) Third-country businesses that operate within the EU (i.e., by means of their own website(s)). With regard to the share of websites using cookies, projections have been carried out in relation to three scenarios (minimum, medium, maximum). In general, the available evidence has been used to project the medium scenario, but have also run projections for a higher and lower scenario in order to account for uncertainty factors around the share of websites using cookies.
Art. 5(3): Shares of businesses that have a website	
0 to 9 persons employed (micro-enterprises)	The share of micro-enterprises that have a website is not available, but it can be assumed that it is below 75% (as for SMEs), since micro-enterprises may be less active online in order to concentrate better on their core business. This does not say that the core business of micro-enterprises cannot be online-based. However, the overwhelming majority of micro-enterprises consists of local shops, small/medium restaurants, and other types of shops that do not necessarily have to have a website in order to be able to provide their products or services. Moreover, the use of general platforms or social networks like Facebook, Youtube, Resto.be, etc. as an alternative to fully-fledged websites is has become widespread Thus, it is assumed that the **share of micro-enterprises that have a website is 60%.**
10 to 19 persons employed (SMEs)	According to Eurostat's latest available data, in 2013, **75% of all enterprises** employing 10 or more persons in the 28 EU Member States had a website.[131]
20 to 49 persons employed (SMEs)	
50 to 249 persons employed (SMEs)	We assume that the share of businesses of this size class that operate a website is higher than 75%. However, no quantitative data is available. Nevertheless, it has been **assumed that the share is 85%.**
250 persons employed or more (large enterprises)	We assume that the share of businesses of this size class that operate a business is higher than 75%. However, no quantitative data is available. Due to the size of such businesses, it has been **assumed that the share is 95%.**
Share of non-EU businesses that have	Non-EU businesses are by definition active across borders and therefore do not only provide domestic services. Therefore, they are very likely to run a website.it is

[129] With specific regard to Art. 13, it should be noted that the number of businesses affected is independent of Member States having enacted an opt-in or opt-out solution in national legislation, as e.g. the Robinson lists are checked by each business anyway on a regular basis.
[130] Overall, the model estimates costs for businesses in relation to Art. 5(3) and Art. 13. Information on costs in relation to other Articles is generally scarce and has, as much as possible, been reflected in the report qualitatively.
[131] [isoc_ci_eu_en2]. Last updated on 9 June 2016.

Broad area of assumption	Assumption and brief explanation
a website	assumed **that the share is 100%**
Art. 5(3): Share of websites using cookies	
Maximum scenario	As indicated above, minimum, medium, and maximum projections have been carried out based on the share of websites using cookies. **The medium value, for which evidence is available, is 50.2%** based on information by W3Techs who run web technology surveys[132] ("50.2% of all websites use cookies"). In addition, the European Commission's 2015 Article 29 cookie sweep action[133] showed that only 70% of websites with cookies were using tracking cookies. However, as concerns the baseline scenario, such tracking cookies are not relevant for the estimate of the compliance costs but only for the assessment of the impact of the policy options as currently all types of cookies used on websites trigger the cookie notification. We have added / subtracted 5% for each the minimum and maximum scenario in order to project a corridor in which the *actual* figure is most likely to be in (i.e. 40% in maximum and 30% in minimum respectively). This is used as a sensitivity analysis.
Medium scenario	
Minimum scenario	
Compliance costs	
General assumption concerning the *origin* of compliance costs related to the ePD	In general, information on costs incurred in order to comply with the ePD is scarce. Businesses nor business associations only have patchy, anecdotal information on the costs related to the ePD in general. Information on particular provisions is even less available. However, feedback received as part of the interviews suggests that the majority of costs for the ePD is related to: • Art. 4 on the security of processing; • Art. 5(1) and Art. 5(2) on confidentiality of communications; • Art. 5(3) on cookie consent; and • Art. 13 on unsolicited communication. In relation to Art. 4, as well as Art. 5(1) and Art. 5(2), businesses have indicated that they have incurred a significant amount of compliance costs after the adoption of the ePD. However, businesses were not able to provide any quantitative information on this as the costs were already incurred in the past (almost 15 years ago) and have since then been written off. However, businesses indicated in qualitative terms that they incur still today (and will in the future) costs in relation to regular updates, maintenance, and repair of the necessary hard- and software to safeguard the security and confidentiality of communications. However, it was not possible to obtain any quantitative information from businesses on the magnitude of such costs. Art. 5(3) is expected to be responsible for a significant amount of compliance costs. This is due to the extensive coverage of this provision (potentially all businesses in the EU that run a website and use cookies), as well as its importance for today's communication, marketing, advertising, and sales techniques. As businesses are increasingly developing data-driven business models, the importance of the substance of Art.5(3) is also expected to grow over the next years. The costs associated with this provision mainly stem from the need to collect users' consent to be able to use cookies on websites, i.e. to implement the relevant technical solutions on websites. In addition, Deloitte has been requested to undertake particular efforts to estimate compliance costs in relation to Art. 13 on unsolicited communications as this provision, in addition to covering voice calls, also involves the implementation of a technical solution on websites to collect users' consent to *unsolicited* communication. As only very limited quantitative information was obtained from businesses, expert judgment was used to estimate respective compliance costs (see the

[132] https://w3techs.com/technologies/details/ce-cookies/all/all
[133] See: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf

Broad area of assumption	Assumption and brief explanation
	assumptions below in the section on the assumptions). Finally, after the adoption of the ePD, in particular telecommunication service providers have – according to our interview results – incurred high capital costs in relation to the implementation of: • Articles 6 and 9 on traffic data and location data other than traffic data; • Article 7 on itemised billing; • Article 8 on control of connected line identification (incl. Art. 10 on exception); and • Article 11 on automatic call forwarding. Under Art. 6 & 9, and 12 concerning directories of subscribers, businesses incur some costs regarding information obligations to consumers. Based on the feedback received, these costs can be expected to be fairly large. However, these costs, which were incurred in the past by telecommunication service providers, can be expected to be already written off. Initially high investments have already amortised themselves over the years. In addition, over time, the operational expenditures in relation to these provisions have decreased and are expected to be insignificant in view of the overall costs incurred by businesses today – keeping in mind that costs are incurred in relation to e.g. maintenance, updates, repair etc. Apart from itemised billing (which today is expected to be a standard process with no additional costs for service providers), the services regulated by these provisions are generally regarded as outdated or built-in by design in devices. Overall, this means that the compliance costs estimated as part of this study are based on costs related to Art. 5(3) and Art. 13 (based on expert judgment). The quantitative findings of the study are thus very likely to underestimate the actual amount of compliance costs incurred in the past, today, and thus in the future (at least for new businesses who have not yet incurred the initial capital costs for implementing these provisions). This is due to the fact that capital and recurring expenditures relating to other Articles than Art. 5(3) and 13 could not be estimated. The available evidence has, however, been taken into account in qualitative terms as much as possible.
Art. 5(3) Share of websites that would need to comply	
Maximum scenario	For the purpose of projecting compliance costs, in addition to the share of websites using cookies, it is also important to account for websites that are not active or not complying with legislation. While all *businesses* that run websites with cookies may potentially be affected, costs are only incurred in relation to those *websites* that need to comply with legislation, e.g. no holding pages, pay-per-click sites, and private (password-protected) sites.
Medium scenario	
Minimum scenario	The 2014 ITIF report on the economic costs of the European Union's cookie notification policy cites data by EURid, the European registry in charge of ".eu", indicates that 41.9% of websites in the EU are active and complying with legislation.[134] Similarly to the scenarios concerning the share of websites using cookies, this information is used to project a minimum, medium, and maximum scenario for the share of websites that would need to comply. **The medium value is 41.9%,** while 5% have been added / subtracted respectively to project a corridor in which the *actual* figure is most likely to be in (i.e. 47% and 37% respectively).
Costs per website to be compliant	The projection of the compliance costs relies on the costs per website to comply with legislative requirements. The 2014 ITIF report projections a lump sum of 900 EUR per website incl. costs associated with legal advice, updates to privacy policies, and technical updates to websites. The ITIF study was indeed cited by different stakeholders consulted as part of this initiative, implying that this estimate is considered realistic by these stakeholders. Similarly, an online retailer estimated that the costs relating to the implementation of the cookie banner lie around 1150 Euro per website. This estimate is again very

[134] See: http://www2.itif.org/2014-economic-costs-eu-cookie.pdf, page 4.

Broad area of assumption	Assumption and brief explanation
	close to the estimated 900 Euro per website, although this online retailer also indicated that additional costs occur to deal with customers who complain about seeing the banner even after consenting (e.g. because they clear their browser history or move to a new browser). However, there were also a few stakeholders that indicated that compliance costs would be significantly higher or lower. For instance, an internet content provider replying to the public consultation indicated that the costs to implement the cookie banner would be relatively small and could be similar to the annual costs of hosting a website. A large IT hardware and network systems company reported significantly higher annual costs: they estimate annual costs for a cookie opt-out tool of ca EUR 280,000, and additional costs of ca EUR 70,000 for a trained resource. Based on the information available, it seems that such high costs only apply to large businesses, i.e. the minority of businesses that need to apply the cookie banner. In addition, the ITIF report indicates, however, that it is expected that costs are higher for larger organisations with more complex web operations. Finally, the ITIF report indicates that the average useful lifetime of a website is three years over which the 900 EUR are incurred. Therefore, the annual **price per website has been set at a lump sum of 300 EUR**, knowing that this is only a very raw estimate based on very limited, but best data available.[135] It is expected that this estimate includes technical and legal advice, as well as regular updates and maintenance of the websites cookie policies.
Art. 13 on unsolicited communication	
General assumption	Although only very limited quantitative information is available in relation to costs associated with Art. 13 (apart from information that eCommerce businesses generally check the Robinson list about every two weeks as part of a standardised process), quantitative estimates were still carried out – mostly based on expert judgment. In general, we assume that compliance costs are incurred not by all businesses that provide for unsolicited communication but only by those that also have a website and use cookies because collecting the consent of users over the counter does not produce costs. There are two reasons for which this can be reasonably assumed: (1) All businesses can, potentially, make use of unsolicited communications by electronic communication means– either in a B2B or B2C context. However, it is only those businesses that provide for a website that are actually able to collect users' consent, either by an opt-in or opt-out solution. Furthermore, such businesses are generally expected to make also use of cookies in order to understand better "who their customers are" with a view to providing *targeted* unsolicited communication by electronic communication means. (2) Businesses that provide for unsolicited communication by electronic communication means but do not make use of a website are not able to collect the consent of their customers – both from a B2B and B2C perspective. Therefore, such businesses are expected to simply provide for unsolicited communication – even though this may not necessarily be compliant with national law. In any event, though, the compliance costs incurred by such businesses (e.g. related to legal advice) are (1) expected to be insignificant in view of the overall amount of costs; and (2) even though businesses may have costs related to legal advice, they could still make use of unsolicited communication as the chances of being detected of non-compliance are close to zero. In a nutshell, the compliance costs associated with Art. 13 are thus only incurred by businesses that also incur costs in relation to Art. 5(3). Based on the feedback received from businesses and business associations, three main cost elements can be distinguished in relation to Art. 13[136]: • The technical implementation of the opt-in / opt-out solution; • Checking the Robinson list for B2B and B2C customers that have registered; and

[135] In fact, the ITIF report itself indicates that the 900 EUR number was chosen based on *feedback from European colleagues* and *personal correspondence with a European think tank*.

[136] As part of the interviews, feedback was received that businesses e.g. check the Robinson lists irrespective of whether or not a Member State has implemented an opt-out solution because you citizens may opt-in at the start and then afterwards withdraw their consent through an opt-out again. This means that although consumers might need to opt in at the start by default they can still withdraw their consent (even one second after they opted in theoretically).

Broad area of assumption	Assumption and brief explanation
	• Assisting B2B and B2C customers to register / de-register on such a list. As available evidence is very scarce, estimates are only possible with regard to the first two of the above cost elements. Overall, it has to be kept in mind that the most significant cost element in relation to Art. 13 is not the compliance costs but the opportunity costs – i.e. the costs businesses would incur / the revenue businesses would lose in case they were not allowed to provide for unsolicited communication.
Share of businesses that have a website, use cookies, and potentially provide for unsolicited communication by means of electronic communication	No quantitative information is available in this regard. Deloitte is still making efforts to validate the assumptions with businesses. We assume that almost all businesses that have a website and use cookies could potentially provide for unsolicited communications by electronic communications means – in either a B2B or B2C context. Therefore, we have set the share at a value of 90% of respective businesses.
Additional annual costs for websites to be compliant	No quantitative information is available in this regard. Deloitte is still making efforts to validate the assumptions with businesses. There are some costs associated with the technical implementation of the opt-in / opt-out solution on businesses website. As businesses were not able to provide such quantitative information though, an estimate of an additional share of 25% of the costs per website to be compliant (see above) – i.e. 25% * 300 EUR = 75 EUR, has been assumed per business in order to provide for the respective technical solution on a website.
Frequency of checking Check Robinson list (per year)	As part of an interview with an eCommerce business association, we have received the information that eCommerce businesses generally check the Robinson list every two weeks as part of automated standard processes that only trigger further work in case a B2B or B2C customer has registered on the Robinson list and may thus not be targeted by means of unsolicited communication anymore. Given that the year has 52 weeks, we have set the value therefore at 26.
Duration of checking Robinson list	No specific quantitative evidence was obtained as part of the interviews on the duration of checking the Robinson list. However, it was indicated that this is more or less an automated standard procedure. Without further quantitative evidence available, we assume that it takes an average business therefore not more than 15 minutes to check the Robinson list on a given occasion. For the purpose of the quantification of the costs associated with checking the Robinson list, we have used an average salary of 18 EUR (see the section on administrative burden below).
Overall compliance costs related to Arts. 5(3) and 13	Based on our assumptions outlined above, a given business is expected to have incurred approx. 490 EUR in 2016. This estimate is a recurring cost. However, the magnitude of the costs is decreasing. This means that in 2002, the amount in Euro incurred was higher than today while it is expected to be lower in 2030. The cost Is decreasing because businesses adapt and learn over time and get more acquainted to a certain set of legislative rules. This is closely connected to "economies of scale" in which a solution, once developed and implemented, can be re-produced and adapted at relatively low cost. This has been estimated in the following way: *Art. 5(3):* • Costs per website to be compliant: 900 EUR • Average life time of a website: 3 years • Costs per website to be compliant per year: 300 EUR *Art. 13:*

Broad area of assumption	Assumption and brief explanation
	• Additional annual costs for websites to be compliant: 25% of costs per website to be compliant with Art. 5(3) per year • Frequency of checking Check Robinson list (per year): 26 • Duration of checking Robinson list: 15 minutes (i.e. 0.25 hours) • Average salary in the EU: 18 EUR per hour *Formula applied:* (900 EUR / 3 years) + 25% * (900 EUR / 3 years) + 26 * 0.25 * 18 EUR = **490 EUR** *Expected development of costs:* It is expected that the value of costs incurred by businesses per year in 2016 has decreased since 2002 and will further decrease until 2030.
Administrative burden	
General assumption on the average salary per hour	We have set the average labour costs (wages and salaries) per hour concerning website-related tasks at 18 EUR across the EU. This is largely in line with Eurostat data on the average amount of wages and salaries in enterprises employing more than 10 persons (excluding other labour costs).[137] Although country-specific differences of course exist concerning the cost of labour, this average amount has been used to estimate costs in relation to each country.
Art. 4: Number of hours consumed with an information obligation	
Maximum scenario	In addition to the average salary per hour, the projection of the costs stemming from the administrative burden is based on the number of hours it is expected to take one full-time equivalent (FTE) to carry out the tasks related to the information obligations set out by legislation. Under the ePD, information obligations only exist under Article 4 concerning data breach notifications. Such information obligations only apply to electronic communication service providers (i.e. not all businesses as under Art.5(3). Information obligations in relation to provisions other than Art.4 (incl. Art. 4.2 on notifying risks) only exist in relation to an investigation – and are therefore depending on the frequency of enforcement in the specific Member States. The ePD study SMART 2013/0013 has shown, however, that the level of enforcement of most of ePD provisions in most of the Member States is very low.[138] It can be estimated that the overall administrative burden for the application of the ePD provisions, other than Article 4, to be negligible in average terms or in any event very low. Without having received any quantitative evidence from stakeholders – only qualitative information on the duration of related tasks has been obtained – it is assumed (i.e. an assumption, not based on hard facts) for the purpose of this projection that data breach notifications are a standardised electronic procedure (at least within the major market participants' organisations) that, given that national thresholds for reporting are met or exceeded, do not take more than 16 hours per case (i.e. two working days). This has been used as the maximum scenario. Furthermore, the medium scenario has been set to 8 hours per case (i.e. one working day). As a minimum scenario, it is assumed that it takes an FTE 4 hours per case (i.e. half a working day) to process data breach notifications. Since the adoption of the ePD until today, costs in relation to such information obligations are expected to have been mostly occurred by telecommunication service providers. Such costs would decrease further under the Policy Options although the scope of the ePD would be extended to OTTs. However, it has to be considered that none of the policy options provide for regular information/notification obligations for OTTs. Thus, administrative costs would also in this case only materialise in case of enforcement/auditing.
Medium scenario	
Minimum scenario	

[137] See e.g.: http://ec.europa.eu/eurostat/statistics-explained/images/a/ac/Estimated_hourly_labour_costs%2C_2015_%28%C2%B9%29_%28EUR%29_YB16.png
[138] See also the Commission Staff Working Document -- Impact Assessment in relation to the GDPR proposal, page 101.

Broad area of assumption	Assumption and brief explanation
Art. 4: Frequency of information obligations per annum	
Maximum scenario Medium scenario Minimum scenario	In addition to the average hourly wage and the number of hours it takes an employee to carry out tasks in relation to information obligations, the projection of costs related to administrative burden depends on the frequency of information obligations per year. The data received from competent authorities on the frequency of data breach notifications shows that such information obligations are rare, at least on an individual company-by-company basis.[139] For instance, the feedback received (a number of smaller and larger Member States have not provided information on this) indicated that in 2015, 2,915 notifications of personal data breaches were received with number in the years before being (significantly) lower (almost all, 2,867, of these notifications relate to the UK and Ireland). Keeping in mind the sheer number of businesses in the EU that could potentially be affected by personal data breaches, we therefore expect that notifications to be a rarity for individual businesses at least.[140] This is also reflected in the 2015 ePD study. The available data on the number of data breach notifications can, however, not be translated directly into a measure for the frequency of data breach notifications per company as it might be that several notifications stem from one or the same company (e.g. relating to one specific data breach or a series of notifications as part of a larger data breach). Despite the absence of further quantitative evidence concerning frequency of data breaches, it is assumed that an individual business would at most have to **report once every two years** (see also the GDPR IAs, NIS impact assessment, and Telecom package IA). The maximum scenario has been set at once every four years, while the minimum scenario has been set at once every eight years. Information obligations concerning data breaches only concern businesses in the telecommunications sector and not all businesses that might otherwise be affected by the ePD, e.g. by Art.5(3).
General assumption concerning projections of costs into the past and future	
Social discount rate for Net Present Value	In relation to costs in the past and the future, it is important to apply discount rates when projecting over a certain time period. The European Commission's Better Regulation Guidelines foresee a standard social discount rate of 4%[141], which has been applied to project the net present value of figures. The Net Present Value (NPV) is calculated in order to make past and future payments over a certain number of time periods comparable to today. This means that e.g. payments in the future would (in the future value of the currency) exceed today's payments, while in today's terms, the payment in the future will actually be lower than today. In addition, according to the Better Regulation Guidelines, "calculating the present value of the difference between the costs and the benefits provides the NPV of a policy measure. Where such a policy or project generates a positive NPV, there would be no obvious reason to prevent it from proceeding, as long as the distribution of costs and benefits among different social groups is deemed to be acceptable and all costs and benefits are included in the computation (which is often methodologically challenging)."

Source: Various sources, tabulated by Deloitte.

[139] Information obligations in relation to data breach notifications are rare on an individual company-by-company basis – in relation to both subscribers and users, as well as public authorities. This is not due to the non-existence of data breaches but mostly due to the limited severity (i.e. do not affect users' privacy).
[140] In the UK and especially IE there are higher number of security breaches compared to other Member States. However, it can reasonably be assumed that it would be a significant share if seen in relation to the total number of businesses in those countries. As a consequence, this this sentence applies to the whole EU, including UK and IE.
[141] See page 377 of the Better Regulation Toolbox. The Better Regulation Guidelines also indicate that a lower discount rate could be applied for costs in order to account for social benefits achieved through policy intervention. However, for the sake of comparability as emphasised by the Better Regulation Guidelines, 4% have been used.

Approach and assumptions used for the assessment of the policy options

This section presents the assumptions made regarding the impact of the policy options.

The general approach used to translate qualitative reasoning into quantitative assumptions[142]

One of the prime challenges of impact assessments is the translation of qualitative analysis into tangible, quantitative findings. In fact, the Better Regulation Guidelines specify "significant impacts should be assessed qualitatively and, whenever possible, quantitatively." In this respect, "if possible" means that impacts are susceptible of being quantitatively estimated through a sound methodology and if the required data exists and can be collected at a proportionate cost.

Keeping this in mind, an approach consisting of six consecutive steps used is based on a translation of qualitative reasoning of the impacts of the policy options vis-à-vis the baseline scenario into quantitative percentages that are used to estimate in how far the policy options would contribute to an increase or decrease of:

- Number of citizens affected[143];
- Number of businesses affected;
- Compliance costs; and
- Costs stemming from administrative burden.

As a **first step** of the assessment of the policy options, we have carried out a qualitative analysis[144] regarding the potential impact of each element of each policy option:

- What does it mean in practice?
- What types of businesses would be affected? How would the number of affected businesses develop?
- Would these businesses incur (additional) compliance costs and/or costs stemming from administrative burden?
- Would these costs be reduced through the implementation of each element of the policy options?
- To what extent would the policy options contribute to achieving the policy objectives?

As a **second step**, we have attributed to the answers to each of these questions for each element of the policy options a quantitative rating / colour coding. The purpose of this rating

[142] There is no explicit methodology to assess the impact on administrations and other economic impact, we have not drafted separate chapters for this.

[143] The number of citizens is a key component of our estimates although it is not subject to change under the policy options (as presented in the main body of the report). The reason why for still keeping this estimate is that it shows that although POs may be introduced, privacy threats to citizens will still exist in the future as the POs change the set-up of how they are dealt with – but do not solve the issue that citizens may be subject to privacy breaches.

[144] As presented above and in the main body of the report, we have used a standard rating scale from -3 to +3 so indeed the ratings are comparable amongst the policy options for each criterion. The criteria itself are naturally not fully comparable with each other (e.g. effectiveness vs. efficiency). The ratings of specific (elements of the) POs are provided in the respective tables in the main body of the report. The main body of the report also provides comparative tables of the POs.

is to compare the magnitude of the impacts on businesses towards each other and to provide the basis for the calculation of possible actual impacts. The rating, thus, provides the qualitative basis for the percentages presented in the previous section. The following scale has been applied:

Significant decrease (-3)	Medium decrease (-2)	Slight decrease (-1)	Neutral (0)	Slight increase (+1)	Medium increase (+2)	Significant increase (+3)

Source: Deloitte

The specific ratings for each element can be found in the coloured cells in each of the tables in the section on the qualitative reasoning.

The scale should be read from left to right: A significant decrease of costs being colour coded green and a significant increase of costs stemming from each element of the policy options being coloured red. The figures in each box represent the quantitative value attributed to each of the ratings with the most negative value having received a -3 and the most positive a +3.

As a **third step**, we have summed up the ratings for each specific element of each policy option in order to provide an overall rating. The overall ratings can be found in the individual assessment tables in chapter 9 of the main body of the report.

The impact of each of the policy options on the number of citizens affected is expected to be 0 as all citizens are affected who use electronic (or online) communication services and/or surf on the internet in general. These citizens are either affected positively (e.g. benefitting from higher privacy standards) or negatively (e.g. if companies are not compliant). This is not changed by any of the policy options: although some of the policy options change the scope in relation to the types of services covered, it is expected that users of online services are also covered under the current situation e.g. as holders of fixed line, mobile phone or internet contracts.[145]

As these qualitative overall ratings of the impacts of the policy options on the number of businesses affected, their compliance costs, and costs stemming from administrative burden are not suitable to estimate in quantitative terms the impact of the policy options, we have used a *hinge (or translation factor, see below).*

This means that, as a **fourth step**, we have translated the qualitative overall ratings of the impacts of the policy options into quantitative percentages. The percentages represent the impact of the policy options in quantitative terms, i.e. how much a given policy option would increase / reduce the number of businesses affected, their compliance costs, and costs stemming from administrative burden. Such a step is a pragmatic means to cope with the general lack of quantitative evidence concerning the impact of (hypothetical, theoretical) policy options on businesses in the future.

Each qualitative overall rating has been translated into a minimum and maximum percentage by means of a simple multiplication with a so-called translation factor. This translation factor has been set ad hoc, based on expert prior experience. It has been chosen as the most

[145] The number of citizens "potentially" affected is always the same across all policy options, as it can always be that – although there are measures in place – citizens are affected by privacy breaches. the question is about the group that is potentially affected, not those that are actually affected (in case of citizens e.g. those that suffer from privacy breaches and in case of businesses those that could actually exploit data for their own purposes).

reasonable to be applied in this case, in light of the subject matter and the type of findings that had to be analysed in this impact assessment. Thus, the translation factor ranges from 0.01 (minimum) to 0.05 (maximum). Hence, if a policy option has for example an overall rating of "+3", the minimum value would be "3%" while maximum value would be "15%", which means for example the compliance costs would rise by a 15%.

The most likely *actual* impact of the policy options is expected to be somewhere within the minimum and maximum value.

Given the specific ratings above, the maximum "translation factor" can mathematically not exceed 0.9 because this would translate the rating concerning the compliance costs under policy option 4 to already 99%. If this policy option was not ranked positively but negatively, for instance -11, the translation factor would result in a decrease of costs by 99%. This can only be exceeded by the total repeal of the ePD – which is the "natural boundary" of impacts. A decrease of compliance costs of more than 100% is logically not possible because it would mean that businesses would not only have less cost but in addition "win something". This is not in line with economic theory.

Therefore, we have used 0.05 as maximum translation factor because it is actually a quite moderate, reasonable, and balanced value. In fact, 0.05 is the median value between 0.01 and 0.09.

The use of a standardised translation factor makes the impacts of the policy options comparable vis-à-vis the baseline scenario, as well as towards each other. Thus, the translation factor is a pragmatic means to cope with the general lack of quantitative evidence concerning the impact of (hypothetical, theoretical) policy options on businesses in the future.

The impact of each of the policy options on the number of citizens affected is expected to be 0%, as explained above. Policy option 5, i.e. the total repeal of the ePD is expected to reduce the number of businesses affected, their compliance costs, and their costs stemming from administrative burden to zero.

The relationship between the percentages presented above represents the expected magnitude of the impact of the different policy options. This means that policy options that have a bigger impact also have a higher (or lower in case of negative impact) percentage. It is important to keep in mind that these assumptions are mainly based on expert judgement, as it was generally challenging to substantiate / validate these with stakeholders. The reasons for this are: (1) Businesses and business associations are focused on the "now". This means that they usually do not have quantitative information on policy options which, to them, are hypothetical scenarios that do not (yet) have a direct effect on their daily operations; (2) Businesses and business associations were able to provide qualitative, anecdotal evidence concerning their costs and how a specific policy option would impact on them. Such evidence has been used to develop the figures above. However, a direct one-to-one translation of qualitative evidence into quantitative estimates is not possible.

Below, we have provided a brief explanation of the assumptions.

- **Numbers of citizens affected**: The number of citizens affected depends on the usage rates of the services. For the baseline scenario, it is assumed that all citizens who use any of the services concerned (including fixed line or mobile phone as well as

internet) are potentially affected by the ePD. This is not changed by any of the policy options.

- **Numbers of businesses affected**: For the purpose of the economic analysis, the broadest group affected by the ePD (all businesses that have a website) was taken as a basis. It can be expected that under policy options 3 (at least scenarios 1&2) and 4, the number of businesses affected decreases due to the exceptions implemented under these policy options.
    - **Policy option 1:** This option does not entail any changes that impact on the number of businesses affected by the ePD.
    - **Policy option 2:** Although OTTs would apply additional provisions compared to the current situation, no significant impact on the overall number of businesses (i.e. those applying Article 5.3) is expected. At the same time, the clarification of the scope of the provision and make it technologically neutral may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to companies placing ads on social networks' personal spaces.
    - **Policy Option 3:** Based on the new exceptions, the website that use non-privacy invasive cookies would no longer be affected by the consent rule. Based on current statistics, this would lead to a 30% decrease. Depending on the development in relation to the use of cookies, the actual number could be slightly lower as well. An additional decrease is possible based on the possibility to introduce adequate safeguards. The magnitude of this impact is unknown, as it depends on the types of safeguards employed and the willingness of businesses to implement these. At the same time, Point 5(i) may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to advertisings on social networks' personal spaces.
    - **Policy option 4:** Based on the new exceptions, the website that use non-privacy invasive cookies would no longer be affected by the consent rule. Based on current statistics, this would lead to a 30% decrease. Depending on the development in relation to the use of cookies, the actual number could be slightly lower as well. An additional decrease is possible based on the possibility to introduce adequate safeguards. The magnitude of this impact is unknown, as it depends on the types of safeguards employed and the willingness of businesses to implement these. At the same time, Point 5(i) may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to advertisings on social networks' personal spaces.
    - **Policy option 5:** No business would be affected by the ePD anymore as it would be repealed entirely.
- **Compliance costs**: In relation to policy options 1 and 2, the compliance costs would slightly increase compared to the baseline scenario. Option 1 entails the participation of industry as part of self-regulatory initiatives. Option 2 would entail some compliance costs based on the fact that the scope of some provisions would be broadened to OTTs and the fact that it includes some new costs, including e.g. in relation to unsolicited communications. At the same time, some savings would occur

partially countering these additional costs. Under policy option 3, compliance costs are expected to decrease compared to the baseline scenario. Although there would also be some new costs, the options entail savings that are overall higher than the new costs. In particular, based on the exceptions introduced in relation to the consent rule, the number of businesses affected by the ePD is expected to decrease significantly. Furthermore, the policy option introduces some simplifications. The magnitude of the savings depends on the solution chosen in relation to the management of users' consent. The savings would be highest if consent would be solely managed via the browsers and lowest if consent would still be managed via individual websites. Under option 4, compliance costs are expected to increase due to the extension of the scope of the ePrivacy to OTTs, as well as explicitly prohibiting the practice of denying access to a website or an online service in case users do not provide consent to tracking. The prohibition of denying access to a website/service in case users do not consent to tracking will lead to an increase of IT costs for businesses. Businesses will need to amend their websites/services so that they are also available to the extent possible without the use of cookies. Under policy option 5, no compliance costs would ensue for businesses from the ePD anymore as it would be repealed entirely.

- **Administrative burden**: In the current situation, the main cost factors in relation in administrative burden relate to personal data breach notifications under Article 4 as well as the preparation for / dealing with audits by competent authorities. Option 1 does not affect these aspects. Options 2 and 3 both entail the deletion of the provision on personal data breach notifications. As this is one of the main cost factors (in some Member States applying to more companies than audits), a significant decrease of costs may be expected. Option 4 would also contribute to decreasing cost from administrative burden. Option 5 would remove the costs stemming from administrative burden in its entirety.

As a **fifth step**, for each of the ranges, we have indicated which "end of the range" is more likely to provide a picture of the actual, real-life value. The following assumptions were made based on expert judgment:

Table 5 –Qualitative assessment of the plausibility of the quantitative estimates

	Policy Option 1		Policy Option 2		Policy Option 3						Policy Option 4		Policy Option 5	
					Scenario 1		Scenario 2		Scenario 3					
Provision	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**
Number of citizens affected	X		X		X		X		X		X		X	
Number of businesses affected		X	X			X		X		X	X		X	
Compliance costs		X		X		X		X		X		X	X	
Costs stemming from administrative burden	X			X		X	X		X		X		X	

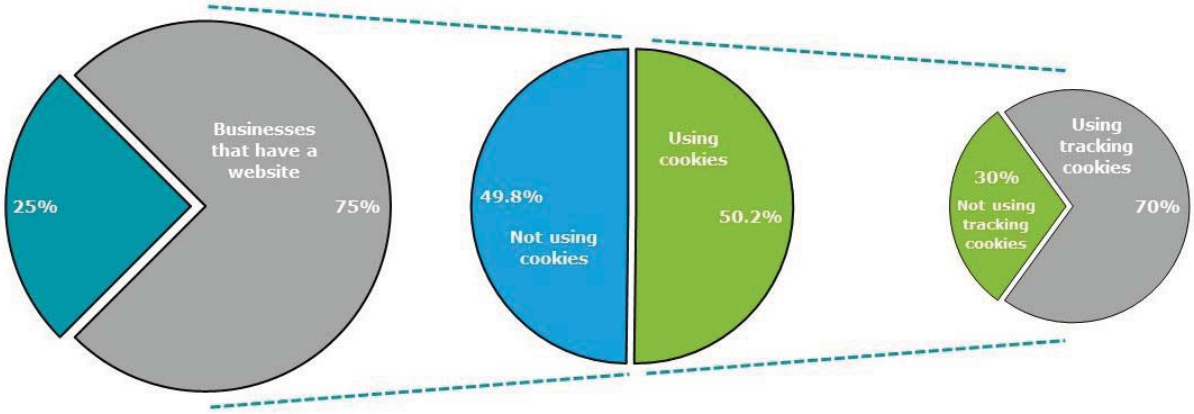
Source: Deloitte

As a **sixth and final step**, we have multiplied each of the selected percentages with the values estimated based on the "basic assumptions" (see previous section) per year (2016-2030), per Member State, and per size class of business. In the following sub-section, we provide the qualitative reasoning behind the quantitative assessments of the impacts of the policy options on businesses

1. Basic considerations concerning the share of websites potentially affected

Even before assessing the impacts of the policy options vis-à-vis the baseline scenario in both qualitative and quantitative terms, it is necessary to reflect what the basic population of businesses is on which the policy options can impact, as well as what the magnitude of the impacts on the number of businesses and their costs could be in theory. The basic population is visualised below.

Figure 1 – Basic population which the policy options can impact



Source: Deloitte

The figure above shows that the number of businesses that have a website (in this case e.g. 75%) is the basis for the estimates. Half of these websites (50.2%) use cookies, while the other half does not use cookies (49.8%). Only the former is relevant for the quantitative assessment of the policy options. Of the websites that use cookies, 70% use tracking cookies, while 30% do not use tracking cookies. The elements of the policy options relating to exceptions of the cookie consent rule under Art. 5(3) would, compared to the baseline situation, free those 30% of businesses from having to implement a cookie banner.

Possible technical solutions to collect the consent of the users

There are different potential technical solutions to facilitate users to diverge from their default setting for individual websites, all with different implications on costs. The following scenarios exist: (1) All communication runs centralised via the browsers; (2) The party placing the cookie is responsible for asking the consent; (3) Individual websites are responsible for asking the consent.

The impact of the policy options on the remaining 70% (see above) depends on the specific solution implemented e.g. under policy option 3:

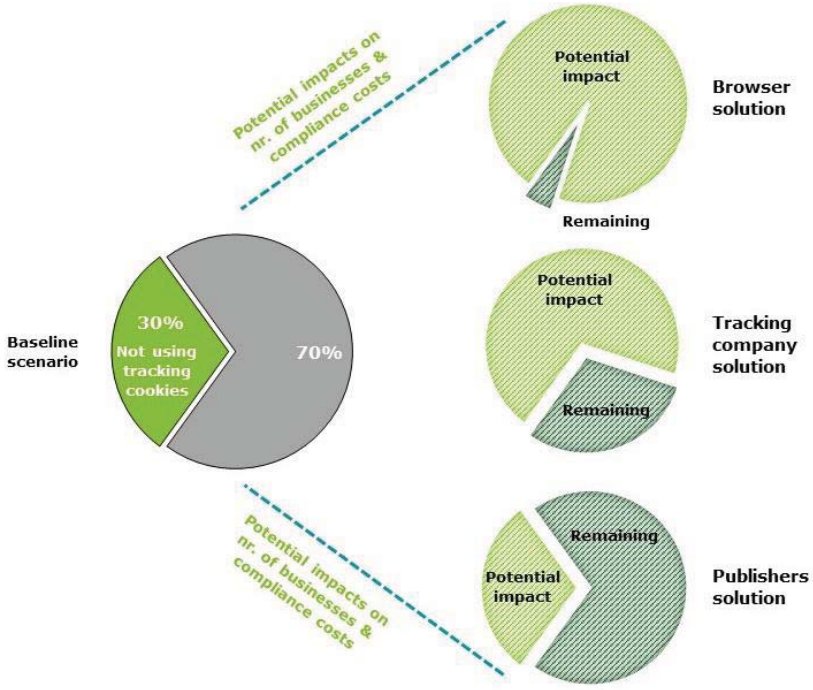
- *Scenario 1 ("Browser solution"):* Assuming that the communication would exclusively run via the browsers, all the costs would lie with the browser providers (as

reflected above). Websites on the other hand, would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses, this would be a significant decrease.

- *Scenario 2 ("Tracking company solution"):* In this scenario, the costs would lie with the companies placing the data. It is expected that this would be slightly more expensive compared to solution 1, as a higher number of businesses would be concerned. Although most tracking cookies are placed by few main players, other smaller players will be affected as well. Furthermore, this solution would require the development of new practical and technical solutions to implement the option. Websites would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses with the ePD, this would be a significant decrease.
- *Scenario 3 ("Publishers solution"):* In this case, there would be no significant changes for website operators, as they would in principle still employ cookie banners (or a similar technical solution).

This is depicted in the figure below.

Figure 2 – Potential magnitude of impacts of the scenarios under policy option 3



Source: Deloitte

It can be seen from the figure above that, in theory, it is expected that the "browser solution" would be able to free up most businesses from costs (the light green part of the pie chart at the top is largest) while costs are imposed on a small number of browser operators. In addition, a limited number of businesses would also incur "some" costs under this scenario. As part of the "tracking company solution", impacts on the number of businesses and compliance costs are also expected to be large, but less pronounced than under the "browser solution". The number of businesses that would still incur costs (i.e. "remain") would be a bit larger than

under the “browser solution". Finally, the “publishers solution” is not expected to be *game changer* compared to the baseline situation as only the websites that do not use tracking cookies in the baseline scenario would be exempted under the ePD.

Key findings of the quantitative analysis: Average values over time

In this section, the policy options are compared against the baseline scenario.

As a first step, the main quantitative outcomes of the economic analysis are presented in the form of tables. This section will contain separate tables concerning:

- Average annual values;
- Absolute changes of the average annual value compared to the REFIT / baseline scenario; and
- Relative changes of the average annual value compared to the REFIT / baseline scenario.

This section contains the average values for the quantitative indicators:

- The number of businesses affected;
- Compliance costs, incl. average compliance costs per business; and
- Administrative burden, incl. average costs from admin. burden per business.

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

As a second step, the results are compared against the baseline scenario in the form of charts in order to be able to spot clearly the different impacts of the policy options compared to the baseline scenario.

A sub-section is devoted to each of the above quantitative indicators. Within each sub-section, different figures are provided in relation to: Micro-enterprises; SMEs; large enterprises; foreign controlled enterprises; and all businesses (i.e. the sum of the aforementioned).

In relation to policy option 3, only the “browser solution” has been visualised.

The number of citizens affected by the ePD under each policy option is not compared with the baseline scenario. The reason for this is that the policy options have no impact on the number of citizens affected – both are independent from each other. This means that, under each policy option, the number of citizens affected is equal to the baseline scenario.

Table 6 – Key figures of the quantitative assessments concerning businesses (absolute values)

Average annual value	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3[146]			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	2.84	3.11	3.70	3.70	3.89	0.19	0.74	2.22	0.37	0.00
Micro-enterprises	2.53	2.78	3.31	3.31	3.48	0.17	0.663	1.99	0.33	0.00
SMEs	0.26	0.25	0.26	0.26	0.27	0.01	0.052	0.16	0.03	0.00
Large enterprises	0.01	0.01	0.01	0.01	0.01	0.00	0.002	0.01	0.001	0.00
Foreign controlled enterprises	0.05	0.06	0.12	0.12	0.13	0.01	0.024	0.07	0.01	0.00
Compliance costs (in million Euro)	1,861.7 €	1,505.7 €	1,355.4 €	1,423.15	1,558.7 €	406.6 €	542.152	1,287.6 €	1,287.6 €	0.0 €
Micro-enterprises	1,655.8 €	1,349.0 €	1,213.0 €	1,273.6 €	1,394.9 €	363.9 €	485.188	1,152.3 €	1,152.3 €	0.0 €
SMEs	169.8 €	122.2 €	97.0 €	101.9 €	111.6 €	29.1 €	38.808	92.2 €	92.2 €	0.0 €
Large enterprises	5.6 €	4.2 €	3.3 €	3.5 €	3.8 €	1.0 €	1.332	3.2 €	3.2 €	0.0 €
Foreign controlled enterprises	30.5 €	30.3 €	42.1 €	44.2 €	48.4 €	12.6 €	16.823	40.0 €	40.0 €	0.0 €
Average compliance cost per business (in Euro)	658.4 €	484.5 €	373.5 €	392.2 €	409.1 €	2,240.9 €	746.978	591.4 €	3,548.1 €	0.0 €
Administrative burden (in million Euro)	0.28 €	0.23 €	0.23 €	0.23 €	0.21 €	0.208 €	0.226 €	0.23 €	0.22 €	0.00 €
Micro-enterprises	0.23 €	0.19 €	0.18 €	0.18 €	0.16 €	0.163 €	0.178 €	0.18 €	0.18 €	0.00 €
SMEs	0.03 €	0.03 €	0.03 €	0.03 €	0.03 €	0.031 €	0.033 €	0.03 €	0.03 €	0.00 €
Large enterprises	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €	0.002 €	0.002 €	0.00 €	0.00 €	0.00 €
Foreign controlled enterprises	0.02 €	0.01 €	0.01 €	0.01 €	0.01 €	0.013 €	0.014 €	0.01 €	0.01 €	0.00 €
Average costs from admin. burden per business (in Euro)	48.9 €	36.0 €	27.8 €	28.0 €	23.8 €	499.5 €	135.982 €	45.33 €	269.2 €	0.0 €

Source: Deloitte

[146] As part of this model, it was not possible to estimate reasonable average compliance costs and costs from administrative burden for businesses for the "browser" and the "tracking companies solution" of policy option 3. The reason for this is that the average costs are calculated on the basis of all businesses affected, i.e. also those that would incur higher costs than others and vice versa. As part of these two solutions, however, a very small share of businesses would have to bear the largest share of costs (i.e. browser operators and tracking companies) while the costs would be significantly lower for others. Therefore, it is not appropriate to indicate an "average amount per business" as this would return misleading estimates.

Table 7 – Key figures of the quantitative assessments concerning businesses (absolute changes)

Absolute changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	n/a	n/a	0.86	0.00	0.19	-3.52	-2.96	-1.48	-3.33	-3.70
Micro-enterprises	n/a	n/a	0.78	0.00	0.17	-3.15	-2.65	-1.33	-2.98	-3.31
SMEs	n/a	n/a	0.00	0.00	0.01	-0.25	-0.21	-0.10	-0.24	-0.26
Large enterprises	n/a	n/a	0.00	0.00	0.00	-0.01	-0.01	0.00	-0.01	-0.01
Foreign controlled enterprises	n/a	n/a	0.07	0.00	0.01	-0.12	-0.10	-0.05	-0.11	-0.12
Compliance costs (in million Euro)	n/a	n/a	-506.3 €	67.8 €	203.3 €	-948.8 €	-813.2 €	-67.8 €	-67.8 €	-1,355.4 €
Micro-enterprises	n/a	n/a	-442.8 €	60.6 €	181.9 €	-849.1 €	-727.8 €	-60.6 €	-60.6 €	-1,213.0 €
SMEs	n/a	n/a	-72.8 €	4.9 €	14.6 €	-67.9 €	-58.2 €	-4.9 €	-4.9 €	-97.0 €
Large enterprises	n/a	n/a	-2.3 €	0.2 €	0.5 €	-2.3 €	-2.0 €	-0.2 €	-0.2 €	-3.3 €
Foreign controlled enterprises	n/a	n/a	11.6 €	2.1 €	6.3 €	-29.4 €	-25.2 €	-2.1 €	-2.1 €	-42.1 €
Average compliance cost per business (in Euro)	n/a	n/a	-284.9 €	18.7 €	35.6 €	1,867.4 €	373.5 €	217.9 €	3,174.7 €	-373.5 €
Administrative burden (in million Euro)	n/a	n/a	-0.04 €	0.002 €	-0.02 €	-0.023 €	-0.005 €	-0.005 €	-0.007 €	-0.23 €
Micro-enterprises	n/a	n/a	-0.05 €	0.002 €	-0.02 €	-0.018 €	-0.003 €	-0.004 €	-0.006 €	-0.18 €
SMEs	n/	n/	0.01 €	0.000 €	0.00 €	-0.003 €	-0.001 €	-0.001 €	-0.001 €	-0.03 €
Large enterprises	n/a	n/a	0.00 €	0.000 €	0.00 €	0.000 €	0.000 €	0.000 €	0.000 €	0.00 €
Foreign controlled enterprises	n/a	n/a	0.00 €	0.000 €	0.00 €	-0.001 €	0.000 €	0.000 €	0.000 €	-0.01 €
Average costs from admin. burden per business (in Euro)	n/a	n/a	-21.2 €	0.278 €	-4.0 €	471.8 €	108.2 €	17.6 €	241.4 €	-27.8 €

Source: Deloitte

Table 8 – Key figures of the quantitative assessments concerning businesses (relative changes)

Relative changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	n/a	n/a	30.2%	0.0%	5.0%	-95.0%	-80.0%	-40.0%	-90.0%	-100.0%
Micro-enterprises	n/a	n/a	30.9%	0.0%	5.0%	-95.0%	-80.0%	-40.0%	-90.0%	-100.0%

Relative changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
SMEs	n/a	n/a	1.6%	0.0%	5.0%	-95.0%	-80.1%	-39.8%	-90.0%	-100.0%
Large enterprises	n/a	n/a	0.0%	0.0%	0.0%	-100.0%	-77.8%	-44.4%	-88.9%	-100.0%
Foreign controlled enterprises	n/a	n/a	157.4%	0.0%	5.0%	-95.0%	-80.2%	-40.5%	-90.1%	-100.0%
Compliance costs (in million Euro)	n/a	n/a	-27.2%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Micro-enterprises	n/a	n/a	-26.7%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
SMEs	n/a	n/a	-42.9%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Large enterprises	n/a	n/a	-40.9%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Foreign controlled enterprises	n/a	n/a	38.0%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Average compliance cost per business (in Euro)	n/a	n/a	-43.3%	5.0%	9.5%	500.0%	100.0%	58.3%	850.0%	-100.0%
Administrative burden (in million Euro)	n/a	n/a	-16.0%	0.9%	-10.0%	-10.0%	-2.2%	-2.2%	-3.0%	-100.0%
Micro-enterprises	n/a	n/a	-21.3%	1.1%	-9.9%	-9.9%	-1.7%	-2.2%	-3.3%	-100.0%
SMEs	n/	n/	25.9%	0.0%	-8.8%	-8.8%	-2.9%	-2.9%	-2.9%	-100.0%
Large enterprises	n/a	n/a	-33.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	-100.0%
Foreign controlled enterprises	n/a	n/a	-6.7%	0.0%	-7.1%	-7.1%	0.0%	0.0%	0.0%	-100.0%
Average costs from admin. burden per business (in Euro)	n/a	n/a	-43.3%	1.0%	-14.3%	1700.0%	390.0%	63.3%	870.0%	-100.0%

Source: Deloitte

ANNEX 9: COVERAGE OF OTTS WITHIN THE SCOPE OF NATIONAL IMPLEMENTING LEGISLATION

The interpretation and implementation of the scope varies across Member States. Indeed, some Member States have extended the ePD provisions to OTT services. Spain, UK, Austria, France, Estonia, Croatia, Finland, Denmark, Latvia, Norway, The Netherlands, Germany and Spain consider VoIP with access to telephone number an electronic communications service[147]. To the contrary, peer-peer VoIP does not constitute the said service by the countries previously mentioned. In the Czech Republic VoIP communication is considered an electronic communications service solely in cases where the communication is secured by a third party (external) provider within the scope of such provider's business. The German competent authority explained that they consider the scope of the ePD to be unclear in this respect[148].

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Austria	X			
Belgium				X
Bulgaria	X			
Croatia				X
Cyprus				X
Czech Republic		X		
Denmark				X
Estonia		X		
Finland				X
France	X			
Germany			X	
Greece	X			
Hungary				X
Ireland		X		
Italy			X	
Latvia	X			
Lithuania				X
Luxembourg		X		
Malta				X
Netherlands		X		
Poland		X		
Portugal		X		
Romania		X		
Slovakia		X		

[147] Swedish Post and Telecom Agency (PTS), "Which services and networks are subject to the Electronic Communications Act", guidance, 11 March 2009, Stockholm, p. 16.
[148] *Source: Deloitte (SMART 2016/0080).*

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Slovenia	**X**			
Spain	**X**			
Sweden				**X**
UK				**X**
Overall	**7**	**9**	**2**	**10**

Source: Deloitte (SMART 2016/0080) – Transposition check

ANNEX 10: OPT-IN AND OPT-OUT REGIMES PER MEMBER STATE

The table below further illustrates the wide diversity of regimes on unsolicited communications calls (with human intervention) and the fragmentation of the rules in the EU. The table shows that in relation to fixed-line phones, 24% of EU businesses currently are governed by an opt-in regime while the share is 52% in relation to mobile phones[149]. By contrast, 88% of EU businesses are currently governed by an opt-out regime in relation fixed-line phones while 61% are governed by an opt-in regime.[150]

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Austria	321,661	X		X	
Belgium	593,421		X	X	
Bulgaria	319,856	X		X	
Croatia	147,337		X		X
Cyprus	46,938	X		X	
Czech Republic	995,754		X		X
Denmark	212,740	X[1]	X[2]	X[1]	X[2]
Estonia	64,040		X		X
Finland	229,248		X		X
France	3,188,138		X	X	
Germany	2,193,135	X[1]	X[3]	X[1]	X[3]
Greece	700,166		X		X
Hungary	514,537	X		X	
Ireland	146,741		X	X	
Italy	3,715,164		X		X
Latvia	100,491	X		X	
Lithuania	174,611	X		X	
Luxembourg	31,385	X		X	
Malta	26,193		X		X
Netherlands	1,054,562		X		X
Poland	1,549,326		X		X
Portugal	781,823	X		X	
Romania	455,852	X		X	
Slovakia	400,683	X[1]	X[3]	X[1]	X[3]
Slovenia	130,088		X		X
Spain	2,377,191		X	X	
Sweden	673,218		X		X

[149] The sum of the percentages is higher than 100%, as traders is some countries (Denmark, Germany, Slovakia) are subject to both opt-in and opt-out, depending on the type of addressee (e.g., natural or legal persons).

[150] *Source: European Commission, tabulation by Deloitte (SMART 2016/0080) [1]For 'consumers'; [2]For 'businesses'; [3]For 'other market players'. Statistical data from taken from Eurostat (most recent data from 2014). Some exceptions apply to the opt-in consent rule for consumers in Denmark.*

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
United Kingdom	1,841,715		X		X
		12	19	16	15
Number / share of businesses affected	22,986,014	5,553,712	20,238,860	11,859,203	13,933,369
		24%	88%	52%	61%

ANNEX 11: TABLE OF COMPETENT AUTHORITIES

The enforcement of the ePD provisions at national level is entrusted to a "*competent national authority*" (Article 15a of the ePD), without further defining that authority or body. This has led to a fragmented situation in the EU and within Member States. Member States have allocated the competence to DPAs, telecom NRAs, to another type of body (e.g. consumer protection bodies) or to several different bodies within the same country.

The table below shows that not only competence for the ePD is scattered over several authorities, but that competence can even be scattered per article. For Article 13, in 11 Member States the DPA has sole competence, in 1 Member States the consumer agency has sole competence and in 4 Member States the NRA and DPA share competence. In the remaining Member States other combinations of authorities, up to five different ones, have competence on Article 13. Article 13 stands as an example for the distribution of competences for the other ePD articles.

The current situation in which several authorities can be in charge of the ePD and several authorities can be in charge of one article causes several risks:

- The risk of having several interpretations of ePD provisions within one Member State. The different competent authorities may have different views and use different enforcement strategies;

- The risk of duplication of enforcement powers of the same article, which is detrimental for consumers. It may be difficult to single out the enforcers to complain to and the risk exists they are send back and forth between authorities.

Above is multiplied when you take it to a European level.

Moreover, there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD: indeed, DPAs meet through the Article 29 Working Party, NRAs through BEREC. Some consumer bodies meet through the Consumer Protection Cooperation (CPC) network.

Country	Article 5	Articles 6 & 9	Article 13
Austria	NRA Telecom office	NRA Telecom office	NRA Telecom office DPA
Belgium	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector DPA	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector Ministry for Economy DPA
Bulgaria	NRA DPA Commission for	NRA Commission for Consumer Protection	NRA Commission for Consumer Protection

Country	Article 5	Articles 6 & 9	Article 13
	Consumer Protection		DPA
Croatia	NRA DPA	NRA DPA	NRA DPA Ministry for Economic Affairs Ministry of Finance
Cyprus	NRA DPA	NRA DPA	NRA DPA
Czech Republic	DPA	DPA	DPA
Denmark	DPA	The Telecommunications Complaints Board	Competition and Consumer Authority Consumer Ombudsman
Estonia	NRA	NRA	DPA
Finland	NRA	DPA	DPA
France	DPA NRA	DPA NRA	DPA NRA Ministry for Economic Affairs
Germany	DPA NRA Data Protection Commissioners of the German Lands (for art. 5.3)	DPA NRA	DPA NRA
Greece	DPA NRA	DPA NRA	DPA NRA
Hungary	DPA NRA (except 5(3))	DPA NRA	NRA DPA Consumer Protection Inspectorates / National Authority
Ireland	DPA	DPA NRA	DPA
Italy	DPA	DPA	DPA
Latvia	Ministry of Transport NRA DPA - 5(3)	Ministry of Transport DPA	Ministry of Transport DPA Consumer Protection Authority

Country	Article 5	Articles 6 & 9	Article 13
Lituania	DPA	DPA	DPA
Luxembourg	DPA	DPA	DPA
Malta	DPA	DPA	DPA
The Netherlands	Consumer Protection Authority DPA NRA (5(1))	DPA NRA	Consumer Protection Authority DPA
Poland	DPA NRA	DPA NRA	DPA Office of Competition and Consumer Protection NRA
Portugal	DPA NRA (5(1))	DPA	DPA
Romania	DPA	DPA	DPA
Slovakia	Ministry of Transport NRA Ministry of Finance (5(3))	Ministry of Transport NRA	Ministry of Transport NRA
Slovenia	NRA	NRA DPA	NRA Market Inspectorate
Spain	DPA	DPA	DPA
Sweden	NRA	NRA	Consumer Agency
UK	NRA DPA	NRA DPA	NRA DPA Financial Authority

Source: on the basis of European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080).

ANNEX 12: MAPPING OF THE POLICY OPTIONS

I.Table: Summary overview of Policy Options

	Policy Option 1 Soft law measures	**Policy Option 2** Limited reinforcement of privacy and harmonisation	**Policy Option 3** Measured reinforcement of privacy and harmonisation	**Policy Option 4** Far-reaching reinforcement of privacy and harmonisation	**Policy Option 5** Repeal of the ePD
Objective 1 - *Ensuring effective confidentiality of electronic communications*	1. **Increased use of interpretative communications**. 2. **Support EU-wide self-regulatory initiatives** 3. **Specify privacy by design requirements of terminal electronic equipment through EU standards**. 4. **Research and awareness-raising activities**.	1. **Extension of the scope** of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP. 2. Clarify that the ePD applies to communication running over **publicly available communications networks**, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. 3. Specify that confidentiality rules, including of terminal equipment, apply to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator	1. Measures 1 to 3 of Option 2. 2. The new instrument would propose a technology neutral definition of electronic communications, encompassing all the additional elements under **Option 2** (1, 2 and 3). 3. On the subject of confidentiality of terminal equipment and tracking of online behaviour the envisaged	1. All the measures under No 1, 2, 3 and 4 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).	1. The GDPR provides for reinforced rights of individuals and the obligations of data controllers, which are in keeping up 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

		connected to a grocery store web site).	proposal would reformulate and simplify the "cookie" centred approach in favour of a technology neutral approach applying to all forms of tracking of (or other interference with) users' 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. The proposal would require certain software providers that support a terminal equipment basic functions (e.g. Internet browsers and OSs) to provide their products with privacy friendly		unbalance of economic power between the controller and the processor, requesting that this aspect be taken into account in the assessment of the validity of consent. 2. The GDPR would guarantee more effective enforcement in view of the reinforced powers conferred on data protection authorities.

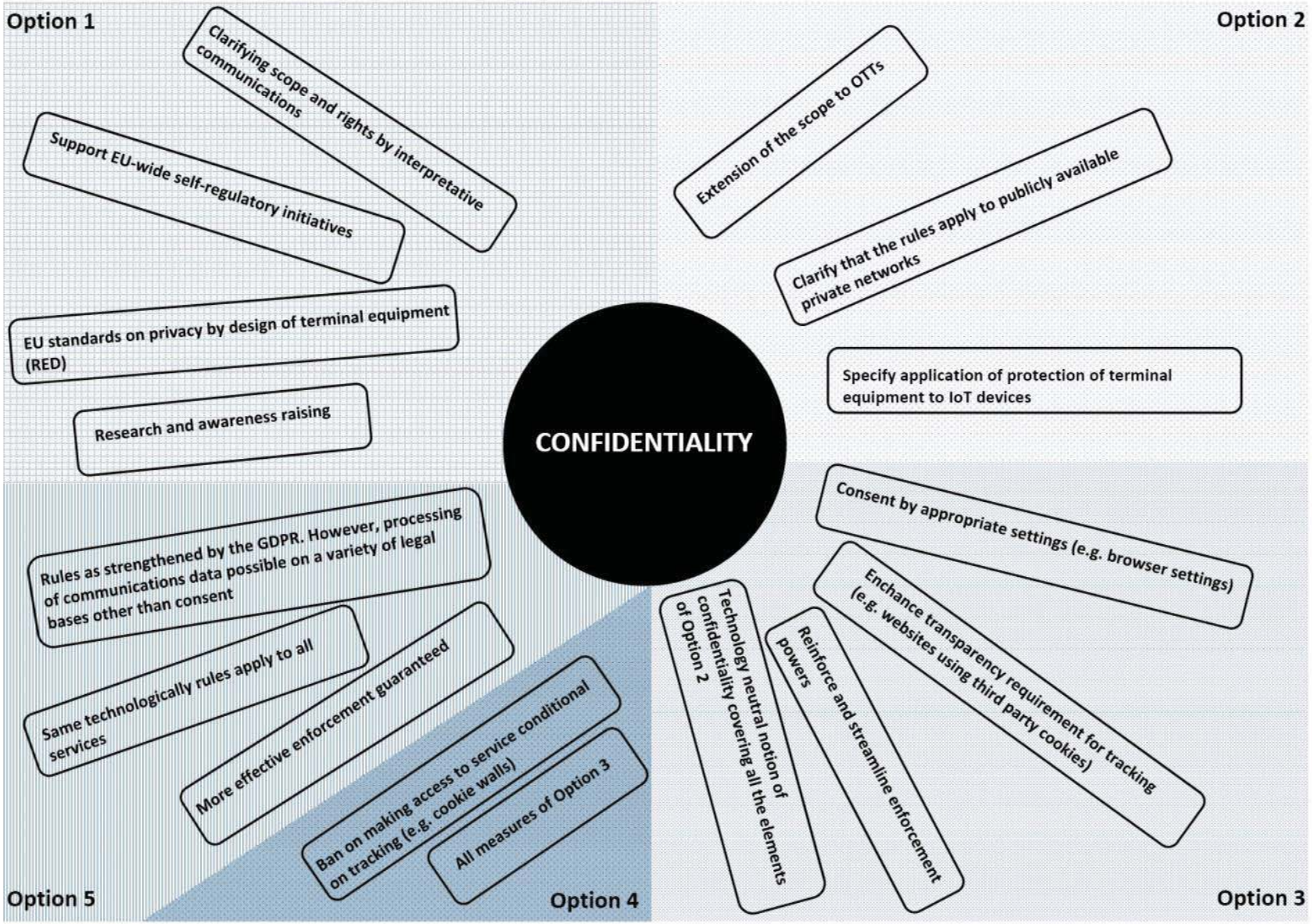
			settings as a means to provide consent and to reinforce user's control over online tracking and the over the flow of data from and into their terminal equipment. 4. Impose **enhanced transparency requirements** on entities processing communications data (e.g. websites, mobile apps and publicly available Wi-Fi private networks). 5. **Reinforce and streamline enforcement powers**: The new instrument would entrust the application and enforcement of the provisions of the ePrivacy instrument to the same independent supervisory authorities		

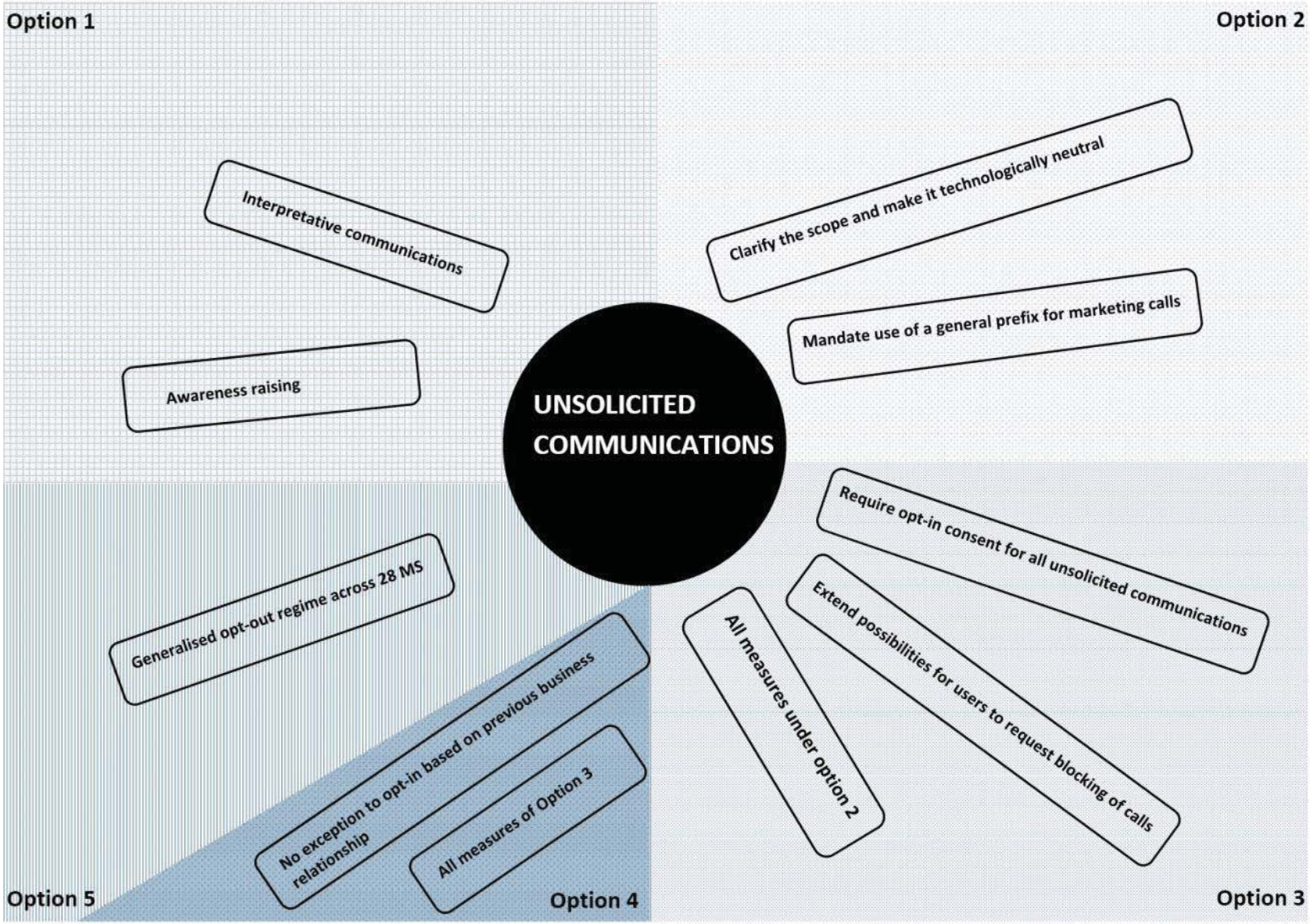
			appointed under the GDPR.		
Objective 2 - *Ensuring effective protection against unsolicited commercial communications*	1. **Interpretative communications**, clarifying the interpretation of unclear or ambiguous concepts. 2. **Awareness-raising initiatives** instructing citizens on how to defend themselves, how to seek redress from national supervisory authorities.	4. **Clarify the scope of the provision on unsolicited communications and make it technologically neutral**: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used (e.g. wallpapers, mailboxes, etc.). 5. **Require for marketing calls the use of a special prefix** distinguishing direct marketing calls from other calls.	6. All the measures from 4 to 5 under **Option 2**. 7. Require **opt-in consent for all types of unsolicited communications covered by the current rules**. 8. Clarify the provision on **presentation of calling line identification** to include the right of users to reject calls from specific numbers (or categories of numbers).	1. All the measures under No 6 and 7 of **Option 3**. **2.** Under this option, the Commission would **repeal** the provision allowing direct marketers to send communications to subscribers and users when they have received their contact details in the context of a **previous business relationship**	**3.** Unsolicited communications would be essentially regulated under a general **opt-out** regime across 28 MS
Objective 3 - *Enhancing harmonisation and simplifying/updating the legal framework*	3. Issue **interpretative communications** to promote an application of the current rules,	6. **Reinforce cooperation obligations** among the competent authorities, including for cross-border enforcement. Under this option, the Commission	8. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions**	13. Measures under No 8, 9, 10, 11 and 12 of Option 3. 14. Introduce	1. All providers of electronic communications will be subject to the **same rules** without

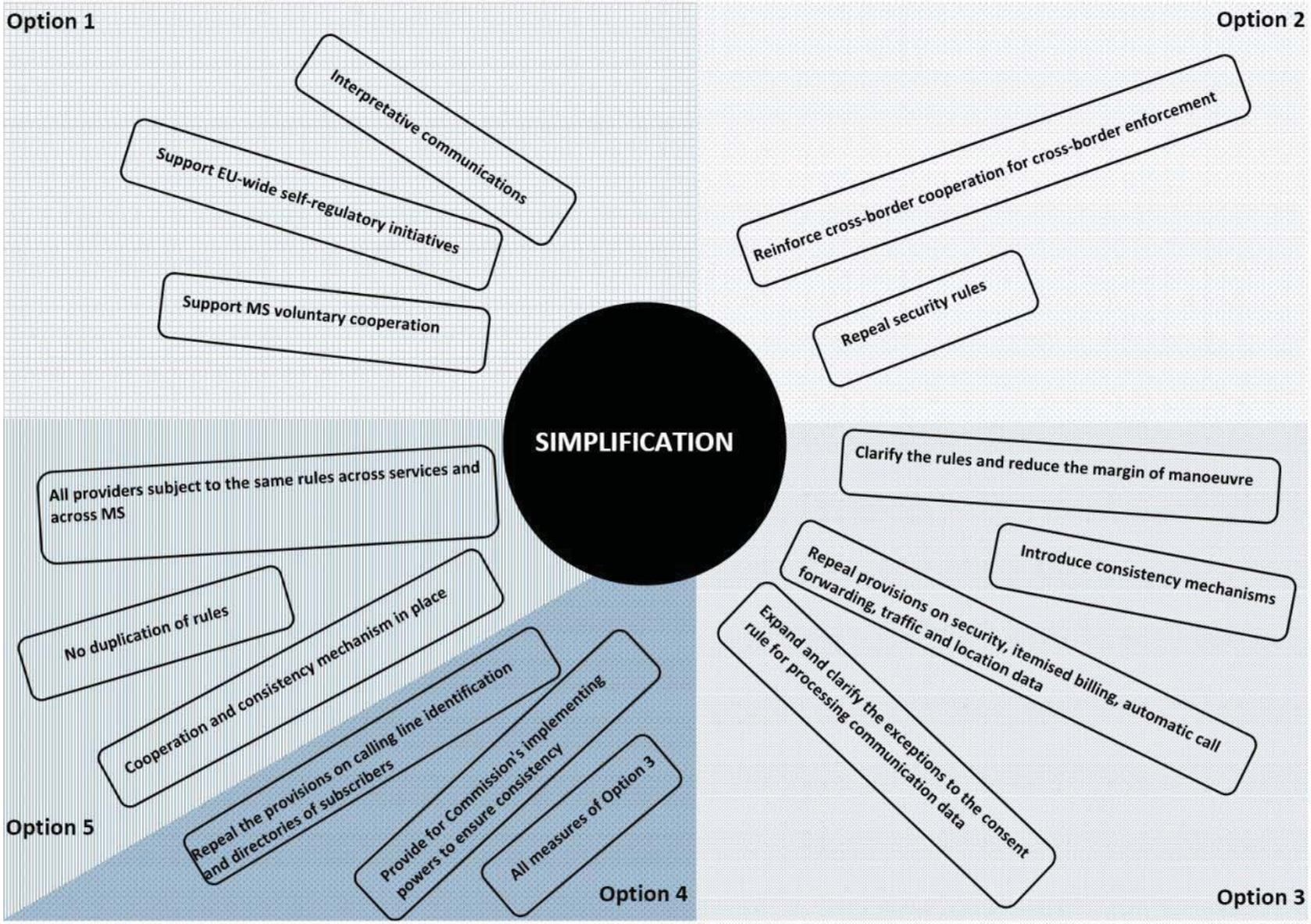
	which is business friendly, while preserving the essence of the protection of confidentiality of communications 4. Work closely with **industry** in order to encourage the adoption of **common best practices**. 5. **Support MS cooperation** to improve enforcement in cross-border cases as well as harmonised interpretation by organising meetings and workshops with authorities	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. The sole exception would be the rules on notification of users of security risks, which is indeed not covered by the latter instruments.	identified by stakeholders as a source of confusion and legal uncertainty. This will be achieved e.g. by regulating applicable law and territorial scope, clarifying the scope of the provisions concerning confidentiality of communications, the scope and requirements concerning confidentiality of terminal equipment and the rules on unsolicited advertising. 9. Extend the application of the consistency mechanism established under the GDPR to the ePrivacy instrument. 10. Repeal provisions on **security** and the provisions on	Commission's implementing powers for deciding on the correct application of the ePrivacy rules. order to ensure correct and consistent application of the EU law.	discrimination based on the technology used. 2. There would be no duplication of rules in the security area and all the ePD provisions related to specific issues in the electronic communications sector (e.g. directories of subscribers) would be dealt with on the basis of the general data protection rules.

			itemised billing. 11. Repeal the provisions on **traffic data and location data.** The processing of traffic and location data will be regulated under the general provision of confidentiality of communications data. 12. Specify that service providers can only process communications data with the consent of the users. Providing for **additional/broadened exceptions** to the consent and enhanced transparency rules for specific purposes which give rise to little or no privacy risks.		

II.Visualisation of the various elements of the policy options in relation to the specific objectives


Option 1
Clarifying scope and rights by interpretative communications
Support EU-wide self-regulatory initiatives
EU standards on privacy by design of terminal equipment (RED)
Research and awareness raising
Option 2
Extension of the scope to OTTs
Clarify that the rules apply to publicly available private networks
Specify application of protection of terminal equipment to IoT devices
CONFIDENTIALITY
Option 5
Rules as strengthened by the GDPR. However, processing of communications data possible on a variety of legal bases other than consent
Same technologically rules apply to all services
More effective enforcement guaranteed
Option 4
Ban on making access to service conditional on tracking (e.g. cookie walls)
All measures of Option 3
Option 3
Consent by appropriate settings (e.g. browser settings)
Enchance transparency requirement for tracking (e.g. websites using third party cookies)
Reinforce and streamline enforcement powers
Technology neutral notion of confidentiality covering all the elements of Option 2


Option 1
Option 2
Interpretative communications
Clarify the scope and make it technologically neutral
Mandate use of a general prefix for marketing calls
Awareness raising
UNSOLICITED COMMUNICATIONS
Require opt-in consent for all unsolicited communications
Extend possibilities for users to request blocking of calls
All measures under option 2
Generalised opt-out regime across 28 MS
No exception to opt-in based on previous business relationship
All measures of Option 3
Option 5
Option 4
Option 3


Option 1
Interpretative communications
Support EU-wide self-regulatory initiatives
Support MS voluntary cooperation
Option 2
Reinforce cross-border cooperation for cross-border enforcement
Repeal security rules
SIMPLIFICATION
All providers subject to the same rules across services and across MS
No duplication of rules
Cooperation and consistency mechanism in place
Repeal the provisions on calling line identification and directories of subscribers
Provide for Commission's implementing powers to ensure consistency
All measures of Option 3
Option 5
Option 4
Clarify the rules and reduce the margin of manoeuvre
Introduce consistency mechanisms
Repeal provisions on security, itemised billing, automatic call forwarding, traffic and location data
Expand and clarify the exceptions to the consent rule for processing communication data
Option 3

ANNEX 13: DETAILED COMPARISON OF POLICY OPTIONS

The following table reflects the assessment of the **effectiveness** policy options as per Section 6.1.1 of the impact assessment report.

Table 2: **Comparison of options in terms of effectiveness**

	Objective 1 - *Confidentiality*	**Objective 2 –** *Unsolicited communications*	**Objective 3 –** *Harmonisation/simplification*	**Total**
Option 0 -- *Baseline*	0	0	0	0
Option 1 – *Soft law*	✓	≈	✓	✓✓
Option 2 – *Limited reinforcement/harmonisation*	✓✓	✓	≈	✓✓✓
Option 3 – *Measured reinforcement/harmonisation*	✓✓	✓✓	✓✓	✓✓✓✓✓✓
Option 4 – *Far-reaching reinforcement/harmonisation*	✓✓✓	✓✓	✓✓✓	✓✓✓✓✓✓✓✓
Option 5 – *Repeal*	××	×	✓✓✓	≈

Effectiveness of the various policy options vis-à-vis the specific objectives, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact

The following table reflects the assessment of the **efficiency** of the policy options as per Section 6.1.2 of the impact assessment report.

Table 3: Comparison of options in terms of efficiency

	Compliance cost (incl. for public administration)	**Administrative burden**	**Opportunity Cost**	**Total**
Option 0 – *Baseline*	0	0	0	0
Option 1 – *Soft law*	×	n.a.	n.a.	×
Option 2 – *Limited reinforcement/harmonisation*	×	≈	××	×××
Option 3 – *Measured reinforcement/harmonisation*	✓✓✓	≈	××	✓

Option 4 – *Far-reaching reinforcement/harmonisation*	××	≈	×××	×××××
Option 5 – *Repeal*	n.a.	n.a.	✓✓✓	✓✓✓

Impact on cost/efficiency of the various policy options, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact

---

The following table reflects the assessment of the **coherence** of policy options as per Section 6.1.3 of the impact assessment report.

Table 4: Comparison of options in terms of coherence

	Internal coherence	**Telecom framework**	**GDPR**	**RED**	**Total**
Option 0 -- *Baseline*	0	0	×	**0**	×
Option 1 – *Soft law*	×	×	×	**0**	×××
Option 2 – *Limited reinforcement/ harmonisation*	✓	✓	✓	**0**	✓✓✓
Option 3 – *Measured reinforcement/ harmonisation*	✓✓	✓	✓	≈	✓✓✓✓
Option 4 – *Far-reaching reinforcement/ harmonisation*	✓	✓	✓	≈	✓✓✓
Option 5 – *Repeal*	×	✓	✓	**0**	✓

Impact on coherence, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact

2. Comparison of options with respect to their impact on different stakeholders

- Option 1 to 4 will benefit **Citizens** (both individuals and legal persons) in increasing magnitude due to the reinforcement of the protection of their privacy. **Option 1** will have a slightly positive effect, through the dissemination of guidance, best practices, standardisation and awareness-raising initiatives. **Option 2** will have a positive effect, thanks in particular to the extension of the scope of the protection. **Option 3** will have greater positive effects thanks to the introduction of mandatory centralised privacy settings. **Option 4** will further increase the level of protection, but may indirectly penalise citizens by excessively limiting OBA based offers. **Option 5** would remove the specific protection of privacy and confidentiality in the electronic communications secor and in this respect may penalise citizens. **Option 3** is the best option for citizens.

- **Businesses:** the following main cateogories of different undertakings would be affected by the new rules in the following way:

  - ✓ **ECS providers**: **Option 1** does not affect ECS providers much. ECS providers would benefit from the level playing field introduced by **Options 2, 3** and **4**. **Option 5** would benefit ECS providers the most, as it would simplify the rules applicable to them and eliminate the specific restrictions concerning traffic and location data. **Option 5** is the best option for ECS providers. Between **Option 2** and **3**, ECS providers would prefer **Option 3** as it would introduce elements of flexibility compared to the present regime.

  - ✓ **OTTs**: **Option 1** and **5** are the most favourable solutions for them, with possibly a preference for Option 1 given that this option would maintain their regulatory advantage over ECS providers. **Option 2, 3** and **4** would significantly affect OTTs as they will have to comply with the ePrivacy rules. Between these, **Option 3** is to be preferred due to the greater flexibility, whereas **Option 4** is the most restrictive.

  - ✓ **Website operators** and **online advertisers**: **Options 1** and **2** would not change anything for these operators. **Option 3** would present some advantages in terms of cost reduction and some disadvantages relating to the binding browser privacy settings greater transparency of tracking. **Option 4** would seriously affect them by banning the cookie wall. **Option 5** is the best option for them as it would basically imply removal of the current rules.

  - ✓ **Providers of browsers, operating systems and app stores** are only affected by **Option 3** in relation to the obligation to provide for general privacy settings. However, the related cost is not expected to be excessively high, considering that the few operators concerned already have developed some solutions in this direction.

  - ✓ **Direct marketers** would not be significantly affected by **Option 1**. They would be affected in increasing magnitude by **Option 2, 3** and **4**. **Option 5** is their most favourite option, as it would remove at least in part the restrictions regarding unsolicited marketing.

  - ✓ **SMEs** who are OTTs would be affected significantly by **Option 2**, **3**, and **4** given the extension of the scope. Compared to large businesses, they would feel in proportion more the burden of the new ePrivacy rules. However, some flexibility and simplification mechanisms included in Option would significantly reduce such burden.

- **Competent authorities**: **Option 3** and **4** will have significant effects on national authorities. **Option 3** would entail some reorganisation costs for those authorities that are currently not equipped with appropriate powers and adequate resources for exercising supervision.

- The **Commission** will have to bear some costs relating to the various soft-law initiatives in **Option 1**. The costs for the Commission are low in **Option 2** and **3** and essentially coinciding with the conduct of the legislative process. In addition, the Commission would have to bear some variable running costs for the implementing measures in **Option 4**.

The above analysis shows that **Option 3** is the best option for citizens, while **Option 5** is the worst. By contrast, **Option 5** is the best option for businesses overall (the second best option for OTTs) and **Option 4** the worst. **Option 4** and **5** being excluded as extreme solutions, **Option 3** is overall a preferable solution to Option **2** for both citizens and businesses (except

some browsers providers). For MS authorities, **Option 3** presents non-insignificant reorganizational costs.

Table 5 – Comparison of options in terms of impact on stakeholders

Impacts	Option 0	Option 1 (soft law)	Option 2 (limited)	Option 3 (measured)	Option 4 (far-reaching)	Option 5 (repeal)
Citizens	**0**	≈	✓	✓✓	✓✓✓/×	××
ECS	**0**	≈	≈	✓	✓	✓✓✓
OTTs	**0**	**0**	××	××	×××	**0**
Websites/ OBA	**0**	≈	**0**	✓✓/××	×××	✓✓✓
Browsers/ OS	**0**	**0**	**0**	×××	×××	**0**
Direct marketers	**0**	≈	×	××	×××	✓✓✓
SMEs	**0**	≈	×××	✓✓✓/××	✓✓✓/××	✓✓✓
National authorities	**0**	≈	≈	×	×	**?**
Commission	**0**	×	≈	≈	×	≈

Impact on various categories of stakeholders, ✓✓✓(Strong and positive– ✓✓ (Moderate and positive) – ✓ (Weak and positive) - ×××(Strong and negative) – ××(Moderate and negative) – × (Weak and negative) – ≈ marginal or neutral - ? uncertain; n.a. not applicable. 0 no impact -- ✓/×; ✓✓/××; ✓✓✓/××× (mixed impact: positive + moderate impact at the same time)

ANNEX 14: GLOSSARY

Article 29 Working Party 29

The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

It has advisory status concerning the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures. It acts independently. It is composed of:

- a representative of the supervisory authority (ies) designated by each EU country;
- a representative of the authority (ies) established for the EU institutions and bodies;
- a representative of the European Commission.

The Working Party elects its chairman and vice-chairmen. The chairman's and vice-chairmen's term of office is two years. Their appointment is renewable.

The Working Party's secretariat is provided by the Commission

Communication

Communication means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information[151].

Cookie

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 you are on (e.g. an advertising network to deliver ads to the online user) for instance in his browser to monitor his behaviour over time.

Do Not Track standard

The Do Not Track (DNT) policy is an opt-out approach for users to notify web servers about their web tracking preferences. It is opt-out since users have to explicitly state they do not want to be tracked by the website. The DNT policy is implemented technically using an HTTP header field binary option where **1** means the user does not want to be tracked and **0** (default) means the user allows tracking in the website. Web servers can also communicate their tracking status, for example, they only track users with consent, they track users anyway, they disregard the DNT header, etc.

Electronic communications service ("ECS")

[151] Article 2d of the ePD.

Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks[152].

European Data Protection Board

The General Data Protection Regulation (GDPR) has transformed the Article 29 Working Party into the "European Data Protection Board" ("**EDPB**"). The Members of the Board are those of the Working Party, except the Commission who has the right to participate, and its secretariat is ensured by the European Data Protection Supervisor. The EDPB has been given powers aimed at ensuring consistent approaches by national DPAs, provide advice and guidance.

European Data Protection Supervisor ("EDPS")

The European Data Protection Supervisor is the independent supervisory authority at EU level with responsibility for: (1) monitoring the processing of personal data by the EU institutions and bodies; (2) advising on policies and legislation that affect privacy; (3) cooperating with similar authorities to ensure consistent data protection.

Internet of Things (IoT)

Internet of Things (IoT) represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment.

Online Behavioural Advertising ("OBA")

Online behavioural advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience. In many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar identifier that could be used to identify the consumer in the offline world. Instead, businesses generally use "cookies" to track consumers' activities and associate those activities with a particular computer or device. Many of the companies engaged in behavioural advertising are so-called "network advertisers," companies that select and deliver advertisements across the Internet at websites that participate in their networks.

Over The Top Provider s (OTTs)

An over-the-top (OTT) service provider is essentially an Internet platform that allows communications to be exchanged by the members of the platform, in the form of voice, text or data. These providers do not control the transmission of the messages, but rely on end-users' internet connections for the messages to be relayed.

Location data

Location data means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal

[152] Article 2c of the Framework Directive 2002/21/EC.

equipment of a user of a publicly available electronic communications service.

Personal data breach

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service[153].

Robinson lists (or opt-out lists)

A Robinson list or Mail Preference Service (MPS) list is an opt-out list of people who do not wish to receive marketing transmissions. The marketing can be via e-mail, postal mail, telephone, or fax. In each case, contact details will be placed on a blacklist[154].

Subscriber

Subscriber means any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services[155].

Traffic data

Traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof[156].

User

User means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service[157].

Value added service

Value added service means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof[158].

[153] Article 2i of the ePD.
[154] Wikipedia.org.
[155] Article 2k of the Framework Directive 2002/21/EC.
[156] Article 2b of the ePD.
[157] Article 2a of the ePD.
[158] Article 2g of the ePD.