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	*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*

provide credible assurances that overall consistency will be ensured and overlaps avoided	*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 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]

---

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

(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.

(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.

---

[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 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.

- 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.

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

[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.

to the obligations. To corroborate the findings of the evaluation, the evaluation process has therefore built on the sources mentioned before.

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

[19] These rules require users' consent for using technologies such as cookies to store or access information on smart devices.

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 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.

[20] SMART study 2016/080, Final Report, p 206.

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.

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

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 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.

[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.

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;

- 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:

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

- 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;

- 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;

---

[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*."

- 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.

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:

[25] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

- 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.

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.

[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.
[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

---

[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.

private and family life (including communications) enshrined in Article 7 of the EU Charter of Fundamental Rights (hereinafter the "**Charter**").

- 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].

---

[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.

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*,
(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

[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.

equipment (phones, tablets, etc.). This applies, for example, to the storage of cookies[43].

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.

---

[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 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 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.

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.

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

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 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

[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.

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.

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

---

[50] COM(2015) 185 final.
[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.

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 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.

---

[54] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).
[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 €

[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.

Member State	Number of enterprises (in thousands, 2014)	Number of persons employed (in thousands, 2014)	Annual turnover in 2014 (in million)
Malta[63]	0.0	1.6	- €
Netherlands	1.4	31.2	16,881.4 €
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]

---

[63] No data on annual turnover available.

[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.

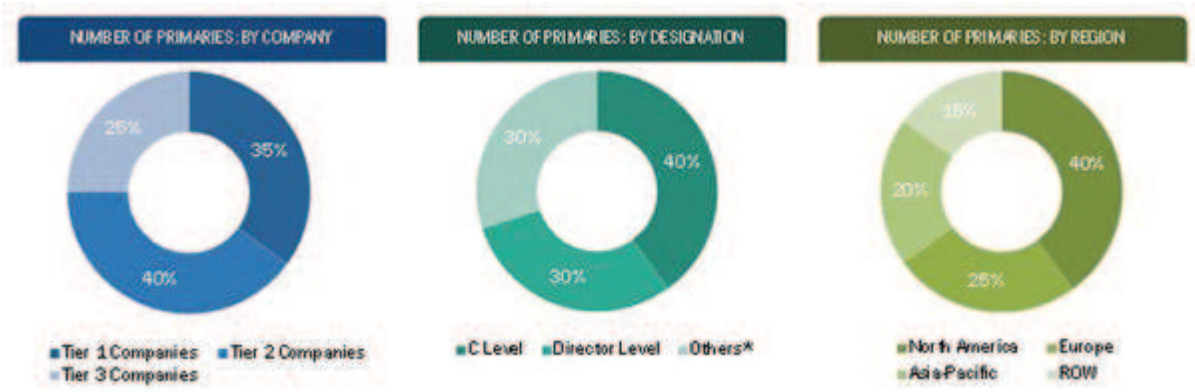
[65] This is based on internal calculations and cannot be directly concluded from the information sources we used for our analysis.

[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

---

[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.

and OTT providers offering voice calls is hard to ascertain. With regard to international 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]

---

[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.

- 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 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

[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.

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".

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

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

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.

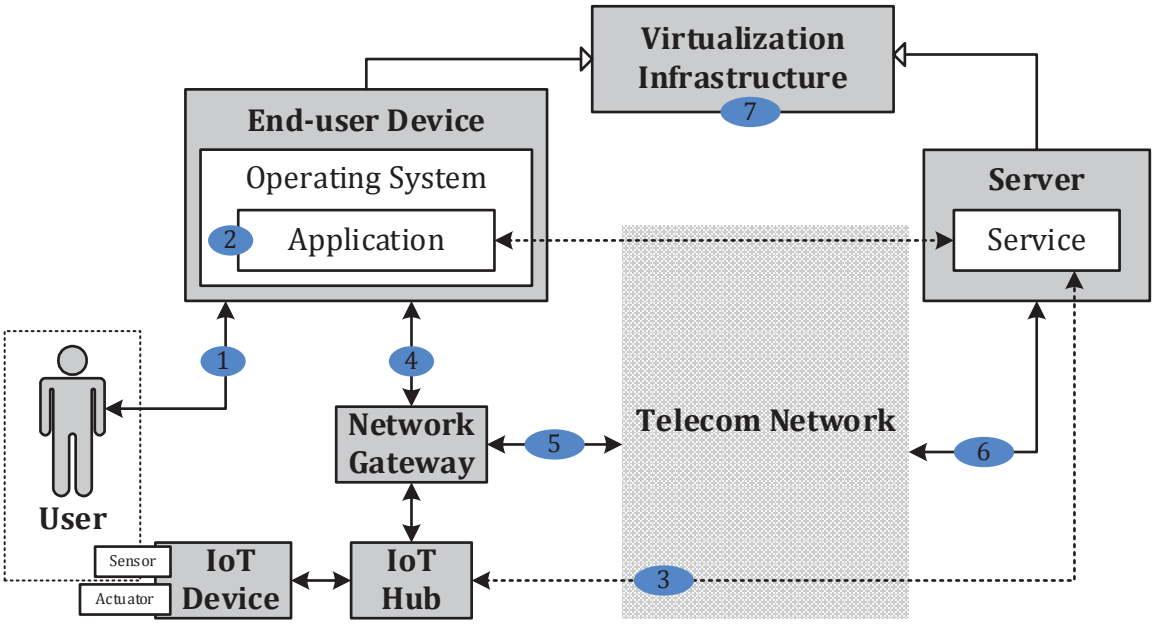


Figure 3 – Abstract architecture diagram

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):

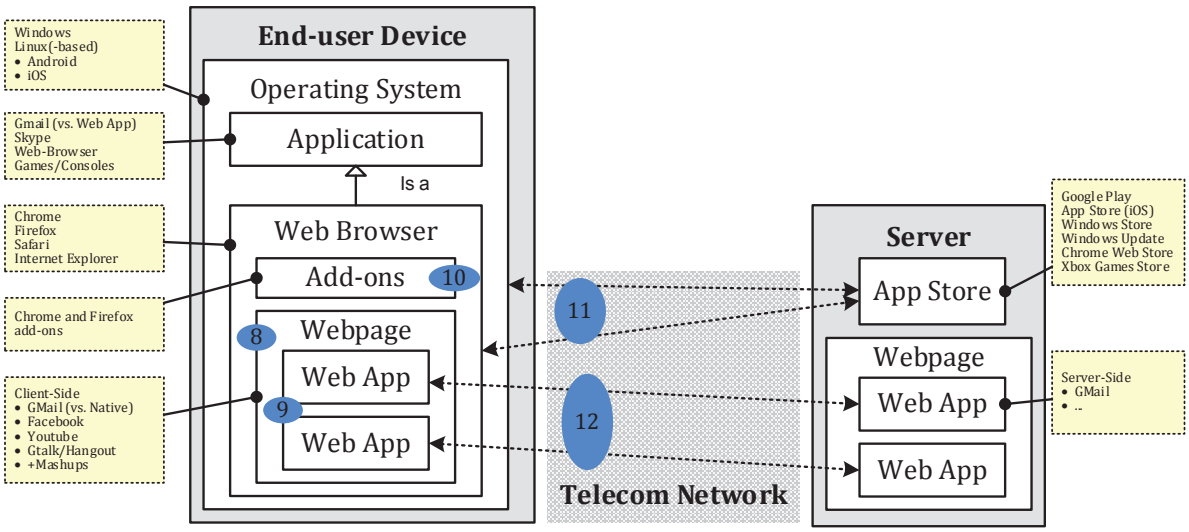


Figure 4 – User Applications and Server Services

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.

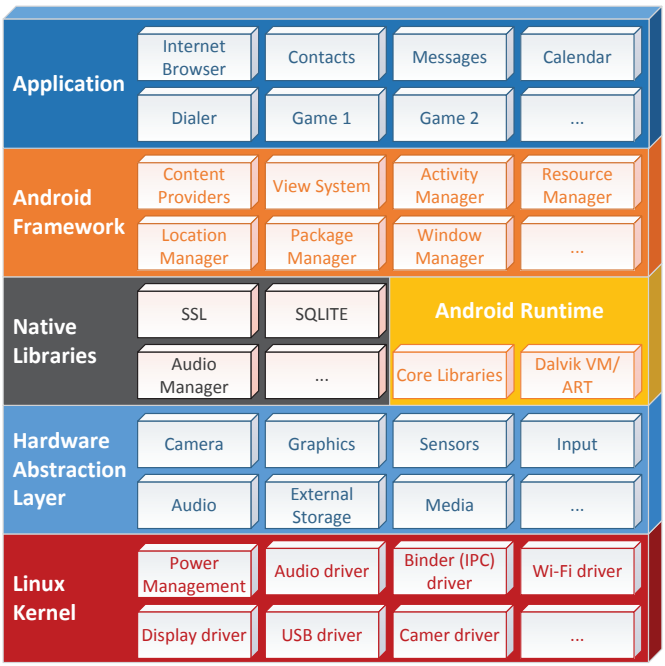


Figure 5 – Android software stack

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 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.

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

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.

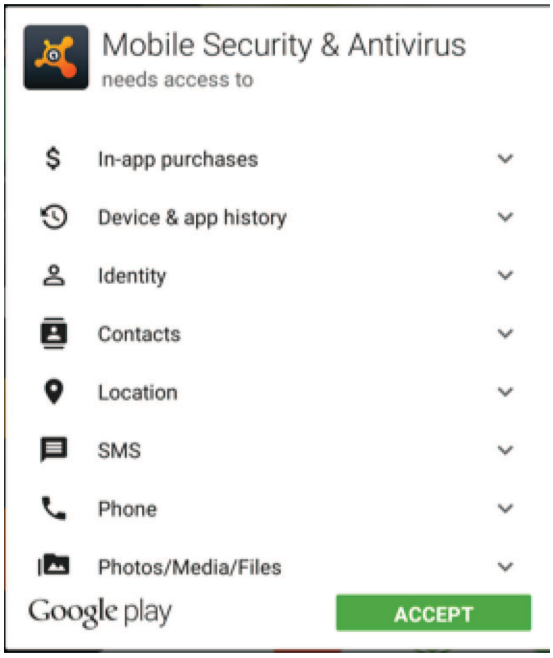


Figure 1 – Permissions on Android prior to version 6.0.

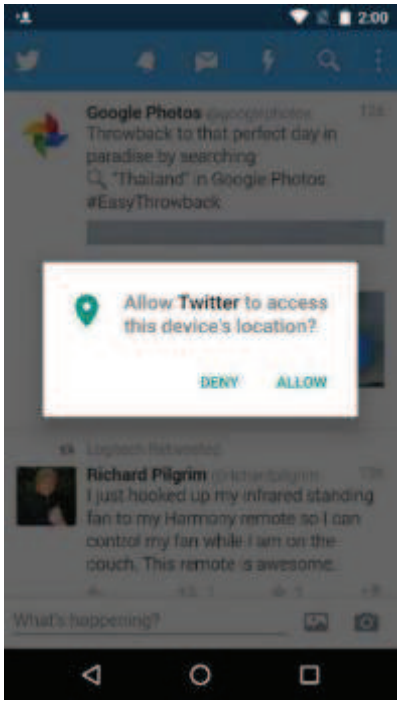


Figure 7 – An app is asking for a permission to use the device's location (Android 6.0)

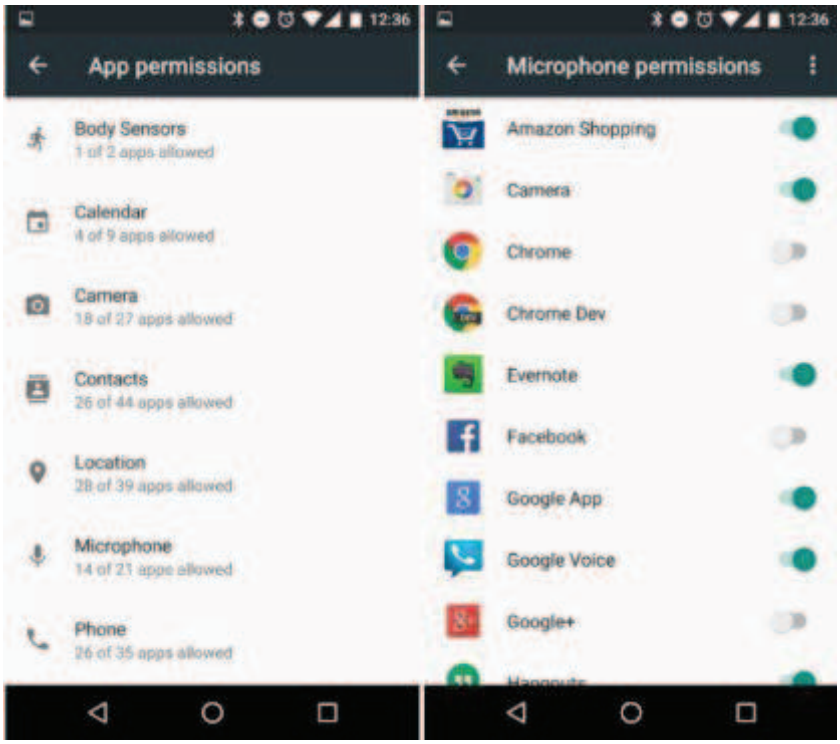


Figure 8 – The user can manually change the permissions of all apps (Android 6.0)

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.

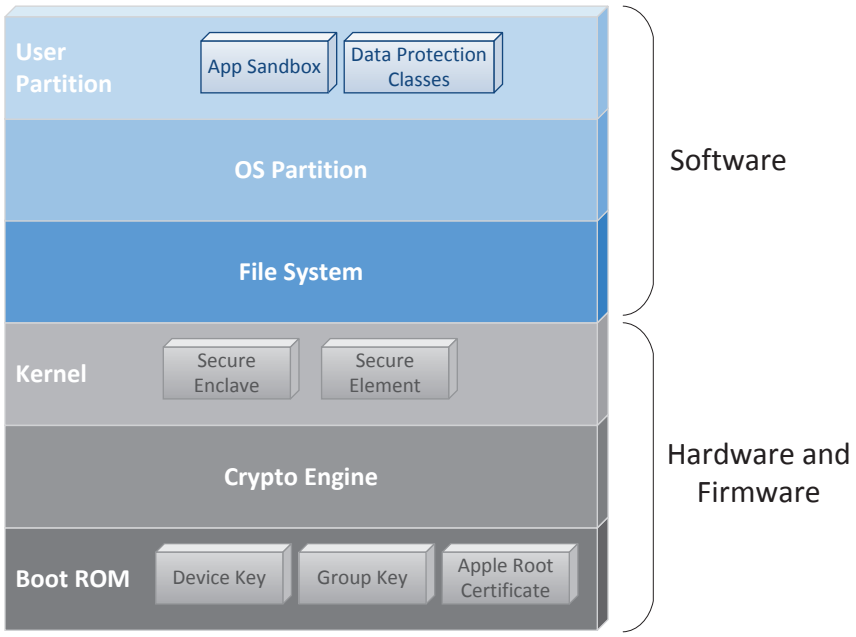


Figure 9 – iOS Security Architecture

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).

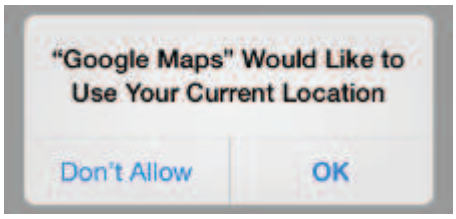


Figure 2 – An app is asking to access the location data in iOS

Figure 11 – Just 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

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

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
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.

Feature	iOS	Android	Comment
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	
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.

Feature	iOS	Android	Comment
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".

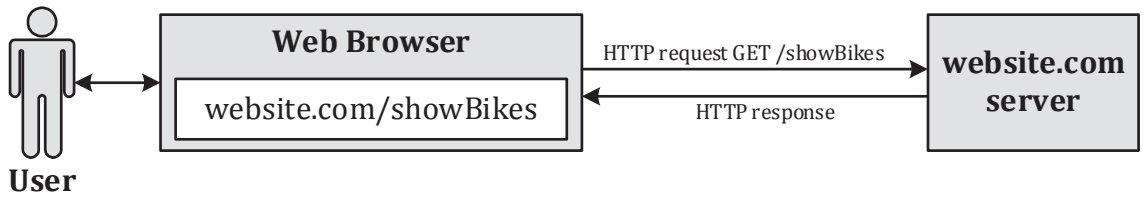


Figure 12 – Access to page in server website.com

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.

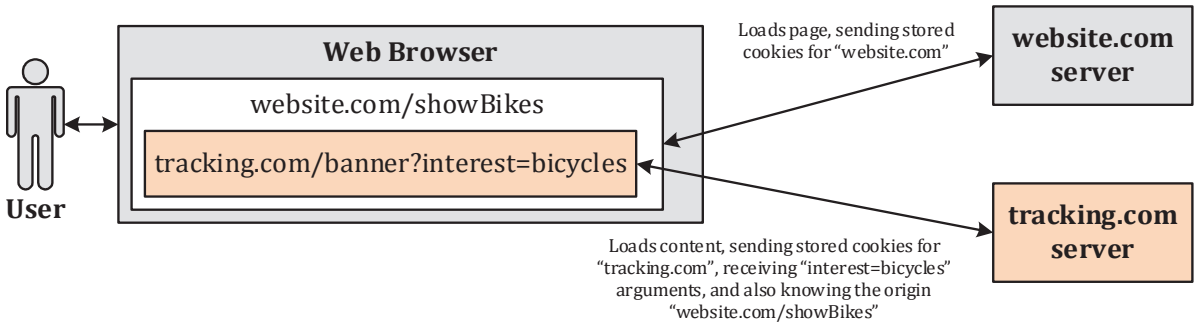


Figure 13 – Example of cookie and data flow in websites with embedded content

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.

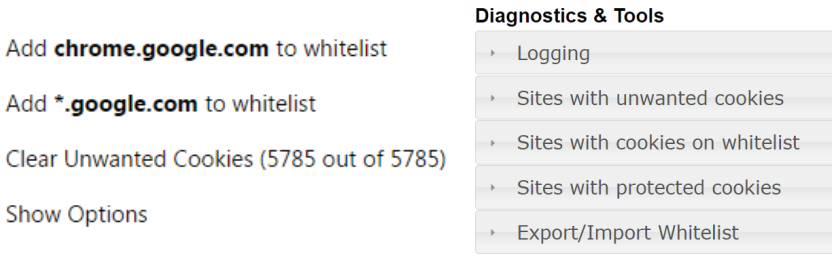


Figure 15 – Vanilla Cookie Manager options

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/

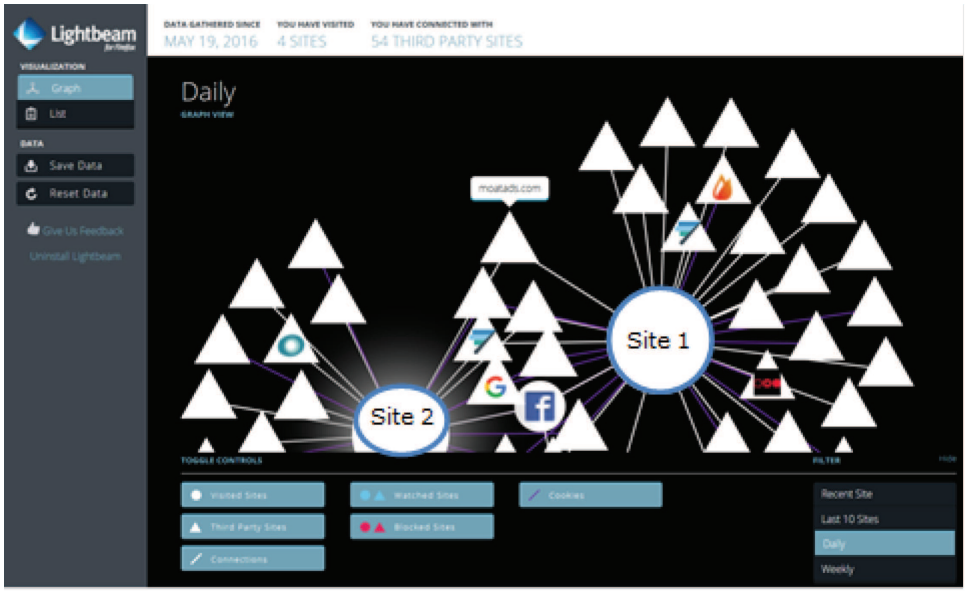


Figure 16 – Lightbeam add-on showing the tracker connection between two news websites

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

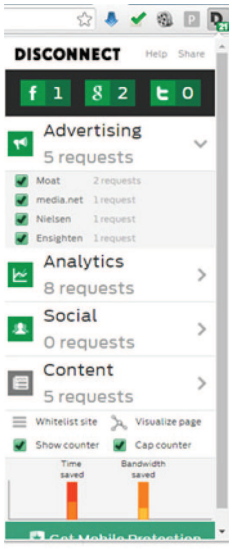


Figure 17 – Disconnect.me plugin showing advertising trackers

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.

---

[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]

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 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.

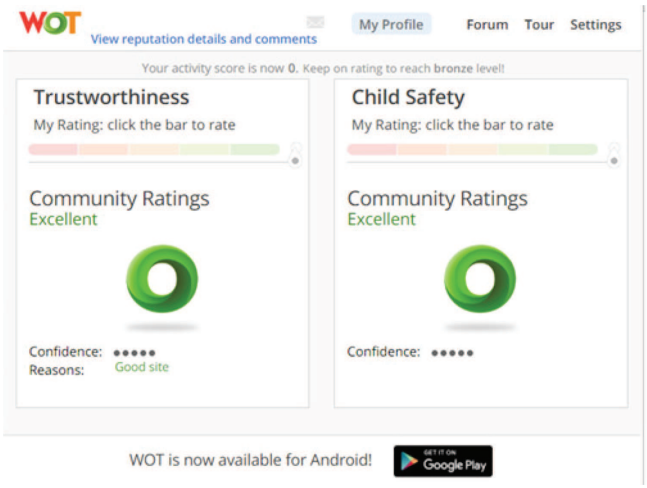


Figure 18 – WOT plugin results for the a news website

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

[97] https://anonymous-proxy-servers.net/en/jondofox.html
[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/

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 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.

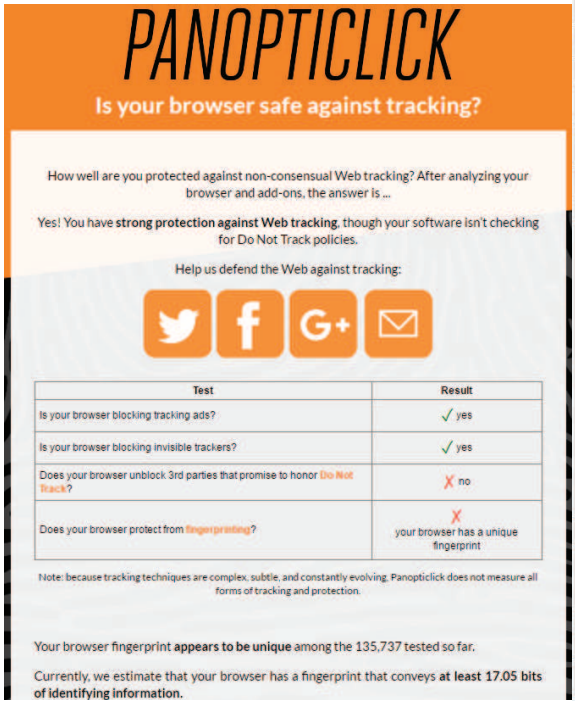
5.6 Software/Browser Metadata Fingerprinting

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

[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.

interpreted exceptions [107]). 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 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.

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

- ✓ **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. 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.

[110] SMART 2016/0080, cited above.

- 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 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

---

[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.

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;

- 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

[114] SMART 2016/0080, cited above.

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 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.

---

[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.

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.

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

[116] SMART 2016/0080, cited above.

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 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	☒ Higher fines in case of privacy breaches ☒ No removal of the ePrivacy rules

	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	
Over-the-top (OTTs), IoT and publicly available private Wi-Fi providers	☑ One directly applicable regulation across 28 MS ☑ Clearer and more consistent rules, filling existing gaps and clarifying relationship with related legislation (e.g., GDPR) ☑ Opportunity to differentiate their offers on the basis of privacy features	☒ New requirements/obligations become applicable (compliance costs) ☒ Potentially increased competition from ECSs in the 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	☒ Additional costs deriving from new obligations ☒ Higher fines for privacy breaches

	features ☑ Increased market competitiveness on non-price factors	
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 cost savings	☒ Ministries will need to ensure adequate resourcing and empowerment of supervisory authorities (where not already the case), and governance changes may require re-organisation in some Member States