# Impact Assessment Institute

The Institute for Impact Assessment and Scientific Advice on Policy and Legislation

**"Impartial Analysis for Policy Making"**

**Study scrutinising the**

**"IMPACT ASSESSMENT**

**Accompanying the document**

**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC**

**(Regulation on Privacy and Electronic Communications)"**

**SWD (2017) 3**

**and the coherence of the legislative proposal COM (2017) 010 with the Impact Assessment.**

IAI-ePrivacy-170714f July 14th 2017

Deleted: Draft s

Deleted: scrutinising

Deleted: ¶

Deleted: 170713d

Deleted: 17071

Deleted: 3

Deleted: f

Deleted: 3

## Main Findings

The revision of the current ePrivacy Directive as a Regulation is presented by the Commission as a key step for the achievement of a Digital Single Market in the EU. The main objectives which underlie the revision are the harmonisation of the market and a strengthened, up-to-date protection of privacy in the changing digital environment.

However, detailed scrutiny of the Impact Assessment and related documents has shown that the evidence presented is not sufficient to support the proposed provisions of the ePrivacy Regulation.

The following significant observations can be made:

- The time allocated to the review of the ePrivacy Directive, data-gathering and Impact Assessment process was not sufficient to generate robust evidence;
- The data-gathering process lacks essential transparency and the presented data is insufficient to support the provisions of the legislative proposal, undermining the legitimacy of the conclusions reached in the Impact Assessment;
- Neither the Impact Assessment nor the proposal sought to identify means to eliminate fully the potential incompatibilities – regarding content and timing – of the new ePrivacy instrument with other pieces of legislation, in particular the GDPR and the EECC;
- Impacts on Fundamental Rights were not adequately assessed, although they constitute the legal basis of the legislative proposal;
- More robust evidence is required to support the provision extending the scope of this Regulation to OTT services;
- The proposed provisions on consent via browser settings do not comply with the consent principle as provided by the GDPR. This issue was not addressed in the Impact Assessment;
- The Impact Assessment evaluates the costs of banning "tracking walls", but does not fully assess the potential benefits, nor compliance of tracking walls with Fundamental Rights, thereby preventing a valid comparison;
- Setting different rules for tracking by first parties and by third parties may affect competition in a substantial way. Nevertheless, impacts on competition and market distribution were not part of the Assessment.

From these findings, the IAI recommends assessing the actual alignment of the ePrivacy Regulation with the provisions of the GDPR, and fully considering the potential repercussions of the new provisions on the Digital Single Market. For the ongoing legislative process, the IAI also recommends taking into account the shortcomings of the evidence presented in the Impact Assessment. Compilation of new robust evidence is necessary to inform consideration and development of measures that will meet the objectives in an effective manner.

Impact Assess titute

**Deleted:** <#>The Impact Assessment fails to provide sufficient evidence which underpins the necessity to extend the scope of this Regulation to OTT services;¶

**Deleted:** For the ongoing legislative process, Tt

**Deleted:** taking into account the shortcomings of the evidence presented in the Impact Assessment. Compilation of new robust evidence may be necessary to feed

**Deleted:** analysing the feasibility of the planned implementation date of the ePrivacy Regulation, and assess whether this date allows sufficient time for

**Deleted:** ——————————Page Break——————————

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

## Visualisation

The following table provides a visual overview of the results of this report for each element of the evidence presented in the Impact Assessment, using an assessment from 1 to 7 to indicate the level of confidence (1 = highest, 7 = lowest confidence level).

| Element | Assessment level & description (1…7) | | Notes |
|---|---|---|---|
| Rhetoric | 2 | Minor questions identified on analysis and/or evidence | The language and assertions in the Impact Assessment are balanced and formulated in a neutral way |
| Assumptions | 6 | Serious concerns identified with analysis and/or evidence | Policy Options were designed before the end of the data-gathering process |
| Background data | 5 | Substantial concerns identified with analysis and/or evidence | Background data are insufficient to support some parts of the Impact Assessment, and not referenced properly |
| Analysis | 5 | Substantial concerns identified with analysis and/or evidence | The methodology for analysing the various impacts is simplistic |
| Results | 6 | Serious concerns identified with analysis and/or evidence | The results of the Impact Assessment sometimes go against the evidence |
| Conclusions | 2 | Minor questions identified on analysis and/or evidence | Some conclusions are not based on a proper assessment. The proposal is consistent with the IA's results despite some inconsistencies and add-ons |

Key to assessment levels

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| Correct analysis, fully evidenced | Minor questions identified on analysis and/or evidence | Several questions identified on analysis and/or evidence | Concerns identified with analysis and/or evidence | Substantial concerns identified with analysis and/or evidence | Serious concerns identified with analysis and/or evidence | Incorrect analysis / evidence absent |

Formatted Table

Impact Assessment Institute

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

## Contents



Impact Assessment Institute

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

**Formatted:** Default Paragraph Font, Check spelling and grammar

**Formatted** ...

**Deleted:** 170619d

**Deleted:** 17071…70713…ff ...

# 1 Introduction

The Digital Single Market Strategy was adopted in a 2015 Communication. It is divided into three pillars:

- Better online access for consumers and businesses across Europe;
- Creating the right conditions and a level playing field for advanced digital networks and innovative services;
- Maximising the growth potential of the Digital Economy.

The review of the Directive on Privacy and Electronic Communications ("ePrivacy Directive") is part of the 16 actions of the Strategy; more particularly, part of the second pillar. A REFIT evaluation was carried out in the first half of 2016, while an Impact Assessment on a new proposal for a Regulation was in progress.

The proposal for a Regulation on Privacy and Electronic Communications was published on 10 January 2017, along with the Impact Assessment, and the results of the REFIT evaluation of the ePrivacy Directive. The proposal aims at updating the provisions of the ePrivacy Directive, by broadening the scope of the legislation, and removing the last barriers to free circulation of data within the European Union.

This IAI study scrutinises the evidence presented for the ePrivacy Regulation, namely the following documents:

- Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications);
- Impact Assessment accompanying the proposal (SWD (2017) 4);
- Synopsis report of the public consultation on the evaluation and review of the ePrivacy Directive;
- 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079), final report;
- Evaluation and review of Directive 2002/58/EC on privacy and the electronic communication sector (SMART 2016/0080), hereafter "the consultant's study".

The above documents have been scrutinised on the basis that they should be consistent, present sufficient detail for full understanding of the results, allow reconciliation by the stakeholder and enable full comparison of different options and scenarios.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

# 2 Justification

## 2.1 Problem definition

The basic requirements set by the Better Regulation guidelines, regarding the timeline of Impacts Assessments, are not fulfilled. The guidelines state that an Impact Assessment should be published at minimum 12 months after the Inception Impact Assessment. Furthermore, the Inception Impact Assessment should precede the evidence-gathering process, specifically, public consultations.

In this case, there was only a period of three months between the publication of the Inception Impact Assessment and the publication of the proposal and its accompanying Impact Assessment. According to the Inception Impact Assessment, the Impact Assessment work started "in the first half of 2016", around the same time as the REFIT evaluation and public consultation activities. This puts forward the question whether the actual process for the IA provided sufficient time to conduct proper analysis for this highly complex topic. In comparison, the evaluation and Impact Assessment process for the General Data Protection Regulation (GDPR) started in May 2009, and the Impact Assessment was published, along with the legislative proposal, in January 2012, hence almost three years after.

A key element of an Impact Assessment is the problem definition. As indicated in the Better Regulation Toolbox:

> *"The first step of an IA is to verify the existence of a problem and to identify who is affected; estimate the scale of the problem; analyse its causes; and assess the likelihood that the problem will persist in the absence of EU policy intervention."*[1]

The Impact Assessment on the ePrivacy Regulation identified 3 problems, whose definitions are analysed in the table below:

[1] Better Regulation Toolbox, p.65

Deleted: , hence

Deleted: ,

Deleted: *[t]*

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

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

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

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

| Steps to be completed in the problem definition[2] | Assessment of the problem definition in the Impact Assessment |
|---|---|
| A. Establish **what the problem is and why it is problematic** (i.e. its negative consequences) | 1. The reasoning which leads to the definition of Problem 1 is incomplete.<br><br>Over-the-Top services (OTTs) and Electronic Communications Services (ECS) are subject to different rules in most countries. However, the Eurobarometer survey and the public consultations provide evidence only that their services are similar, but no source demonstrates that these services are likely to become substitutable and therefore will be in direct competition.<br><br>Some of the shortcomings of the Directive that is currently in force were presented in the REFIT evaluation and are addressed in the Impact Assessment: the lack of information prior to the consent of end-users, and the issues regarding Wi-Fi tracking. However, regarding Machine-to-Machine communications, the Impact Assessment lacks evidence that substantiates the claim that these pose a problem of confidentiality for end-users. |
| | 2. The problem definition is based on the outcome of the Eurobarometer survey: "61% believe that they receive too many unsolicited calls offering them goods or services"; and national statistics on unsolicited calls including information on their frequency. However, the problem definition is expanded to include other types of unsolicited communications. In particular, OTT services are specifically highlighted in the problem definition; however no evidence is presented that unsolicited communications via OTT services raise an issue for end-users. |
| | 3. The REFIT evaluation (SMART 2016/0880) presents appropriate evidence for this problem. However, no evidence is presented to estimate the problem related to costs specifically |

[2] Better Regulation Toolbox p. 65-67

Deleted: or to have become

Impact Assessment Institu

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

| | |
|---|---|
| | entailed by the fragmented transposition of the Directive, and their repercussions on innovation and the expansion of cross-border activities.<br><br>The lack of competitiveness of the EU digital arena is partly supported by the REFIT evaluation (p.58), which estimates that the EU market for OTTs will grow "at a similar pace […] as the North American market" but slower than other markets. However this statement is true only for OTTs.<br><br>Furthermore, this problem might be inconsistent with Problem 1 as it is stated that provisions applying on ECS are "too strict", and should be relaxed to create a level-playing field with OTTs. The solution that is envisaged in the description of Problem 1 is an extension and a strengthening of the rules on OTTs. |
| B. Assess the magnitude and **EU dimension** of the problem | No evidence is presented to demonstrate the extent to which these problems have an EU dimension. |
| C. Establish the causes ("**drivers**") and assess their relative importance | 1. The quoted lack of technological neutrality and the outdated provisions of the current Directive are addressed. However, the reasons and the extent of the competition between ECS and OTTs should have been assessed as well.<br><br>The reasons for why the current legislation on consent to tracking is not working are not fully assessed. The Impact Assessment does no go beyond saying that the current policy is complex and inefficient. |
| | 2. The Impact Assessment does not present the reasons why the current legislation has failed to limit unsolicited calls, nor other types of unsolicited communications.<br><br>Therefore the causes of the problem are not established. |
| | 3. The causes for the divergence in transposing the ePrivacy Directive are not sought. |
| D. Identify who the **relevant stakeholders** are | Annex 7 provides an accurate mapping of the stakeholders affected by the Directive and its revision. |
| E. Describe how the problem is likely to evolve with **no new EU intervention** | 1. It is possible to infer from the data that OTTs should be subject to rules on confidentiality. However, no evidence is presented to support that the rules on ECS and OTTs should be the same to avoid unfair competition. |



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

| | |
|---|---|
| | The potential consequences of maintaining the status-quo are not assessed and not based on evidence. This applies in particular to new types of tracking technologies and Machine-to-Machine communications. |
| | 2. For Problem 2 as well, the potential consequences of leaving the legislation as it is are not addressed in this section of the Impact Assessment. |
| | 3. The Impact Assessment states that ultimately the lack of harmonisation will discourage businesses and will negatively affect the EU's competitiveness. No evidence is provided that supports such forecast. |

*Table 1: Assessment of the problem definition, according to the Better Regulation guidelines*

The conclusion is that the problem definition is incomplete. Even though there is some evidence for the identified problems, they are not robustly substantiated. An insufficient assessment of the problem definition risks undermining the entire Impact Assessment, since it might focus on achieving the wrong objectives. This seems to be particularly the case for the extension of the scope of the Regulation to OTT services, as questions of subsidiarity and proportionality of such a provision remain unanswered.



## 2.2 Legal basis

The legal basis and subsidiarity checks are presented under the Section 2 of the Impact Assessment. As stated in the Better Regulation Toolbox, *"the choice of legal basis must be based upon the nature of the main/predominant objective"*. In this case, the proposal is based on two legal bases, namely Article 16 and Article 114 of the TFEU.

Article 16 of the TFEU provides the right of everyone to the protection of the data which concerns them. This right concerns natural persons. However, it is explicitly provided in Article 1 of the proposal that the scope extends to the protection of legal persons' personal data.

The lack of legal ground for the protection of data for legal persons is addressed, by referring to Article 7 of the Charter of Fundamental Rights, and its interpretation by the Court of Justice, in a case-law[3] which is referenced in the proposal on page 4. In view of the relevance of Article 7 of the Charter, it should have been clearly cited as a third legal basis, along with Article 16 and Article 114 of the TFEU as a third legal basis.

In addition to this, Article 16(2) provides the following:

[3] Judgment of the Court (Third Chamber) of 14 February 2008, *Varec SA v Belgian State*, C-450/06

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

> *"The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data."*

This article does not provide a legal basis for legislation that would apply to the processing of data by non-public entities. Besides, it is stated in the proposal for a Regulation (p.3):

> *"the proposal does not apply to activities of Union institutions, bodies and agencies. However, its principles and relevant obligations as to the right to respect for private life and communications in relation to the processing of electronic communications data have been included in the Proposal for a Regulation repealing Regulation (EC) No 45/20018."*

Using this Article as a legal basis appears inconsistent with the content of the proposal. This requires clarification to ensure a solid legal foundation for the Regulation.

Article 114 of the TFEU provides that the co-legislators have a shared competence with Member States concerning the achievement of the single market. The choice for this legal basis is related to Objective 3 of the review of the ePrivacy Directive, "*Enhancing harmonisation and simplifying/updating the legal framework*".

This legal basis appears to be relevant, in view of the main objectives of the review of the ePrivacy Directive, and the Problem definition that ensued.

According to the Better Regulation Toolbox, on page 21:

> *"The nature of the particular market should, therefore, be characterised in terms of the market participants, the **extent of cross-border trade**, presence/market share of companies from other Member States, territorial restraints on trade, share of foreign workers, ease of cross-border purchasing, rules related to the use/movement of capital, etc;"*

The characterisation of the internal market is developed in the Impact Assessment's section on subsidiarity, which will be analysed in the following Section 2.3.

## 2.3 Subsidiarity

By choosing Article 114 of the TFEU as a legal basis the Commission is required to characterise the market onto which the proposal would apply. The characterisation in the Impact Assessment consists of general statements, not underpinned by any evidence:

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

Such a statement cannot be considered as a proper characterisation of an internal market, as it provides an assumption on electronic communications, and types of services other than electronic communications services are omitted. No source is cited for such a statement, and no evidence can be found across the sources used by the Commission.

Section 3.5 of the consultant's study is an attempt at characterisation of the market. Nevertheless, it solely provides an overview of the current and potential market participants,



**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

and the extent of the competition between the various types of communication services. There is no information on the extent of cross-border services.

> *"MS cannot effectively solve the problems in the current situation. In order to achieve the internal market in the electronic communications sector, it is necessary to reduce the current fragmentation of national rules and ensure an equivalent level of protection across the whole EU."*

While solid evidence is provided to demonstrate that the transposition is fragmented is disparate across Member States, the study does not further analyse the reasons behind this fragmented transposition, and the extent to which this problem could be tackled by first revising the national implementing legislation currently in force.

> *"Moreover, the proper functioning of the internal market requires that the rules ensure a level playing field for economic operators."*

This is a Policy Objective, but it does not provide information that would confirm the respect of the subsidiarity principle. As mentioned above, there is no evidence that the achievement and proper functioning of the internal market cannot be handled at a national level.

The third paragraph of this section of the Impact Assessment does not provide relevant information on subsidiarity. While it is worthwhile noting that the proposal is in line with a political agenda – namely the Digital Single Market strategy – this does not provide evidence that the proposal respects subsidiarity.

In the fourth paragraph, although the reasoning is correct, no source of information is cited to underpin the conclusions that are made:

> *"Whilst it is therefore possible for MS to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of EU rules and would create restrictions on cross-border flows of personal and non-personal data related to the use of electronic communications services to other MS that do not meet the same protection standards."*

Finally, coherence with the GDPR is mentioned as an objective of the proposal, thus requiring the review of the provisions of the ePrivacy Directive:

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

This statement is not relevant for the subsidiarity check. Ensuring consistency of the legislation is indeed an objective of the proposal, as inconsistency is part of Problem 3. However, the proposal here is deemed to reach this objective, while respecting subsidiarity.

The conclusion is that the analysis in the Impact Assessment does not properly address subsidiarity. This means that the outcomes presented in the Impact Assessment do not necessarily provide a complete overview of relevant options.

## 2.4 Proportionality

The Impact Assessment does not include a section on proportionality, although it is mentioned on page 49 as an outcome of the comparison of the Policy Options, that "Option 3 is considered a more proportionate, and thus preferable, solution compared to Option 4."

Impact Assessment Institute

Deleted: (

Deleted: ),

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

However, there is a statement on proportionality in the proposal (Section 2.3). Overall, the statement does not provide clear and proper explanation for why the proposal is proportionate. There is no clear link made between – on the one hand – the problems identified in the Impact Assessment and the review of the ePrivacy Directive, and – on the other hand – the likeliness of solving them by implementing this regulation.

Moreover, it is stated that proportionality is ensured by the possibility for Member States to take "national derogatory measures for specific legitimate purposes". This refers to Article 24 of the proposal. Such derogatory measures were actually not included in the definition of any Policy Option, and their need and potential impact was not assessed (for example with regards to potential future fragmentation which is listed as one of the drivers of the current problem definition). The proportionality check is therefore based on an unverified assumption.

Finally, important changes such as the extension of the consistency mechanism – the enforcement mechanism introduced in the GDPR – should not be assumed to be proportionate. As an example, there would be no point in extending the consistency mechanism if the issues of protection of the confidentiality of communications were not caused by the current enforcement mechanism. This reasoning should be included in the proportionality check.

## 2.5 Choice of legal instrument

Problem 3 as defined in the Impact Assessment provides a justification for the replacement of the current Directive with a Regulation. As stated in the Impact Assessment, the fragmentation of the existing legislation across Member States and the resulting barriers to the provision of services was caused by the possibilities and choices that were granted to Member States.

A Regulation, as it is in principle directly applicable in the Member States, eliminates potential discrepancies in the implementation.

Furthermore, the Commission is put in charge of the delegated acts related to the provisions of the Regulation.

Nevertheless, the proposal defers the implementation of specific provisions to the Member States:

- Article 13(2) on exceptions to presentation and restriction of calling and connected line identification, provides that Member States "shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls."
- A similar provision can be found at Article 16(4) on unsolicited communications.
- As provided in Article 7(3) on storage and erasure of electronic communications data, the maximum allowed period of storage of the metadata used for billing is not harmonised, as it still depends on national laws. This provision is in line with the 2014 decision of the Court of Justice of the European Union, *Digital Rights Ireland*, which invalidated the 2006 Directive on data retention, and therefore handed back





**Formatted:** Font: Italic

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

the competence to the Members States. Such an explanation should have been provided, in order to understand better the reason for this provision.

- Finally, Articles 23(4) and 23(6) provide that the rules on penalties related to Articles 12, 13, 14, 17 and the infringements by public authorities and bodies shall be laid down by the Member States.
- Article 24 leaves a margin of manoeuver for the Member States to set up other penalties, so long as they are "effective, proportionate and dissuasive". As mentioned above, such a provision is not part of a Policy Option and therefore not assessed in the Impact Assessment.

Therefore, whilst part of the Regulation provides a common legislative framework, directly applicable in all the Member States, some of the provisions are not directly applicable and will require national transposition, which may once again lead to fragmentation.

In addition to this, the Impact Assessment does not provide enough justification for this choice of instrument. As developed in Section 2.2, there is insufficient evidence that the problems of fragmentation (which justify the choice for a Regulation) highlighted by the REFIT evaluation of the ePrivacy Directive cannot be solved by further national intervention or a revision of the national implementing legislation that is currently in force.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

# 3 Input data

The availability and the quality of data is a key element which will determine the reliability of the findings presented in an Impact Assessment. According to the Better Regulation guidelines, "data sources should be provided and underlying assumptions illustrated in relation to any quantification"[4]. Furthermore, a potential lack of quantitative data should be acknowledged in the Impact Assessment and compensated by further qualitative assessment[5].

In this case, the lack of available quantitative data was acknowledged all throughout the consultant's study. However, there is no statement in the Impact Assessment about the lack of data and its potential consequences on the quality of the assessment of the various policy options. Such a statement would have been necessary to ensure full transparency.

The Institute has scrutinised the main sources of data that were used for this Impact Assessment and the consultant's study, and drawn the conclusions that the data sources used are not transparent and that the analysis thus does not comply with Better Regulation principles.

## 3.1 The public consultation

The results from the public consultation on the ePrivacy Directive, which are available in the synopsis report, are the most significant input for the problem definition.

The consultation received 421 replies. 195 respondents were citizens and consumer or civil society associations, 186 respondents were businesses or trade associations, and 40 respondents were public bodies. There is a range of respondents from all main relevant stakeholders' categories. Yet, there is no guarantee that these responses are representative of those parties interested in and affected by the issues.

The way in which these results were used is problematic. Consultations cannot be deemed to be a robust source of evidence for an Impact Assessment. They provide valuable information on opinions, which require further evidence to be corroborated.

Throughout the consultant's study, the Commission's consultations are used and mentioned to support a high number of assumptions. For instance, the Impact Assessment only cites the public consultation as a piece of evidence for the substitutability of electronic communications and OTT services, although only 35.3% of the respondents to the consultation perceived such substitutability. This undermines the validity of the problem definition, in particular, the need for a level-playing field between these two types of communications.

Some of the assessments are supported by other similar sources, such as the online surveys and interviews carried out by Deloitte – for instance, the need for a strengthening of the

[4] Better Regulation guidelines, p.28

[5] Ibid



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

rules on confidentiality of communications. Again, while they provide important information for the discussion on the policy, they do not provide sufficiently robust evidence.

More importantly, most of the assumptions are not supported by any evidence other than the consultations. This is alarming since the interpretation of the consultation outcomes is questionable. A striking example of this is the evaluation of the added value of the ePrivacy Directive, as a specific instrument for data protection and privacy in the electronic communications sector. The added value "can be confirmed" according to the evaluation, based on the fact that during the consultations "close to two thirds (61%) of all respondents indicated that there is an added value of having specific rules on the confidentiality of electronic communications for the electronic communications sector."

The public consultations, whose lack of representativeness has been highlighted above, cannot be considered as a robust source to demonstrate the added value of the current Directive. The same comment on representativeness can be applied to the evaluation of the rules on traffic and location data, which are assumed not to be effective. Furthermore, the justification given in the final report (p.149) is that "a majority of respondents (45% or 173 of 332) faced problems in applying/understanding the rules on traffic and location data", but 45% is less than a majority.

Overall, the excessive use of the consultations as a justification of the findings of the evaluation and the Impact Assessment, particularly in the consultant's study, undermines the credibility of the Impact Assessment and could lead to important mistakes in the proposal.

## 3.2 The Flash Eurobarometer survey on ePrivacy

The Flash Eurobarometer survey 443 on e-Privacy (SMART 2016/079) was conducted in July 2016, as part of the review process of the ePrivacy Directive.

A Flash Eurobarometer survey is conducted through the phone, unlike standard Eurobarometer surveys, which are based on face-to-face interviews.

The methodology is described in an Annex of the report, as well as the content of the survey and the country of origin of the respondents. The number of respondents (26,526) is relatively high for a Flash Eurobarometer. This compares to the average number of respondents for the last 15 Flash Eurobarometer surveys is 15 594, ranging between 2004 and 40 798 respondents, according to the Commission's website.

The results from this Eurobarometer survey are used as evidence for stakeholder support, and for the problem definition (for setting the market context). Several assumptions in Annex 4 are presented as based on Eurobarometer results. These assumptions contribute to the definition of the problem, thus strongly influencing the decision-making process. The following assumptions in Annex 4 (p.23-24) are drawn from the survey's results:

- *"The rise of free online services has enticed a shift in citizens' attitude to share information related to their surfing behaviour."*
- *"Citizens have grown increasingly irritated by the continuous requests for consent online and most likely click them away to get rid of them"*
- *"The changing notion of privacy in an evolving digital environment"*

The survey provides indications of these opinions. However, the survey did not include a dynamic analysis through a comparison of data over time. The evidence is therefore not presented for those conclusions that imply changes over time.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

Comparison with previous surveys is not possible. The last survey which was conducted on this matter was a standard Eurobarometer survey in 1996 on "Information technology and data privacy". The methodology and type of questions were different, and any attempt of comparison would be undermined by the strong technological evolution which differentiates the two periods.

Further, examples of misinterpretation of the survey's results can be found in Annex 4:

> *"While citizens generally value privacy and confidentiality very much, they are prepared to give up part of their privacy for convenience and performance."*

As mentioned in a footnote linked to the assumption, "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%)." Such a figure does not prove that citizens would agree on giving up a part of their privacy for convenience and performance.

The results of the survey are also used for the assessment of the policy options, in particular regarding the impacts of the different provisions on tracking (p.143-144 of the consultant's study).

The results of the Flash Eurobarometer survey, although useful to gain a clearer picture of the policy context, should not be considered as robust evidence for all aspects of the Impact Assessment.



## 3.3 Member States data inputs

The Member States have provided the Commission and the consultant with extended information about the transposition of the most relevant provisions of the ePrivacy Directive. This information can be found in the Annexes of the final report made by Deloitte (SMART 2016/0080). Annexes 9, 10 and 11 of the Impact Assessment contain a summary of the main findings of the transposition checks carried out by Deloitte.

However, it is unclear which information was obtained by which means. Questions of transposition and potential disruptions are included in the scope of several data inputs – the public consultation, the online surveys and the interviews carried out by Deloitte. It is also impossible to know the country of origin of the 20 competent authorities which were interviewed in the data-gathering process.

As the information gathered on the Directive's transposition then led to the conclusion that a new instrument was needed, to avoid disruptions of the internal market rules, transparency on the way this information was gathered would have been necessary.

## 3.4 Online surveys

Two online surveys were conducted, one targeting public authorities and one targeting businesses.

As mentioned above in Section 2.4, not all authorities or governments responded to the survey. As for the content of this survey, it is not entirely displayed in the Annexes, and it is not fully made public. Transparency on these surveys would have been useful to provide information to stakeholders and create confidence in the data.

**Deleted:** (2.4)

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

The respondents were asked to rate their agreement or their level of concern over specific issues, formulated in statements, or targeted articles of the current Directive.

37 businesses responded to the survey, which makes the quality and relevance of the information gathered, very unequal in comparison to the information obtained by the means of the public consultation, which received 421 answers. Moreover, the content of the surveys, the identity of the businesses, their size and country of origin, are not available. Between a third and a half of the respondents are placed in the "Other" category of service offerings, which gives very little information to the reader.

The presentation of the outcome of the survey is sometimes misleading. For instance, in some parts of the survey targeting competent authorities, a majority of the 34 respondents chose the "cannot answer" option (see below). However, the graphic presentation of the results emphasises the second most popular replies (by colouring them), which supports the idea that the ePrivacy Directive functions well, according to this survey's respondents.
The large number of "cannot answer" replies in the survey targeting businesses is highlighted and explained in the Annexes.

| | Poor | Fair | Good | Very good | Excellent | Cannot answer |
|---|---|---|---|---|---|---|
| Obligations for service providers on the security of processing (Article 4.1) | 1 | 2 | 9 | 4 | 0 | 14 |
| Notifications in relation to breaches of security (Article 4.2) | 3 | 2 | 7 | 3 | 0 | 15 |
| Notification of personal data breaches (Article 4.3 and 4.4) | 4 | 4 | 8 | 1 | 0 | 13 |
| Confidentiality of electronic communications (Article 5.1 and 5.2) | 2 | 4 | 7 | 4 | 1 | 12 |
| Confidentiality of information stored on the users' terminal equipment (Article 5.3) | 3 | 13 | 3 | 0 | 0 | 11 |
| Specific rules on traffic data (Article 6) | 3 | 6 | 6 | 3 | 1 | 11 |
| Specific rules on location data other than traffic data (Article 9) | 4 | 8 | 4 | 3 | 0 | 11 |
| Itemised billing of invoices (Article 7) | 1 | 5 | 5 | 7 | 2 | 10 |
| Presentation and restriction of calling and connected line (Article 8) | 3 | 3 | 7 | 4 | 1 | 12 |
| Automatic call forwarding (Article 11) | 1 | 6 | 8 | 1 | 1 | 13 |
| Directories of subscribers (Article 12) | 3 | 5 | 8 | 5 | 0 | 9 |
| Unsolicited marketing communications sent and received through the Internet (Article 13) | 6 | 5 | 6 | 3 | 0 | 10 |

*Figure 1: Assessment of the functioning of the ePD provisions by the respondents to the public consultations (N=30), Deloitte*

The results of the two surveys are used throughout the consultant's study to justify and underpin the conclusions of the evaluation of the ePrivacy Directive, which are then directly used as an evidence basis for the problem definition. However, the answers did not reveal a widely shared opinion for most of the questions. Therefore, there has been an over interpretation of the results of these two surveys. The opacity of these surveys and their lack of representativeness make them unreliable as a viable source. This should have been explicitly acknowledged in the study, and the surveys should not have been used as the only source of evidence. This concern is expressed in Section 2.1.

Impact Assessment Institute

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

## 3.5 Phone interviews

46 interviews with stakeholders – mainly public authorities – were conducted. Annex B of the final report of the evaluation provides a general structure of these interviews (p.31 of the Annexes), but the content of the questions is not published. Only a summary of the content of the answers is displayed, making it complicated to assess the relevance of the answers. In addition to this, the same shortcomings as those of the surveys can be highlighted: little information is available about the respondents – their identity, a detailed description or their profile is unknown.

The answers to the interviews are cited as an input for the entire analysis of the relevance of the ePrivacy Directive, in Section 5 of the consultant's study. Nonetheless, it is hard to determine to what extent these answers were used as a source in the analysis, although there are a few mentions of the interviews throughout the section.

For instance, p.98 of the final report, it is stated that *"[o]n this basis, the fact that OTTs are not covered by the ePD were in particular considered to be problematic by Telecom providers interviewed by Deloitte."* The other sources mentioned for such a statement are the Terms of Reference, which cannot be considered as a proper source of factual information, and an academic article, in which only assumptions are made. Therefore, this statement is questionable as no other robust source is presented to support and confirm the opinions of the interviewees, on which – as is stated above – very little information is available.

This statement about an uneven playing field is used as the justification of the definition of Problem 1 and the extension of the scope of the new proposal. Basing such an important statement on unverifiable, intransparent and therefore highly unreliable sources is contrary to the Better Regulation principles and calls into question the conclusion which fed into the problem definition.

## 3.6 The "cookie sweep action"

This data-gathering process on the implementation of the provisions on cookies (Article 5(3) of the ePrivacy Directive) was carried out by the Article 29 Working Party. The information on this "sweep" is available in the Working Party's report[6].

The main findings of this sweep are displayed in the executive summary of the report. Some of them are mentioned in the consultant's study, but some of them have not been taken into account, even though they could have consequences for the determination of the best policy.

For instance, the findings of the "automated sweep" are particularly insightful. It is stated in the report that *"[t]he sweep highlighted differences in the use of cookies across different target sectors and between the individual member states."* Indeed, as shown in the report, the average number of cookies widely differs from one sector and/or country to another. For example, the average number of cookies in the British media sector is 15.7 times higher than

[6] Article 29 Working Party, "Cookie sweep combined analysis – report", 3 February 2015



Deleted: 170619d
Deleted: 17071
Deleted: 3
Deleted: f

in the Slovenian media sector. These high differences amongst Member States were not taken into account when assessing the options with regard to subsidiarity, although they could be relevant. Moreover, the differences in the technological and economic national contexts could help understand the variations from one Member State's transposition of the ePrivacy Directive to another.

Finally, although cookies are a common mechanism for tracking, they are not the only ones. Therefore, the cookie sweep is not representative of the reality of tracking on internet in Europe.

## 3.7 Workshops and various meetings

Annex 1 of the Impact Assessment provides a list of various meetings and workshops which the DG used as a source of information and evidence:

- Two workshops that were organised by the Commission, involving stakeholders and national authorities;
- Ad hoc meetings with stakeholders;
- Questionnaires sent to Member States on the implementation of Article 4(2) of the ePrivacy Directive.

Most of these sources were not explicitly mentioned in the Impact Assessment or the consultant's study. However, there are several mentions of the workshops as evidence for the consultant's analysis, but the minutes of the workshops were not published and have not been made available on request. It is therefore impossible to know which stakeholders and public authorities were represented at these meetings, and to what extent information from these meetings was used. This undermines the relevance and the validity of the conclusions which were drawn from the workshops. For instance, the workshops are cited as the only evidence that justifies the extension of the scope of the Regulation to metadata. This has significant implications, notably in terms of compliance costs.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

# 4 Analytical methodology

The analytical methodology of the Impact Assessment was set out by Deloitte in the "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector" (SMART 2016/0080). The main input data used by the consultant for this study has been reviewed above, in Section 3.

Deloitte's study is a 432 pages report, which comes along with 508 pages of Annexes mainly containing the data used for the study and the detailed national transposition checks of the ePrivacy Directive. The study is partly based on Eurostat data on European citizens and businesses. The scarcity of the data available, as well as the assumptions that were made in order to simplify the analysis, are clearly stated, in the final report as well as the draft study in Annex 8 of the Impact Assessment, and throughout the final report, which can be found on the Digital Single Market website of the Commission.

The introduction of the final report presents the scope and objectives of the study. Three questions are intended to be addressed, as presented on page 16:

- *What is the problem and why is it a problem?*
- *What are their economic, social and environmental impacts and who will be affected?*
- *How do the different options compare in terms of their effectiveness and efficiency (benefits and costs)?*

However, a full scrutiny of the final report shows that the study fails to address and assess the social and environmental impacts, focusing only on costs, without assessing the benefits of the various policy options. These shortcomings of the study should have been acknowledged in the final report, along with the statements on the scarcity of the available data. The results of the scrutiny of the consultant's study are displayed in the following sections.



## 4.1 Baseline and assumptions

In the table below, the Institute has scrutinised the pertinence and robustness of the four criteria used by the consultant to assess the impacts of the policy options:

| Criterion | Pertinence | Robustness of the estimate |
|---|---|---|
| **Number of citizens affected** | The study states that the number of citizens which are effectively affected by the proposal will not differ, no matter the option.<br><br>Legal persons are not taken into account, although the proposal includes legal persons in its scope. | The estimate was obtained by projecting the number of citizens affected back to 2002 and until 2030, based on Eurostat data and the CAGR of the data set.<br>However, the validity of CAGR to evaluate growth in the digital area over 28 years is highly questionable as the sector is highly disruptive and conditions are changing frequently. |
| **Number of businesses affected** | Only Business To Business (B2B) and Business to Client (B2C) communications are taken into account for this analysis, although other types of communications, particularly Machine to Machine | The criterion for businesses that are affected varies throughout the study:<br>- P.14 of the Annexes, by referring to the ITIF study, the percentage of websites having to comply with article 5(3) is 41.9% (not all the businesses |

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

| | | |
|---|---|---|
| | (M2M) communications such as the Internet of Things (IoT), and ancillary communications, are included in the scope of Policy Option 3 and the final proposal.<br><br>The assessment of B2B communications is pertinent as it enables the study to cover legal persons.<br><br>However, the scope of this analysis is too restricted and outdated, as it covers only websites using cookies, although personal data can be obtained through other means than cookies (see Section 8.3). | using cookies on their website are affected);<br>- P.13 of the Annexes, it is stated that potentially all businesses using cookies would be affected by Article 5(3) of the Directive. Therefore, not 41.9% but 50.2% of all businesses would be affected.<br><br>It is mentioned that, according to the cookie sweep action carried out by the Article 29 Working Party, an estimate of 70% of websites use tracking cookies only. This should be taken into account when assessing the Policy Options targeting only this type of tracking. |
| **Compliance costs** | The estimate only includes the costs related to Articles 5(3) and 13 of the Directive, although it is stated in the study that other costs that have occurred from the compliance with the rest of the Directive, are significant. In particular, opportunity costs related to Do-Not-Track default settings (p.370 of the final report). | The ITIF report 2014 is used as a source for the projection of the average compliance cost per website, regarding the implementation of Article 5(3). The ITIF report does not cite any public source for this estimate, and does not specify how it was calculated.<br>The only information given on this figure is that it supposedly includes "legal advice, updates to privacy policies, and technical updates to websites."<br>It is unclear whether or not these are the only costs taken into account to project this figure.<br><br>Another estimate is mentioned (€1150), but its source is not available, so it is impossible to break down this estimate. |
| **Costs stemming from administrative burden** | This criterion is relevant. | On page 132 of the study, it can be inferred from the key figures that amongst the businesses affected by the Directive and the various options, more than 89% are microenterprises (with less than 10 employees). However, the hourly labour costs are based on Eurostat data for businesses with more than 10 employees.<br><br>Although hourly costs for microenterprises are not available, it would have been appropriate to specify that the data used were not |

Impact Assessment Institute

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

| | | |
|---|---|---|
| | | accurate for most of the affected businesses, as there may be differences between the hourly costs of microenterprises and SMEs. |

*Table 2: Assessment of the criteria in the consultant's study*

It appears that further reflection should have been given to the definition of criteria, as the criteria are used as a basis to calculate the impacts. A general criticism that can be made about the criteria chosen by the consultant is that they only allow an assessment of the economic impacts of the Policy Options, whereas the main problems raised by the evaluation of the ePrivacy Directive were not only related to costs and burdens.

## 4.2 Presentation of Policy Options

The choice of the options presented in the consultant's final study is not supported by evidence or an explanation.

Overall, the descriptions of the options lack precision, particularly regarding the implementation plan. The presentation of Option 3, which is the most detailed of the 5 options, does not give any detail on which EU and/or national authorities will be responsible for enforcing the Regulation. Therefore there is no assessment of the costs related to the implementing acts which are necessary for Article 13(2), Article 16(4), Article 23(4) and Article 7(3), as stated in the proposal. As a result, the assessment and comparison of the overall expected costs figures is impossible.

A definition of "privacy friendly settings" in Policy Option 3 is not presented. It is unclear whether or not this means that the default settings are Do-Not-Track settings. It is not clear either whether or not first-party analytics are excluded from consent requirements, unlike in the current ePrivacy Directive. This is highly problematic as the consequences on businesses are important (see Section 8.3). Precision in the definition of Policy Options is essential for the Impact Assessment to be valid, since it determines the actual assuage possibilities in the future. Whenever provisions or elements were added in the proposal, without being primarily included in the Impact Assessment, it should have been clearly stated, to ensure transparency on the political decisions that were made.

## 4.3 Methodology

The consultant's study narrows the assessment of impacts to administrative and compliance costs. Social impacts are presented in the final tables summarising the impacts; there is a short description of the potential impacts, but there is no information on the data which was used to draw the conclusions. The section on methodology in the consultant's study does not provide information on the criteria used for this assessment either.

The methodology for assessing and comparing impacts is displayed in Section 9 of the study. Based on the data collected and inferred, the consultant assessed the impact of each Policy Option on a number of elements, and attributed ratings. These ratings, presented below, are displayed on page 413 and allow a comparison of the assessments in order to highlight the preferable option:

Deleted: Section

Deleted: Page

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

| Assessment criteria | Baseline scenario | Policy Option 1 | Policy Option 2 | Policy Option 3 | | | Policy Option 4 | | | Policy Option 5 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | "Browser solution" | "Tracking companies solution" | "Publisher solution" | "Browser solution" | "Tracking companies solution" | "Publisher solution" | |
| **Economic impacts** | | | | | | | | | | |
| Impacts on costs for businesses | 0 | 1 | 1 | -8 | -6 | -5 | -4 | -2 | -1 | -20 |
| Impacts on costs for public authorities | 0 | 14 | 0 | 3 | 3 | 3 | 4 | 4 | 4 | 2 |
| Other economic impacts | 0 | 0 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | -2 |
| **Effectiveness in reaching the policy objectives** | | | | | | | | | | |
| Objective 1: Ensuring effective confidentiality of communications | 0 | -1 | -2 | -3 | -3 | -3 | -3 | -3 | -3 | 3 |
| Objective 2: Ensuring effective protection against unsolicited commercial comm. | 0 | -1 | -2 | -3 | -3 | -3 | -3 | -3 | -3 | 2 |
| Objective 3: Simplifying the legal framework and adapting it to the new legal, market and technological reality | 0 | -1 | -2 | -3 | -2 | -2 | -3 | -2 | -2 | -3 |
| **Social impacts** | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| **Total** | 0 | 12 | -4 | -13 | -10 | -9 | -5 | -2 | -1 | -18 |

*Figure 2: Qualitative rating of the Policy Options by Deloitte*

These ratings should relate to the amount of costs or savings engendered, and the extent to which objectives are potentially achieved. However, a comparison of the various ratings and the changes in costs they represent has indicated inconsistencies.

As an example, under Policy Option 1, the administrative burden is expected to increase by 0.9% over the next 15 years. This evolution is rated -2[7]. Under Policy Option 3, the administrative burden would decrease by 10% over the 2016-2030 period, as compared to the baseline scenario. This decrease is also rated -2[8]. For Policy Option 4, the administrative burden is expected in the consultant's study to decrease by 3%. This is rated -3[9].

Therefore, the attribution of ratings is inconsistent, and the results that this analytical method generates are not reliable. The ratings would indicate that Option 5 is preferable according to the criteria that are used in the consultant's study. However, the Impact Assessment concludes that Option 3 is the most preferred option. Thus, it is impossible to know whether it is the consequence of a conscious choice, or an acknowledgment of the shortcomings of the consultant's study.

Impact Assessment Institute

[7] SMART 2016/0080, p.305

[8] Ibid, p.310

[9] Ibid, p.389

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

# 5 Impacts

In the following sections, the Impact Assessment Institute has reviewed each of the impacts which were assessed in the Impact Assessment, namely:

- The economic impacts (efficiency);
- The impact on SMEs, competitiveness and competition;
- Coherence with the internal market;
- The impact on Fundamental Rights;
- The impact on innovation.

The scarcity of the available data is explicitly acknowledged in both the consultant's study and the Impact Assessment. Even taking this scarcity into account, the assessments raise serious concerns.

## 5.1 Economic impacts

Regarding efficiency – the compliance costs, the opportunity costs and administrative burden, the assessment is necessarily limited by the lack of evidence. Opportunity costs were not assessed, due to the lack of available data. This is regrettable, as it is stated in Annex 7 of the Impact Assessment that the extent of these costs could be particularly important, and could have an impact on competition and competitiveness. These costs are also presented in the Impact Assessment as problematic for SMEs of Policy Option 3. A serious shortcoming of the Impact Assessment is the absence of an estimate of the number of citizens and legal entities which would potentially choose Do-Not-Track browser settings. Such an estimate is necessary to assess properly the potential economic impact of Policy Option 3, and proportionality of such measures in general.

Furthermore, the administrative costs for the Member States are not assessed and compared to the potential costs for the Commission if it were fully in charge of the implementation of some provisions. Therefore, the implementation plan does not rely on any evidence-based comparison of the possible options. The only costs which are assessed are the ones related to streamlining enforcement and consistency (P.35 and 38 of the Impact Assessment), and no source is cited for these estimates.

Finally, the assessment of the administrative costs related to the consistency mechanism is questionable. Policy Option 3 includes the competence of the European Data Protection Board on the consistency mechanism. The cost is estimated by the EDPS to be low for the EDPB as it already deals with electronic communications which are not covered by the Directive. The extension of the consistency mechanism to the enforcement of the ePrivacy Regulation is said in the Impact Assessment to *"ensure consistency, simplify the regulatory framework and thus reduce the administrative burden"*[10]. Nevertheless, on p.103 of the

[10] Final Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), SEC(2012) 72



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

GDPR's Impact Assessment, it is stated that the new consistency mechanism will entail additional costs and administrative burden for the DPAs and the EU budget (through the EDPS and the setting up of the EDPB). These costs are not only one-off costs, but also running costs. Therefore, it may be a simplistic approximation to assume that the extension of the consistency mechanism will not create additional costs, or at least costs that are too low to be properly taken into account.

## 5.2 Impacts on SMEs, competitiveness and competition

None of the policy options are assessed in relation to their potential effect on competitiveness, therefore including it in the title of the section on impacts gives a false indication of the content.

The Impact Assessment does not provide evidence on the effect of the policy options on competition, making only qualitative unreferenced statements on their potential outcome. For example, in the section on Policy Option 3 (p. 39), the assessment states:

> *"In general, the additional costs are expected to affect in proportion more heavily SMEs than bigger players, given the lower amount of resources and installed customer base that smaller firms can rely on."*

However, the potential consequences of this are not investigated. If they were significant, particularly for microenterprises, they could have a serious influence over market concentration.

A proper "SME test", according to the Better Regulation Toolbox[11], is a four-step process. The following table is an evaluation of the Impact Assessment's compliance with these steps:

| Better Regulation Toolbox:<br>Steps of the SME test | SME test in the Impact Assessment |
|---|---|
| *(1) Consultation of SME stakeholders* | The public consultation on ePrivacy did not target SMEs in particular. No information was required from the businesses about their size, and no question mentions SMEs.<br>The consultations do not provide enough information on the situation of SMEs faced with the ePrivacy Directive, the consequences of the ePrivacy rules and what they expect from the future Regulation. |
| *(2) Identification of affected businesses* | The businesses affected by the policy options have been identified, according to their size.<br>However, further information on their sector |

[11] Better Regulation Toolbox, p.129



Deleted: 170619d
Deleted: 17071
Deleted: 3
Deleted: f

| | |
|---|---|
| | of activity would have ensured a more comprehensive assessment of the consequences of the policy options on the different types of SMEs (for instance, browsers providers, or SMEs relying on OBA). |
| *(3) Measurement of the impact on SMEs* | This step should have included additional data on opportunity costs, and the consequences for the smallest enterprises. |
| *(4) Assessment of alternative mechanisms and mitigating measures* | This step does not appear in any part of the Impact Assessment, although it should have been considered, as it is relevant for example to market concentration. |

*Table 3: Compliance of the Impact Assessment with the Better Regulation Toolbox's framework for SME tests*

Overall, the SME test was not carried out according to the guidelines. The Impact Assessment only includes assumptions of potential impacts on SMEs without reference to evidence. This is an important shortcoming which therefore undermines the assessment in this section, because compliance costs are estimated in the Impact Assessment to be borne almost exclusively by SMEs, as mentioned in Section 4.1.

## 5.3 Environmental and social impacts

Environmental impacts were included in the Terms of Reference of the consultant's study and mentioned as an objective in its introduction. However, they were assessed neither in this study, nor in the final Impact Assessment. If no environmental impacts are expected, there should at least be an explanation for why they are expected not to be significant to support the choice not to assess them.

Regarding social impacts, the scope of the assessment was narrowed to "impact on employment and labour markets" according to page 23 of the consultant's study.

For Policy Options 0, 1, 2 and 3, a statement is made that no significant social impact is expected, without explanation or reference to evidence.

The impact on employment of Policy Options 4 and 5 is briefly assessed, without any cited source of evidence. This section includes statements on impacts on confidentiality, hence on Fundamental Rights, although this impact is not included in the intended scope of this part of the assessment, as mentioned above. There is a section on the impacts on Fundamental Rights.

The final Impact Assessment does not include any additional details in the assessment of the social impacts. Such a shortcoming undermines the relevance of the impact analysis.

## 5.4 Impacts on the internal market

This section of the Impact Assessment provides conclusions without supporting evidence on the impacts of the Policy Options on the achievement of a single market, which is not clearly defined. Indeed, the assessment includes statements on communications, comprising electronic communications and OTTs, but the Policy Options would potentially affect other



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

markets – particularly as Machine-to-Machine communications are also targeted. The potential impacts on the achievement of these markets are not taken into account. Thus, a clarification on what is assessed in this section would have been useful.

Further assessment of the impacts of the newly harmonised market – namely the OTT market, would have been relevant as well.

As regards Machine-to-Machine communications, the effects of the provisions were not assessed. As Machine-to-Machine communications are used in an increasing number of domains, the new provisions could potentially affect several branches of the EU economy, and affect their harmonisation. Therefore, the overall effect of the new provisions on the overall single market may have been underestimated.

## 5.5 Impacts on Fundamental Rights and Innovation

Provided that the legal basis of the proposal is Article 16 of TFEU, and that Objective 1 of the revision of the ePrivacy Directive is to ensure effective confidentiality of electronic communications, the assessment of the impact on Fundamental Rights should be central in this Impact Assessment.

Despite this, the policy options are simply deemed to comply with the rules on Fundamental Rights. As mentioned in Section 4.1, the criteria chosen by the consultant to carry out the assessment of the Policy Options do not allow a proper assessment of impacts other than economic impacts. The Terms of Reference for this study, provided upon request by the Commission, did not mention the need for an assessment of the impacts on Fundamental Rights. On the contrary, the Commission required the consultant to assess the impacts of the various Policy Options, "notably from an economic perspective."[12]

However, the compliance of a number of provisions of the proposal with Fundamental Rights is questionable. As developed in Section 8.1, the new provisions on consent via browser settings may not be in line with the notion of consent as provided in the GDPR.

The same conclusions can be drawn from the lack of coherent assessment of the impacts on innovation. Although it is acknowledged that the compliance costs entailed by the new provisions could potentially limit the capacity of innovation for businesses, there is no assessment of the extent of this negative consequence, nor of any potential positive effect on innovation. No source or evidence is provided in the Impact Assessment. The consultant's study does not assess these impacts either.

Moreover, the short period of time which would be given to businesses to comply with the ePrivacy Regulation if it was made applicable in May 2018, as provided in the proposal, could

[12] Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector SMART 2016/0080, Terms of Reference, p.7



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

be expected to have a significant impact on innovation, as stated in the Better Regulation Toolbox[13]. Therefore, it should have been further assessed.

Innovation could play a major role in the increase in data flows, which are a central objective of the Digital Single Market strategy; it could also create new solutions to ensure better control over personal data. Therefore, assessing the long term effects of this Regulation on innovation would have been coherent with both the specific objectives of the Regulation and the objectives of the overall Commission's strategy.

## 5.6 Impact on international trade

The impact on international trade is not included in the main body of the Impact Assessment. However, the new provisions proposed in the policy options may have consequences on the external exchanges which could be as important as the ones on the internal market. This potential impact is briefly evoked in Annex 5 and Annex 7. In particular, it is mentioned in Annex 7 that the extension of the scope of ePrivacy rules to OTT services could be a barrier to trade, as most of the OTT services are located outside the Union, and partly financed by the incomes from Online Behavioural Advertising (OBA) in the Union. Annex 5 gives an indication of what OBA may represent in terms of profits from non-European companies:

> *"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"*.

In 2016, the European Audio-visual Observatory also highlighted the fact that no European company was amongst the top companies in display advertising spend revenue[14]. As can be seen in the figure below, Google and Facebook are also dominating the European display ad market.

Impact Assessment Institute

[13] Better Regulation Toolbox, p. 122

[14] European Audiovisual Observatory, "The online advertising market in the EU. Update 2015 and Focus on programmatic advertising", August 2016, p.3

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

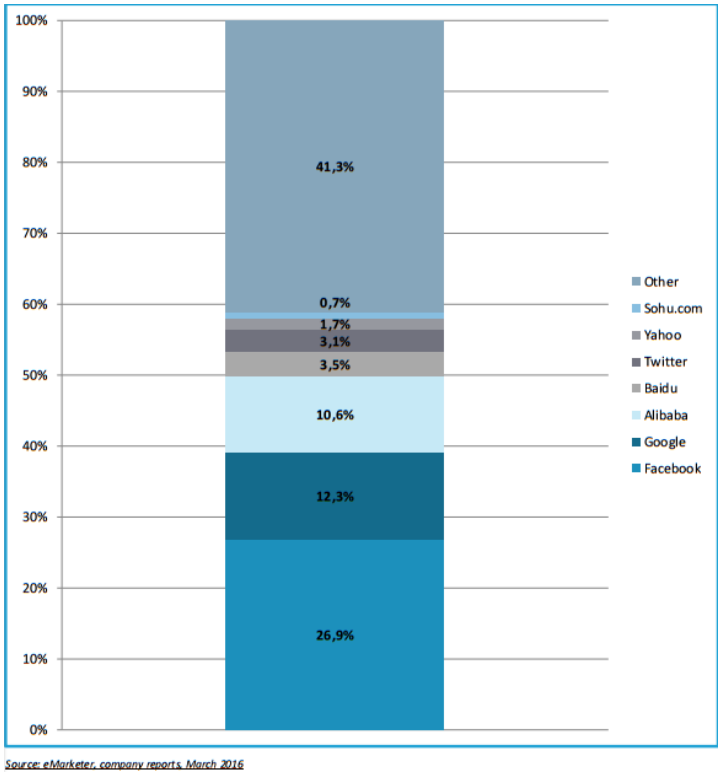



*Figure 3: Share of worldwide net display ad revenues by company, in % of share, 2016, European Audio-visual Observatory, 2016*

According the European Audiovisual Observatory, without any change in the economic and legal context, the trend is likely to continue.[15]

Such a regulation could therefore potentially act as a trade barrier for non-European businesses, and in parallel, modify the structure and the competition within the global digital market. Therefore, assessing the impact on international trade appears to be particularly relevant.

[15] European Audiovisual Observatory, "The online advertising market in the EU. Update 2015 and Focus on programmatic advertising", August 2016, p.4

Impact Assessment Institute

**Deleted:** Ibid,

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

# 6 Coherence with the legislative proposal

## 6.1 Feasibility of the comparison

The consultant's study assesses the costs for public entities and businesses, and in particular SMEs, and the social impacts, as announced in the final report. Despite its limited scope, it does not equally assess the impacts of every option, nor does it assess all the impacts in an equal way. Therefore, it undermines the value of the comparison.

## 6.2 Outcome of the comparison

The outcome of the comparison is that Policy Option 3 is the best option, provided that two of its provisions are eliminated:

- Measure 4 *"Require opt-in consent for all types of unsolicited communications covered by the current rules"*: voice-to-voice marketing calls are excluded;
- Measure 10 (e) *"Providing for additional/broadened exceptions to confidentiality/permitted uses for specific purposes which give rise to little or no privacy risks […] For a lawful business practice (e.g. OBA) where the processing is strictly limited to anonymised or pseudonymised data and the entity concerned undertakes to comply with specific privacy safeguards"*: this provision is eliminated.

Stating explicitly which provisions were excluded is transparent, but there is a lack of justification for the exclusion of these provisions.

Overall, the main provisions of the preferred option are included in the proposal, but some of the provisions of the proposal differ from the outcome of the Impact Assessment.

For instance, Article 12(1) d. provides additional provisions requiring the providers of publicly available number-based interpersonal communications services to allow the called end-user to hide its line identification. This provision was not assessed in any part of the Impact Assessment, although it is likely to entail costs for calling end-users, and it may not always be technically feasible.

Other additional provisions are likely to entail compliance costs for service providers, which were not addressed, such as Article 12(2) and Article 14, which provide that all the possibilities offered to protect the end-user's privacy must be free of charge.

Additional discrepancies due to a lack of precision in the proposal can be noted. Although the preferred option in the Impact Assessment highlights the need for identical rules for ECS providers and OTT providers, the proposal introduces several differences:

- The metadata included in the scope of the proposal, namely Article 6(2), is electronic communications metadata; this excludes metadata processed in other types of communications;
- OTT providers from outside the EU do not fall into the scope of the proposal, as only "electronic communications data processed in connection with the provision of electronic communications services from outside the Union" are mentioned in Recital 9;
- Direct marketing communications falling in the scope of the proposal only include advertising, by the means of electronic communications, according to Article 4(3) (f) of the proposal. Therefore, other types of direct marketing communications are



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

excluded, such as advertising trough OTTs, or direct marketing for purposes other than advertising;

- The exemption for "web audience measuring" stated in Article 8(1) (d) of the proposal does not provide a legal framework for exemptions in the case of communications such as Machine-to-Machine communications (IoT), or web applications.

These discrepancies put into question the technological neutrality of the proposal, and undermine the achievement of the objective of creating a "level-playing field".

These modifications should have been explicitly mentioned and justified in the proposal, as they differ from the original objectives of the proposal.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

# 7 Compatibility with other EU policies

One of the main issues raised by the review of the ePrivacy Directive is the lack of coherence with the overall regulatory framework on data protection and communications. The Commission seeks to tackle this issue in the new proposal, by ensuring consistency, particularly regarding the scope, the implementation and monitoring strategy and the enforcement mechanism.

However, although coherence of the ePrivacy Directive with other pieces of legislation – namely the GDPR, the Electronic Communications Package, the Radio Equipment Directive, and the NIS Directive – was thoroughly analysed in the consultant's study (Annex E), such analysis was not conducted for the policy options. Such analysis is all the more important because inconsistencies can be found in the proposal. These are described below.

Compatibility is a main issue raised by the review of the ePrivacy Directive, and it is a matter of legal certainty. Therefore, where possible, the potential consistency or inconsistency of the future legislation should be assessed, especially in the cases where the proposals' legislative processes are intentionally synchronised, or the content of the proposals are related.

## 7.1 Compatibility with the legislative framework

### 7.1.1 Consistency with the GDPR

The General Data Protection Regulation has been cited throughout the evaluation and the Impact Assessment process, as the main piece of legislation for which coherence should be ensured, both from a formal and material point of view. Despite this, a number of inconsistencies can be noted.

First of all, the GDPR clearly differentiates between data controllers and data processors, while the ePrivacy proposal does not. Controllers are responsible for the implementation of the GDPR, but it is unclear whether the processors are also given responsibilities in the ePrivacy Regulation. This creates legal uncertainty for the actors which would face difficulties understanding which rules to comply with.

Furthermore, the processing of data is allowed for specific cases, as provided in Article 6 of the ePrivacy Regulation's proposal. However, the scope of this article differs from the scope of Article 6 of the GDPR, which defines different circumstances in which the processing of personal data is allowed: the scope of allowed processing is narrower in the ePrivacy proposal. This could potentially create legal uncertainty for the service providers in some cases.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

Overlaps can also be noted between the GDPR and the proposal. As raised by the EDPS in its latest opinion[16], in certain circumstances, both regulations can apply, with different rules. For instance, when the end-user gives consent to the control of personal data by a third party, it is unclear whether further processing, controlled by the third party, should comply with Article 6 of the GDPR or Article 6 of the ePrivacy Regulation. The provisions in these two articles differ. An objective of the review and the revision of the ePrivacy Directive was to eliminate all potential overlaps. Thus, the articulation of the two Regulations should have been further addressed, as early as the Impact Assessment, in order to ensure proportionality and clarity in the proposal.

### 7.1.2 Consistency with the EECC

The current Directive on the European Electronic Communications Code (EECC) is currently being revised, and a proposal has been published by the Commission in September 2016.

The ePrivacy proposal refers to the EECC Directive for a number of definitions, in Article 4(1): 'electronic communications network', 'electronic communications service', 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service', 'end-user' and 'call'. These definitions may evolve, in view of the new EECC Directive, which will probably be adopted after the ePrivacy Regulation (see Section 7.2). The definition of 'end-user' and 'electronic communications services' are particularly important for the latter. This situation may create legal uncertainty over some of the provisions of the ePrivacy Regulation.

## 7.2 Coherence of the timelines

The timeline for ePrivacy Regulation's proposal is inconsistent with the timeline of related pieces of legislation, particularly the GDPR.

According to Article 29 of the proposal, the ePrivacy Regulation "shall apply from 25 May 2018". This date is in line with the date of application of the GDPR. The reason evoked for this alignment of the dates of application of these two instruments is consistency. The strong interconnection of these two pieces of legislation justifies the need for coherent timelines.

However, consistency was not sought for the instruments of the regulatory framework for electronic communications, of which the ePrivacy Regulation is a component. For instance, there is no consistency between the timelines of the EECC – which is a directive – and the ePrivacy Regulation. Article 115 of the proposal for a Directive establishing an EECC, does not mention a date of application. This is mainly because the date of application will be left up to the Member States. As mentioned in Section 7.1, it is likely that some modifications will be made to the EECC proposal throughout the legislative process. These modifications

[16] EDPS opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), p.15



Deleted: 170619d

Deleted: 17071

Deleted: 3

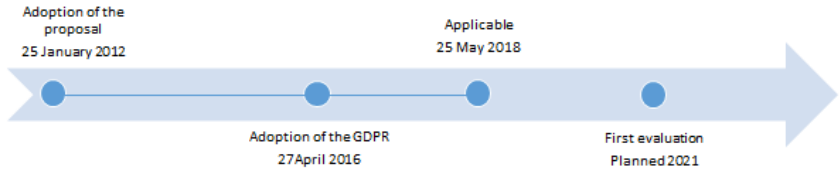
Deleted: f

could affect the definitions used in the ePrivacy Regulation, and therefore lead to legal uncertainty.

Therefore, it is not clear why the Commission is seeking full consistency with the GDPR's timeline and not the EECC's timeline. The following analysis indicates the challenges associated with this timeframe.

Hereinafter are the planned timelines for the GDPR and the ePrivacy Regulation:

- **Timeline for the GDPR**




- **Timeline for the ePrivacy Regulation**

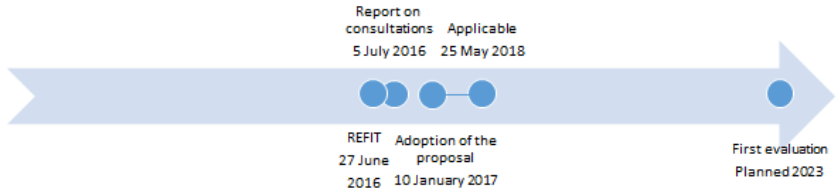



*Figure 4: Comparison of timelines of the GDPR and the ePrivacy Regulation*

As shown in the timelines above, there is an important difference between the pace of the legislation process in the case of the GDPR, and the projections for the ePrivacy Regulation. The GDPR will start to apply more than six years after the proposal was adopted by the Commission. As for the ePrivacy Regulation, if it is implemented by the planned date, there will only be 16 months between the publication of the proposal and the application of the legislation. Due to the expected time needed for completion of the legislation, this will leave little time for businesses to comply with the new rules. In the case of the GDPR, two years were allowed. For ePrivacy, in the best case the time would be a few weeks.

It therefore appears very unlikely that the legislative process for the ePrivacy Regulation can remain within the deadlines set in the proposal, without compromising the quality of the adopted legislation.

A second issue can be raised from the timeline that was chosen by the Commission for the ePrivacy Regulation. Some of the provisions in the proposal directly refer to the GDPR. This is especially the case of the enforcement mechanism, also called "consistency mechanism", described in Articles 18-19-20 of the proposal. As the GDPR will only fully apply in May 2018, the ePrivacy provisions are only based on the first assessment made for the GDPR, and not on actual evidence from its implementation.

In assessing the effects of the consistency mechanism, the GDPR's Impact Assessment states *"it is difficult to establish the balance between these effects as this will depend very much on the current size and resources of Data Protection Authorities, the cases they will have to be*



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

*involved in etc."*[17] Besides, the objectives of the consistency mechanism are different in the GDPR and the ePrivacy Regulation. The same mechanism is justified in two different ways. As for the GDPR, *"The new cooperation and consistency mechanism between DPAs will ensure that their concerns are taken into account as they would be able to intervene in cases concerning their citizens and or affecting their country"*[18]. However, the ePrivacy regulation's Impact Assessment emphasises on the mechanism being a solution to the divergences of interpretation, and therefore the disruptions of the internal market[19].

Therefore, it is problematic to include in a new piece of legislation a mechanism which impacts have not been properly assessed, according to different objectives and which is not applicable yet, hence without any hindsight.



[17] SEC(2012) 72 final, p.103

[18] Ibid

[19] SWD(2017) 3, p.46

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

# 8 Specific provisions

## 8.1 The "browser solution"

The browser scenario is the first of three scenarios envisaged for the revision of Article 5(3) of the ePrivacy Directive, on consent regarding the storing of information or the access to information stored in the terminal equipment. The outcome of the assessment in the consultant's study is that this option is the best solution to replace the current provisions.

These changes are estimated to have a significant impact, both on the economy as well as on fundamental rights. Nonetheless, the Impact Assessment falls short of fully addressing the consequences of the new provisions.

First and foremost, the economic assessment is limited, on several aspects.

For the purpose of calculating economic impacts, it is assumed that, under the browser scenario, the costs would be borne only by browser providers, therefore eliminating the compliance costs for all the other businesses with a website using tracking technologies.

Compliance costs for other types of businesses cannot be eliminated without an explanation. One-off costs such as the cost of modifying the website back to how it was before Article 5(3) came into force, or the cost of sharing information with the browser companies, may require a proper assessment.

The Annexes of the consultant's report include the table below:

| Average annual value | REFIT | Today | Baseline scenario | Policy Option 1 | Policy Option 2 | Policy Option 3[39] | | | Policy Option 4 | Policy Option 5 |
|---|---|---|---|---|---|---|---|---|---|---|
| | (2002-2015) | (2016 snap shot) | (2016-2030) | (2016-2030) | (2016-2030) | (2016-2030) | | | (2016-2030) | (2016-2030) |
| | | | | | | "Browser" | "Tracking companies" | "Publishers" | | |
| Number of businesses affected (in million) | 2.84 | 3.11 | 3.70 | 3.70 | 3.89 | 0.19 | 0.74 | 2.22 | 0.37 | 0.00 |
| Micro-enterprises | 2.53 | 2.78 | 3.31 | 3.31 | 3.48 | 0.17 | 0.663 | 1.99 | 0.33 | 0.00 |
| SMEs | 0.26 | 0.25 | 0.26 | 0.26 | 0.27 | 0.01 | 0.052 | 0.16 | 0.03 | 0.00 |
| Large enterprises | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | 0.00 | 0.002 | 0.01 | 0.001 | 0.00 |
| Foreign controlled enterprises | 0.05 | 0.06 | 0.12 | 0.12 | 0.13 | 0.01 | 0.024 | 0.07 | 0.01 | 0.00 |
| Compliance costs (in million Euro) | 1,861.7 € | 1,505.7 € | 1,355.4 € | 1,423.15 | 1,558.7 € | 406.6 € | 542.152 | 1,287.6 € | 1,287.6 € | 0.0 € |
| Micro-enterprises | 1,655.8 € | 1,349.0 € | 1,213.0 € | 1,273.6 € | 1,394.9 € | 363.9 € | 485.188 | 1,152.3 € | 1,152.3 € | 0.0 € |
| SMEs | 169.8 € | 122.2 € | 97.0 € | 101.9 € | 111.6 € | 29.1 € | 38.808 | 92.2 € | 92.2 € | 0.0 € |
| Large enterprises | 5.6 € | 4.2 € | 3.3 € | 3.5 € | 3.8 € | 1.0 € | 1.332 | 3.2 € | 3.2 € | 0.0 € |
| Foreign controlled enterprises | 30.5 € | 30.3 € | 42.1 € | 44.2 € | 48.4 € | 12.6 € | 16.823 | 40.0 € | 40.0 € | 0.0 € |
| Average compliance cost per business (in Euro) | 658.4 € | 484.5 € | 373.5 € | 392.2 € | 409.1 € | 2,240.9 € | 746.978 | 591.4 € | 3,548.1 € | 0.0 € |
| Administrative burden (in million Euro) | 0.28 € | 0.23 € | 0.23 € | 0.23 € | 0.21 € | 0.208 € | 0.226 € | 0.23 € | 0.22 € | 0.00 € |
| Micro-enterprises | 0.23 € | 0.19 € | 0.18 € | 0.18 € | 0.16 € | 0.163 € | 0.178 € | 0.18 € | 0.18 € | 0.00 € |
| SMEs | 0.03 € | 0.03 € | 0.03 € | 0.03 € | 0.03 € | 0.031 € | 0.033 € | 0.03 € | 0.03 € | 0.00 € |
| Large enterprises | 0.00 € | 0.00 € | 0.00 € | 0.00 € | 0.00 € | 0.002 € | 0.002 € | 0.00 € | 0.00 € | 0.00 € |
| Foreign controlled enterprises | 0.02 € | 0.01 € | 0.01 € | 0.01 € | 0.01 € | 0.013 € | 0.014 € | 0.01 € | 0.01 € | 0.00 € |
| Average costs from admin. burden per business (in Euro) | 48.9 € | 36.0 € | 27.8 € | 28.0 € | 23.8 € | 499.5 € | 135.982 € | 45.33 € | 269.2 € | 0.0 € |

*Figure 5: Quantitative assessments concerning businesses (absolute values), Deloitte*

As regards the Policy option 3, the criteria which are used for the cost assessment – specifically, the compliance costs and the administrative burden in million euros – do not provide the information that is necessary to determine which scenario is the most cost-efficient. Indeed, only average costs for all types of businesses, regardless of their activity (browser providers, businesses running a website etc.), are estimated. Thus, the interpretation of the figures is ambiguous. This flaw is acknowledged in a footnote, but no further information about the limits of this assessment is provided in the final report. The table provides average costs per business, although the footnote states that such costs are impossible to assess for Policy option 3. The overall method used for calculating the average administrative burden per business is opaque.

Impact Assessment Institute

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

The only remaining criterion used for comparing the different solutions is the number of businesses that would bear the costs. Consequently, the browser solution is seen as "the best scenario" is because fewer companies bear the costs than in other scenarios. This conclusion is problematic, as the amount and the sustainability of the costs for browser companies are not commented. Amongst the businesses affected – hence the browser providers – a large majority of them are micro-enterprises (170 000 out of 190 000). The browser market is a very concentrated market, as can be seen below:

| **Market share held by internet browsers in Europe from January 2016 to January 2017, in %** | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Chrome | Firefox | IE | Safari | Opera | Android | Others |
| Jan '16 | 48,6 | 19,1 | 12,4 | 11,2 | 3,0 | 1,6 | 4,1 |
| Feb '16 | 48,4 | 19,7 | 12,2 | 11,0 | 3,1 | 1,5 | 4,2 |
| Mar '16 | 48,7 | 19,5 | 11,8 | 11,2 | 3,0 | 1,5 | 4,4 |
| Apr '16 | 49,6 | 19,1 | 11,2 | 11,1 | 2,9 | 1,5 | 4,6 |
| May '16 | 50,2 | 19,1 | 10,3 | 11,4 | 2,9 | 1,4 | 4,7 |
| Jun '16 | 50,1 | 19,2 | 10,1 | 11,5 | 2,7 | 1,4 | 5,0 |
| Jul '16 | 49,9 | 19,3 | 9,7 | 11,4 | 2,7 | 1,6 | 5,5 |
| Aug '16 | 50,2 | 19,3 | 9,3 | 11,1 | 2,8 | 1,5 | 5,7 |
| Sep '16 | 50,7 | 19,0 | 9,2 | 11,2 | 2,7 | 1,4 | 5,8 |
| Oct '16 | 50,4 | 18,8 | 8,6 | 11,5 | 3,5 | 1,3 | 6,0 |
| Nov '16 | 50,2 | 18,9 | 8,7 | 11,8 | 3,1 | 1,3 | 6,0 |
| Dec '16 | 50,5 | 18,7 | 8,4 | 11,8 | 2,9 | 1,3 | 6,4 |
| Jan '17 | 50,3 | 18,5 | 8,7 | 12,3 | 2,6 | 1,3 | 6,3 |

*Table 4: Market share held by internet browsers in Europe from January 2016 to January 2017, in %, Statista*

These figures were extracted from *Statista*; the data may slightly differ from a source to another but all of them confirm the concentration of the market. The study fails to assess the sustainability of the compliance costs and administrative burden for micro-enterprises; as a consequence, it also fails to assess the risks for even higher market concentration.

In addition to this, as mentioned in Section 2.1, the main cause for the lack of effectiveness of the current rules on consent is their lack of flexibility. This concern is neither addressed in the Impact Assessment, nor in the consultant's study. Flexibility is directly related to the notion of specificity of consent, provided in the GDPR as follows:

> *"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*

The consultant's study briefly mentions some potential shortcomings, such as the inevitable limited choice of settings, and the issue of consent through applications which do not require a browser. Nevertheless, previous assessments of the "browser solution" regarding its compliance with the notion of consent, detailed below, are not taken into account.

A first assessment was made in Opinion 2/2010 of the Article 29 Working Party. In this opinion, specific issues related to the implementation of the browser solution were raised.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

To overcome these issues, the Working Party set two conditions[20], which can also be found in the 2013 study on ePrivacy[21]:

- The consent must be prior to the processing and specific;
- Specific information about the purposes of the technologies used must be provided.

The Working Party concluded that, should the new provisions fail to meet these two conditions, consent by the way of browser settings would not be considered as informed consent.

The 2016 Flash Eurobarometer survey on ePrivacy does not provide sufficient data that would confirm that the browser solution is preferred by the citizens. While 69% of respondents would totally agree to have default browser settings that prevent information from being shared, only 48% would like to be asked for consent the first time they enter a website, and 39% would rather be asked each time they enter a website. As there is no predominant view on this matter, one cannot infer from the answers of this survey that citizens are in favour of the browser solution. Thus, it is uncertain whether these new provisions will solve one of the shortcomings of the current Directive – the end-users giving their consent without seeking sufficient information.

This issue is raised again by the Article 29 Working Party in its latest opinion 1/2017, along with the inconsistency of the proposal with the principles of privacy by design and by default, laid down in Article 25 of the GDPR.

Therefore, the Impact Assessment does not fully assess the impact of the browser solution on the Fundamental Right to privacy.

Further, as mentioned in Section 5.1, scenarios for the end-users' choice of settings should have been envisaged, in order to assess the potential effect on businesses, particularly those relying on the incomes of OBA.

Finally, Article 9(3) on consent in the proposal provides that end-users shall be *"reminded of this possibility at periodic intervals of 6 months, as long as the processing continues."* Re-obtaining consent every six months could be expected to lead to additional costs and burdens which were not assessed. In addition to this, it undermines the initial objective of simplifying the consent requirement for end-users.

## 8.2 The tracking walls

Policy option 4 includes the prohibition of the practice of denying access to a website for end-users who refuse to consent to tracking. This practice is also called "tracking walls", although a tracking wall is not necessarily the only technique for forcing the end-user into allowing access to personal data.

[20] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, p.14-15

[21] SMART 2013/0071, p.12-13



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

Businesses which would be affected by this ban are estimated in the consultant's study to face a "significant increase" of their IT costs (one-off costs), as well as "a loss of revenue" due to the potential decrease in their advertising incomes[22].

This assessment of the economic impacts for businesses contains a number of shortcomings.

First of all, no information is available on the number of businesses which resort to tracking walls on their website, and therefore would be affected by the ban. As mentioned in Section 4.1, the way in which the costs were estimated is not transparent as the source is not available. The negative assessment of the costs for businesses cannot be concluded from the limited evidence that is available. The same criticism can be made of the assessment of social impacts, namely the negative effects on employments which are dependent on Online Behavioural Advertising (OBA).

The results of the public consultation on the ePrivacy Directive provide relevant information on this matter, which was only partly taken into account, particularly the answers to Question 22[23]. When asked if they would agree that information service providers should not have the right to prevent access to their non-subscription based services in case users refuse the storing of identifiers in their terminal equipment (option 2), 76,6% of respondents that were citizens, consumer and civil society organisations and 70% that were public bodies agreed. A high proportion of the industry respondents, however, disagree (75,8%). As stated in the synopsis report of the consultations, the main argument given by those against such a provision is that it goes against business models based on OBA. This argument is mentioned in the consultant's economic assessment of Policy option 4.

No further information about the impacts of tracking walls, or diverging opinion, is cited by the consultant's study or the IA. The 2014 "cookie sweep action" carried out by the Article 29 Working Party did not test the extent of such a practice, nor did the Eurobarometer on ePrivacy in 2016. However, in the latter, a question addresses an issue which can be related to the practice of tracking walls:

[22] SMART 2016/0080, p.381

[23] *Question 22: The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated critics that citizens do not have a real choice. To what extent do you agree to put forward the following measures to improve this situation?*



Impact Assessment Institute

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

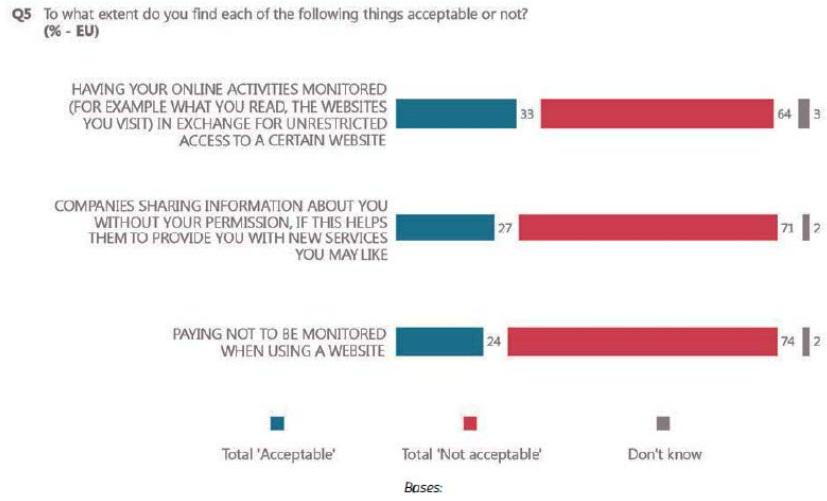



*Figure 6: Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079), p.55*

Although this question does not explicitly address the issue of tracking walls, the answers indicate that this is seen by citizens as a particularly important issue for privacy. The impact on fundamental rights on whether to implement a ban on tracking walls should have been further assessed, in particular, as noted by the Article 29 Working Party[24], with regards to the right to access information and online content.

In its Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240), the Article 29 Working Party identified five cases in which tracking walls should be forbidden in particular:

> *"1. Tracking on websites, apps and or locations that reveal information about special categories of data (health, political, sexual, trade union etc.). Even if visits to services providing information about such special categories of data do not disclose in themselves special categories of data about these users, there is a high impact on the private life of those users if they are labelled as being interested in such information;*
>
> *2. Tracking by unidentified third parties for unspecified purposes. This is for example the case when a website or app auctions its advertising space, and unknown third parties may actually start to track the users through the website or app;*
>
> *3. All government funded services;*

[24] Article 29 Working Party, Opinion 1/2017 on the Proposed Regulation for the ePrivacy Regulation, point 20



Deleted: 170619d
Deleted: 17071
Deleted: 3
Deleted: f

*4. All circumstances identified in the GDPR that lead to invalid consent, such as for example an unequal balance of power, if there is no equivalent alternative, or forced consent is part of a contract;*

*5. Bundled consent for processing for multiple purposes. Consent should be granular."*

A similar opinion was expressed by the European Data Protection Supervisor (EDPS), which supported a ban – complete or partial – in its review of the ePrivacy Directive in 2016[25] and its opinion on the ePrivacy proposal in 2017[26], for the reason that such a practice barely meets the requirements of the ePrivacy Directive, and goes against the new, more specific definition of consent, provided by the GDPR. Recital 42 of the GDPR provides that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

The two possibilities – a complete ban on tracking walls or a partial ban affecting the most sensitive cases – are not addressed in the IA. A partial ban has been implemented in the Netherlands since February 2015. Including a case study on this implementation would have been relevant to assess the potential impacts of such legislation.

In line with the EDPS and the Article 29 Working Party, the Body of European Regulators for Electronic Communications (BEREC) also issued an opinion in 2016[27], suggesting amendments to the ePrivacy Directive, to include more specific provisions on tracking walls, namely the situations when it would be forbidden to deny access for users who tracking.

Finally, the consultant's survey shows that 22 out of 28 competent public authorities considered tracking walls as a problem (moderate or serious). No further information is given about the reasons for these answers and the nature of these authorities.

| | Not at all a problem | Minor problem | Moderate problem | Serious problem | Cannot answer |
|---|---|---|---|---|---|
| The consequences of giving consent is not clear to all users (e.g. the possibility of tracking) | 0 | 1 | 6 | 17 | 4 |
| It is not always clear whether a given consent is valid, e.g. if given via the configuration of browser settings | 1 | 2 | 8 | 13 | 4 |
| Users do not have a real choice, as websites often deny access to websites if cookies are refused | 1 | 1 | 10 | 12 | 4 |
| The rules are vague and leave a lot of room for interpretation to the competent authorities | 1 | 3 | 5 | 13 | 6 |

*Figure 7: Challenges reported in the context of Article 5(3) (N=28), Deloitte*

[25] EDPS opinion 5/2016, on the Review of the ePrivacy Directive (2002/58/EC), p.14-15

[26] EDPS opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), p.16

[27] BEREC Response to the ePrivacy Directive questionnaire, BoR (16) 133, p.15

Impact Assessment Institute

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

These opinions are not taken into account and further discussed. Therefore, the Impact Assessment and the consultant's study have not gathered sufficient input data and opinions, in order to make an evidence-based decision on whether to implement a complete or partial prohibition of tracking walls and other types of restrictions of access for users who refuse to consent to the tracking and processing of their personal data.

## 8.3 Tracking by first and third parties

The ePrivacy Regulation distinguishes tracking by first parties and tracking by third parties. This distinction raises a number of issues.

In the Impact Assessment, the new provisions on tracking under Policy Option 3 are described as follows:

> *"Under the new rules, users would be prompted at the moment of the first utilisation of the equipment to choose their privacy settings among a specifically established set of privacy options, ranging from higher (e.g. "reject third party cookies" /"do not track") to lower levels of privacy protection."*[28]

Do-Not-Track settings are the highest level of protection of confidentiality, as they prevent any tracking, by third parties and first parties. However, the provisions in Article 10 of the ePrivacy proposal differ from this definition, as Do-Not-Track settings are not mentioned. Article 10 only provides that software applications (such as browsers) shall enable end-users to "*prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.*" Therefore, tracking by first parties is exempt from mandatory consent of the end-users.

The distinction that is implicitly made in the proposal between these two types of tracking is not included in the Impact Assessment. Nevertheless, such a distinction could potentially have significant effects.

First of all, it could undermine the effectiveness of the proposal, which was meant to create a level-playing field between all the economic actors (see Section 2.1). Although OTT services and electronic communications services would be subject to the same rules, an uneven playing field would emerge between websites relying on first-party tracking, and those using third-party tracking as they cannot have access to enough information via first-party analytics. First-party and third-party tracking can have the same purpose, namely OBA. Thus in this case, competition advantages in OBA could potentially directly arise from this Regulation.

Moreover, as shown in the figure below, businesses relying on first-party analytics are also the market leaders in third-party advertising. The market leader holds 69% of the global advertising networks market, and 80% of the global analytics and tracking market.[29]

[28] SWD (2017) 3, part 1/3, p.23

[29] https://www.datanyze.com/market-share/



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

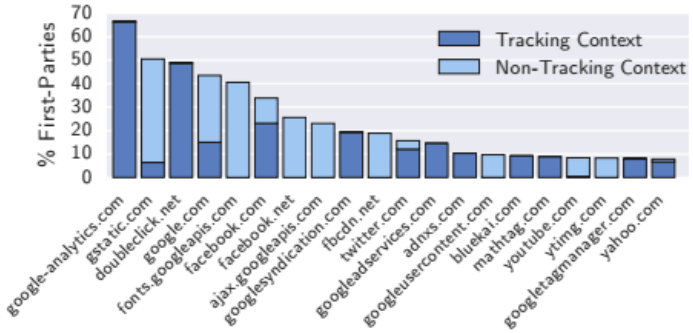



*Figure 8: Top third parties on the top 1 million sites, Englehardt & Narayanan* [30]

Therefore, including a distinction between first-party and third-party tracking, without assessing its economic consequences, in particular for competition on an already highly concentrated market, puts into question the economic assessment of the new provisions.

Furthermore, technological neutrality is presented as a key attribute of the revision of the ePrivacy Directive. However, in the case of tracking, the provisions in Article 10 may not be neutral enough to be applicable to all current and future techniques. For instance, the global leaders in advertising are already using new tracking techniques, such a SSO (*Single Sign-On*), or IDFA (*Identifiers For Advisers*). The assessment of whether the new rules would be relevant and applicable to these techniques is non-existent. As a result, this could potentially create imbalances and legal uncertainty.

Impact Assessment Institute

[30] Steven Englehardt, Arvind Narayanan, "Online Tracking: A 1-million-site Measurement and Analysis", *ACM CCS*, 2016

**Deleted:** 170619d

**Deleted:** 17071

**Deleted:** 3

**Deleted:** f

## Annex I: Accompanying statement

This report has been written according to the guiding principles of the Impact Assessment Institute: transparency, objectivity, legitimacy and credibility. It analyses the subject matter from a purely factual and scientific point of view, without any policy orientation. In respecting these principles it has been compiled following its written Study Procedures[i].

The analysis is open to review and criticism from all parties, including those whose work is scrutinised. Contacts with all relevant parties are recorded to ensure transparency and to guard against "lobbying" of the results.

By its nature the report has a critical characteristic, since it scrutinises the subject document with its main findings entailing the identification of errors, discrepancies and inconsistencies. In performing this work, the intention of the report is to be constructive in assisting the authors of the subject document and its background information as well as all relevant stakeholders in identifying the most robust evidence base for the policy objective in question. It should therefore be seen as a cooperative contribution to the policy making process.

This report is also to be considered as a call for additional data. Peer review is an essential step laid down in the procedures of the Impact Assessment Institute and this is manifested in the openness to further review and to identify new data. Even at publication of the final version, the report explicitly requests additional data where the readily available data was not sufficient to complete the analysis, and is open to newly arising data, information and analysis.



Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f

## Annex II: Responses to comments received from stakeholders on draft report

Comments received from stakeholders to IAI's draft reports are taken into account in the compilation of the final report. The comments are recorded, commented upon by the IAI below, with action taken where new evidence or analysis has thus been highlighted.

In response to the draft report sent for review on 19th June 2017, one comment was received, recorded in the following table along with comments from the IAI:

| Organisation | Feedback received | IAI response |
|---|---|---|
| A think tank active in the policy domain | Suggesting that the process has been too quick might not be advisable because, if anything, we need to speed up the legislative process. Any effort in this direction should be appreciated - as long as there is still a democratic and inclusive process.<br><br>Also, the focus on compatibility with GDPR and other rules is spot on and definitely something to prioritise. Another issue to prioritise is whether there is an actual need to include OTT services or it is rather an emotional argument not backed by clear evidence. | The comments on the timing mainly refer to the process up to the adoption of the proposal. In the ongoing process, there are therefore a number of issues to be rectified, that require more robust analysis. The text and main findings have therefore been amended to reflect that in the ongoing process, the shortcomings of the impact assessment and proposal should be acknowledged and fully taken into account. This replaces the comments focusing on the feasibility of the implementation date.<br><br>The issue related to the lack of evidence for the extension of the scope to OTT services, stressed in Section on the problem definition, has been added to the main findings. |

Deleted: All c

Deleted: the draft report

Deleted: provided on 19th June 2017 have been taken into account in the compilation of the final report. Where publication was approved by the contributor, the comments are recorded, commented upon by the IAI below, with action taken where new evidence or analysis has thus been highlighted.¶
Responses were received by the following organisations:¶
A representative of an NGO (not to be published)¶
The responses and corresponding IAI comments are

Deleted: I

Deleted: Organisation: NGO ¶
Date: 11th July 2017

Formatted Table

Formatted: Justified

Impact Assessment In

Formatted: Justified

Deleted: 170619d

Deleted: 17071

Deleted: 3

Deleted: f