Access to data, consent and the impact of the Proposal for an ePrivacy Regulation

Report to

The Minister for the Economy and Finance
The Minister for Culture
The Minister of State with responsibility for Digital Affairs

By

Claudine Duchesne-Jeanneney
Contrôleur général économique et financier

Gérard Lallement
Ingénieur général des mines

Jacques Serris
Ingénieur général des mines
# TABLE OF CONTENTS

**SUMMARY** .......................................................................................................................................................... 4  
**TABLE OF PROPOSALS** ........................................................................................................................................ 6  
**Introduction** .......................................................................................................................................................... 7  
1 **ePrivacy, a regulation whose purpose is clear but whose scope is yet uncertain** ........................................... 7  
   1.1 The Regulation and its Articles 8, 9 and 10 ................................................................................................. 7  
   1.2 What will be the legal scope of the proposed ePrivacy Regulation? ......................................................... 8  
2 **Privacy at the time of new uses of communication services** ....................................................................... 9  
   2.1 The new uses are driven by smartphones and their applications ............................................................. 9  
   2.2 Protection of privacy: vigilant and proactive users ...................................................................................... 11  
   2.3 Users seek to reduce advertising pressure to improve the comfort of their navigation ..................... 12  
   2.4 Accept advertising or pay: new uses still face this dilemma ................................................................. 14  
3 **Four case studies** ............................................................................................................................................. 14  
   3.1 Browsers ..................................................................................................................................................... 15  
   3.2 The universe of apps .................................................................................................................................. 16  
   3.3 Personal digital assistants ............................................................................................................................ 17  
   3.4 Connected vehicles ...................................................................................................................................... 18  
4 **How Privacy concerns are tackled in the US** .............................................................................................. 20  
   4.1 The US regulatory approach or the temptation of emptiness? ................................................................. 20  
   4.2 When Apple arises as a ePrivacy champion ............................................................................................... 21  
      4.2.1 Data collection, “differential privacy”: a strong but fairly opaque policy ........................................... 21  
      4.2.2 iOS 11 and intelligent tracking prevention: an enhanced protection of private life ...................... 22  
   4.3 The privacy paradox seen from a US perspective ...................................................................................... 23  
5 **What are the technical options?** .................................................................................................................... 24  
   5.1 Filtering through black/white lists .............................................................................................................. 24  
      5.1.1 Mozilla Firefox V 57, a protection by exclusion list with the possibility of exceptions .................. 24  
      5.1.2 Ghostery, protection through personalised exclusion lists ............................................................ 25  
      5.1.3 uBlock Origin, an extension which filters trackers and blocks advertising banners ................... 26  
   5.2 Filtering according to the purpose of targeting .......................................................................................... 27  
      5.2.1 The Do Not Track protocol ................................................................................................................ 27  
      5.2.2 Filtering according to the purpose of trackers ................................................................................... 28
5.3 Filtering according to the tracking techniques or the nature of the tracker ................................................. 29
  5.3.1 Google Chrome (V 62.0.3202.89), three levels of configuration .......................................................... 29
  5.3.2 Apple Safari Version 11.0.1 ................................................................................................................. 31
5.4 Filtering according to the nature of sites ....................................................................................................... 32
5.5 Consent Managers: BayCloud and TartAuCitron ..................................................................................... 34
  5.5.1 The BayCloud solution ......................................................................................................................... 34
  5.5.2 The TartAuCitron solution .................................................................................................................. 35

6 The economic impact of the european proposed regulation ............................................................................. 35
  6.1 Impact on the digital advertising market ............................................................................................... 36
    6.1.1 Search switches over to mobile and makes increasing use of artificial intelligence .................... 37
    6.1.2 The growth of Display (banners) is driven by social media ............................................................. 38
    6.1.3 Advertising plays a special role in the economic viability of the press ........................................... 41
    6.1.4 Advertisers call for more transparency ................................................................................................ 42
  6.2 E-commerce, online marketing and customer relation management ....................................................... 43
  6.3 Impacts on the competitive position of stakeholders ............................................................................. 44
    6.3.1 Filtering according to black/white lists ............................................................................................. 45
    6.3.2 Filtering according to the purposes of tracking ............................................................................... 45
    6.3.3 Filtering according to the nature or the techniques of tracking ....................................................... 45

7 Proposals ....................................................................................................................................................... 46
  7.1 To ensure sustainable protection of privacy, the Regulation must be technology neutral .......... 47
  7.2 The privacy protection software offering must continue to diversify and develop ....................... 47
  7.3 To maintain an open Internet, a “feedback channel” is required ......................................................... 48
  7.4 Regulating advertising pressure on the Internet .................................................................................. 50

ANNEXES ......................................................................................................................................................... 51
  Annexe 1 : Lettre de mission ............................................................................................................................ 52
  Annexe 2 : Liste des personnes rencontrées ou interrogées ........................................................................ 54
  Annex 3: the operation of programmatic advertising .................................................................................. 58
  Annex 4: text of articles 8,9 et 10 .................................................................................................................. 60
SUMMARY

The Minister for the Economy and Finance, the Minister for Culture and the Minister of State reporting to the Prime Minister with responsibility for Digital Affairs tasked the General Council for the Economy with assessing the impact of measures to protect information stored in terminal equipment, as provided for in the Proposal for an ePrivacy Regulation (Articles 8, 9 and 10). The proposal is *lex specialis* to the General Data Protection Regulation (GDPR), which will enter into force in May 2018.

Based on our analyses, we believe that the GDPR and the proposed Regulation address a real demand for better information and protection of Internet users' privacy. As it stands, however, the proposed Regulation, over and beyond the GDPR, could bolster the position of the major Internet platforms that have regular users, many of whom have opened a private account. At the same time, it may undercut those stakeholders that operate services and sites that cater to less regular customers. Were it to introduce mandatory settings for software used to access electronic communications services, this move could be rejected by users, as the user-friendliness has not been tested and it is not known whether these settings meet users’ needs.

This observation is based on the study of electronic communications services use. Time spent using the Internet has caught up with time spent watching television, and logically enough, spending on digital advertising has outstripped that for television since 2016. Digital advertising's success is due to the growth in behavioural advertising, which allows advertisers to switch from media planning to audience planning, i.e. campaigns that are designed based on the profiles of web users. These techniques add value to advertising space, which is particularly important for general-interest sites that cannot offer contextual ads. Without data, advertising is less effective and the value of ad spaces decreases. However, gathering data requires users' consent.

Internet users favour the "free" model, which is financed by advertising. Although users value their privacy, two-thirds are willing to share data to access content or services and more than eight in ten would prefer to access free sites with advertising than pay for content. There is in fact no paradox between a desire to protect one's privacy and the acceptance of data sharing. What a large portion of Internet users reject is not advertising or the creation of databases of their data, but the fact that they are not informed about the gathering and use of this data.

The proposed Regulation prioritises software giving access to electronic communications services. In most cases (browsers, operating systems, personal assistants, etc.), there are a limited number of software publishers and some have a dominant position on their market. These publishers would be in an unusual position as they have to obtain the consent of Internet users for the data they use for their own purposes whilst being seen to uphold these users’ privacy with regard to third-party services. They would be well placed to discuss with Internet users, to provide explanations and, ultimately, to obtain their consent.

Other major Internet platforms, such as social media and very large e-commerce sites, which have regular users who generally open an account, will also be well placed to explain their privacy policies.
to Internet users. On the other hand, other service providers with less regular users will have more difficulty.

We are putting forward four principles that could inform both discussions and the French position when the text of the Regulation is being discussed:

- **To ensure sustainable protection of privacy, the Regulation must be technologically neutral.** The diversity of markets (fixed, mobile electronic communications services, the Internet of Things - from watches to connected vehicles) and, for each market, the variety of options (access software settings or options, installation of add-ons such as anti-tracking software, ad-blockers or anti-viruses) mean that it is impossible to define technical specifications covering such a broad field.

- **The privacy protection software offering must continue to diversify and develop.** This offering may take the form of a functionality proposed by a publisher of access software or of an add-on, which may be provided by another company. The various access or access control software must be considered at the same level, without certain being given a custodial role. In addition to privacy issues, competition law enforcement authorities need to consider the impact of the options offered by software providing access to communications services, when its publishers hold a dominant market position.

- **To maintain an open Internet, a “feedback channel” is required.** Services or websites catering for occasional users need to establish direct contact with them, to customise their offering, or to propose the financial terms of the service. A company must be able to make access to its services contingent on the acceptance of various terms and conditions (subscription, advertising, etc.). This dialogue with the Internet user, which is used to approach him/her, to obtain his/her consent and, if necessary, to amend, for this specific site, the configuration of the control software that allowed access to the service in question represents a “feedback channel”. The timeline for implementation of the ePrivacy Regulation must be adjusted to ensure that these options are technically available.

- **We need to regulate advertising pressure on the Internet.** The rise in the use of ad-blockers reflects a worsening user experience. However, the regulation of advertising pressure is not primarily governed by the ePrivacy Regulation. It is essentially up to the professionals to self-regulate. Improving the image of advertising among Internet users would make it easier to obtain their consent for targeted advertising.

The government commissioned this report from the General Council for the Economy (CGE). Its analyses and proposals reflect the rapporteurs’ conclusions and do not represent the government’s position on the Proposal for an ePrivacy Regulation.
## TABLE OF PROPOSALS

**Proposal n° 1.** The proposed Regulation should be technology neutral, throughout the text including the recitals. 

**Proposal n° 2.** The privacy protection software offering must continue to diversify and develop. The Regulation should not provide certain software with a privileged “gatekeeper” role. Access or access control software for electronic communications services must offer several protection scenarios, clearly explain the implications of these different options and provide a simple procedure for accepting the default settings, reinforcing them or making them more flexible. 

**Proposal n° 3.** Competition law enforcement authorities need to consider the impact of the options (including default settings) offered by software providing access to communications services, when their publishers hold a dominant market position. 

**Proposal n° 4.** Access or access control software for electronic communications services must propose a simple procedure for correcting its settings to include the consent given by an Internet user for a particular site or service. 

**Proposal n° 5.** If a service provider wishes to use, for commercial or service development purposes which are not strictly necessary for the provision of that service, terminal equipment processing or storage capacities, it must be able to offer the user several options for accessing the service, depending on whether the user has given his/her consent or not. 

**Proposal n° 6.** The deadlines for the implementation of the ePrivacy Regulation must be adjusted, particularly after the Regulation has been adopted, to allow the most vulnerable stakeholders to adapt themselves. 

**Proposal n° 7.** Initiatives for the self-regulation of advertising by professionals should be encouraged by the public authorities. 

**Proposal n° 8.** A programme to monitor the transparency of the advertising chain should be implemented by the public oversight authorities.
INTRODUCTION

By letter of 23 October 2017, the Minister for the Economy and Finance, the Minister for Culture and the Minister of State reporting to the Prime Minister with responsibility for Digital Affairs tasked the Vice-President of the General Council for the Economy (CGE) with a mission relating to Article 8, 9 and 10\(^1\) of the proposal for a Regulation on Privacy and the Electronic Communications (hereafter in this document, the “proposed ePrivacy Regulation”). The task force was asked to “provide analytical elements which would allow a more precise assessment of the impact of the measures envisaged in the proposed Regulation on the stakeholders involved, both economically (loss of profits, investment to maintain or adapt, etc.) and on a technological level, through the description of adaptation solutions that could be implemented, taking into account their social acceptability (intrusive or repetitive character) and user-friendliness (ease of use)”.

After a brief reminder of the scope of the ePrivacy Regulation, the task force focused on:

- analysing the new uses of electronic communications services in terms of privacy, illustrating this approach with four case studies - Internet browsers, mobile applications, personal digital assistants (PDAs) and connected vehicles;
- studying the US regulatory approach and Apple’s approach to ePrivacy;
- describing various technical options implemented to set up privacy protection settings (access software or plug-ins);
- studying the impact of the implementation of the proposed Regulation on economic operators.

On the basis of these observations and analyses, the task force drew up recommendations with respect to protection of privacy and economic stakeholders’ interests.

The government commissioned this report from the CGE. Its analyses and proposals reflect the rapporteurs’ conclusions and do not represent the government’s position on the proposed ePrivacy Regulation.

1 ePrivacy, a Regulation whose Purpose is Clear but whose Scope is Yet Uncertain

1.1 The Regulation and its Articles 8, 9 and 10

The European Commission presented on 10 January 2017 a proposal for a Regulation on Privacy and Electronic Communications (hereafter referred to as the ePrivacy Regulation), presented as a lex specialis of the General Data Protection Regulation (GDPR), adopted in April 2016 and entering into force on 25 May 2018.

The proposed ePrivacy Regulation is based on Articles 16 and 114 of the Treaty on the Functioning of the European Union (TFEU). Under Article 16.1 TFEU “everyone has the right to the protection of personal data concerning them”. As electronic communications involving individuals are to be considered as including personal data, the protection of individuals with regard to the confidentiality of communications and processing of such data is based on Article 16 TFEU.

\(^1\) See annex 4
The Proposal is also based on Article 7 of the Charter of Fundamental Rights: “Everyone has the right to respect for his or her private and family life, home and communications”, having the same scope as Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR): “Everyone has the right to respect for his private and family life, his home and his correspondence”.

In accordance with the case-law of the Court of Justice of the European Union and of the European Court of Human Rights, the professional activities of natural persons are included in the scope of the right guaranteed by Article 7 of the Charter of Fundamental Rights and Article 8 of the ECHR.

The proposed Regulation follows the Directives 97/66/EC, 2020/58/EC and 2009/136/EC. Directive 2009/136/EC strengthens the subject’s prior consent for storage of information or for access to information in the user’s terminal equipment.

The proposed ePrivacy Regulation is part of the 2nd pillar “to create the right environment and conditions for digital networks and services to flourish” of the “Digital Single Market Strategy for Europe” presented by the European Commission on 6 May 2015.

In December 2017, there were 2 versions of the proposed Regulation: the original version proposed by the Commission in January 2017 and the version adopted by the European Parliament in October 2017 (see Annex 4).

1.2 What will be the legal scope of the proposed ePrivacy Regulation?

One of the objectives of the proposed Regulation is to extend the rules protecting privacy to new internet interpersonal communications services (voice over IP, instant messaging, e-mail, etc.) which are not subject to the current EU regulatory framework for electronic communications, in particular the Directive on privacy and electronic communications. They would also cover undertakings providing services that use or make possible electronic communications, even as a minor ancillary function to the service rendered. Finally, the proposed Regulation would have to apply to machine-to-machine communications.

The protection of the confidentiality of electronic communications and terminal equipment is not addressed by the GDPR, which does not define what legal grounds for processing may be allowed and in which situations. Instead, it lays down the general framework for the protection of personal data. The current Directive 2002/58/EC already regulates this type of activity, and the proposed ePrivacy Regulation specifies these items.

The Regulation bases the protection of “end users” on consent. The definition of "end user" covers both natural and legal persons. Machine-to-machine communications are also covered. But the case of a supply chain, which deals with business-to-business relations, is very different from that of a smart watch. For legal persons as well as for connected objects, the method for obtaining consent will need to be specified.

The legal analysis of the proposed Regulation falls outside the scope of our remit. However, all the persons interviewed by the task force stressed the complexity of the subject and voiced their concerns. The following points were systematically mentioned during the interviews and should be underscored:

- the economic interest of the service provider is not included in the scope of the exceptions provided for in the ePrivacy, unlike the GDPR;
• concerning the interpretation of the concept of a “tracking wall”, publishers seeking economic equilibrium underline the need to propose different formats, depending on the user’s decision to accept or not targeted advertising;
• many lawyers consider that defining the settings of access software, as called for in ePrivacy, cannot exempt a service provider from obtaining consent under GDPR;
• it is impossible to estimate compliance costs for ePrivacy, at a time when companies are preparing for the entry into force of the GDPR, but there is widespread concern that SMEs will experience the greatest difficulties.

2 PRIVACY AT THE TIME OF NEW USES OF COMMUNICATION SERVICES

2.1 The new uses are driven by smartphones and their applications

The dissemination of communicating objects has increased sharply since 2010. They serve as gateways to messages transmitted over the Internet, whether they are of an advertising or informational nature, targeted or general.

Some figures and trends from the 2017 "Digital Barometer" survey are worth noting:

• more than nine out of ten people have a mobile phone;
• while ownership of computer equipment has tended to stagnate, the growth in the number of mobile devices - tactile tablets and smartphones - has been particularly strong since the beginning of the decade. Nearly three out of four people have a smartphone and more than four out of ten have a tablet. Between 2012 and 2017, the number of smartphones more than doubled and the number of tablets increased more than fivefold.
• ownership of multiple devices is also a reality: more than three out of ten people have a computer, a tablet and a smartphone.

---

2 Source: Survey carried out by CREDOC for the CGE, the French Telecommunications and Posts Regulator and the Digital Affairs Agency, relative to dissemination and use of information technologies in France. Survey conducted through face-to-face interviews with a representative sample of 2,200 people over 12 years of age.
More specific tools such as transactional intermediaries (Cortana, Siri, Amazon) and more generally, the objects of the Internet of Things have recently been added to traditional communicating objects.

**Web browsing, e-mails and app downloads** are the most common uses for mobile devices (64%, 60% and 55% of people respectively). The 2016 edition of the survey\(^3\) showed that geolocation services were used by 42% of people (the question was not asked for the 2017 edition).

**OTT apps** (Whatsapp, Hangouts, etc.) are also experiencing strong growth: 43% of people use them to exchange text messages and 31% use them for voice.

**Each device has its own specific use:** social media and online gaming are, for a majority of users, smartphone- or tablet-based; conversely, emails and online purchases are made primarily with computers. Viewing videos is equally divided between the two channels.

\(^3\) Digital barometer, op cit, 2016 edition
It should also be noted that important developments that primarily concern the media have occurred or are under way. Time spent on the Internet is catching up with the time spent in front of the television (18 hours vs. 20 hours per week respectively\(^4\)) and for the first time in 2017, two out of three Internet users are members of at least one social network (a figure that rises to 86% for those aged 12 to 40). They attest to the growing power of specific application universes (Facebook, YouTube Channels, etc.) and consequently their ability to attract a large advertising flow and impose a specific message format.

When it comes to e-commerce, population characteristics are the primary determinant. Young adults (18-25 year olds) and middle age groups (25-39 year olds) buy massively on the Internet; together they account for 84% of buyers. The propensity to buy online is also higher among those with higher education, the upper-middle class and those with higher incomes. Another factor to consider is the level of trust that sites inspire. The greater the trust, the more the act of buying takes place: 95% of Internet users who have high trust in a site make purchases, but this figure is only 10% among those who do not\(^5\).

### 2.2 Protection of privacy: vigilant and proactive users

With respect to confidentiality and personal data protection, 54% of Internet users state that they are more vigilant on the Internet than in previous years\(^6\). Above all, internet users consider that sharing data is dependent on the expected use: they provide identity-related information to the government or their bank (54% of Internet users provide a copy of an identity document, 43% their bank details and 31% information about their health) but they refuse to do so with social media. 40% of internet users do not want to share their data on social media and 10%, if they had the choice, would not provide any information to anyone.

---


\(^5\) Digital barometer survey, 2016 Edition. The question was not asked for in 2017.

\(^6\) Summary of report "Personal Data and Trust: what are the strategies of French Citizen-Consumers in 2017?", Chaire Valeurs et Politiques des Informations Personnelles, Patrick Waelbroeck, Armen Khatchatourov, Claire Levallois-Barth, 23 June 2017.
At the same time, we are witnessing the establishment of mistrustful behaviour: 61% of Internet users refuse to share their location, 59% erase their search history and 45% set up the parameters of their browser so as to protect their privacy. One internet user out of five goes to extreme lengths to protect themselves: private or anonymous browsing (via the Tor network). In all cases, the goal is to limit the amount of information harvested.

However, people who use protection tools are also the ones who consume the most: 52% make an online purchase at least once a month. Having the means to protect oneself gives the feeling of maintaining control in an environment perceived as intrusive, but Internet users would like to see Internet stakeholders commit to being more transparent and to respecting their privacy. These findings are not new. They corroborate those from the 2014 "Digital Barometer" survey, which showed that for 33% of people, insufficiently protected data is a major obstacle to Internet use.

Internet users are aware of the risks. In 2014, 86% of people felt that software can transmit information on mobile phones (such as one's address book and location) without the user being notified. Nearly one in two also believed that they had previously experienced unwanted access to their personal data.

Faced with these risks, most people said they were attentive to the protection of their personal data, for example by installing firewall or security software, using passwords or storing their data away from any Internet connection; 57% said they were very vigilant and 16% thought about it "from time to time".

These results are consistent with those of the Eurobarometer survey on privacy and electronic communications, cited in the proposed ePrivacy Regulation, on people’s requirements for access to their equipment.

2.3 Users seek to reduce advertising pressure to improve the comfort of their navigation

Ad blockers are software extensions to browsers that filter advertising. They allow faster and clearer display of web pages, a lower consumption of resources (processor, memory and bandwidth) as well as some protection of privacy by deactivating tracking and monitoring systems used by advertising agencies.

Internet users who use an ad blocker seek first to reduce the presence of advertising to make browsing more comfortable. Among the 55% of internet users who have already used an ad blocker, 84% appreciate them for their ability to mask intrusive ads. For more than one user out of two, they make browsing more comfortable and for 36% they protect personal information.

---

7 Digital barometer survey, 2014. One chapter deals with confidentiality and privacy.
8 Eurobarometer 443 survey on privacy and electronic communications (SMART 2016/079).
10 The ratios of one in two Internet users and 36% of Internet users are related to the number of Internet users who install advertising blockers on their browser (55% of all Internet users). Source: Digital Barometer 2016
It is necessary to distinguish users’ perception of intrusive advertising that arises from the size and format of ads that appear on web pages from their perception of tracking, which is linked to privacy concerns.

Although ad blockers are mainly used on computers, they are also used on mobile devices: a 2016 study\(^{11}\) shows that 309 million people (16% of the 1.9 billion smartphone users worldwide, a percentage that doubled between 2015 and 2016) use an ad blocker on their smartphone browser, including 116 million in China, 89 million in India and 28 million in Indonesia. Europe and North America are less affected, with 8.9 million active users per month.

This rise in ad blockers has led to a reaction from advertising professionals, who have become aware of the negative effects of an advertising presence that users consider to be excessive. In 2015, representatives from consumer groups (Center for Democracy & Technology, Open Rights Group), advertisers (World Federation of Advertisers), media (World Association of Newspapers, Association Nationale des Journaux, International Federation of Periodicals), advertising agencies (Havas), browser publishers (Google, Mozilla) the European Commission, the British government and the World Economic Forum took part in roundtables on ad blockers.

A majority view has emerged from these roundtables. The following points constitute the view of the stakeholders:

- page loading times must remain under a given threshold to be acceptable;
- the number of exposures should be reduced, particularly for premium spaces. This will have a better impact on trademarks, improve the user experience and stimulate creativity;
- ad quality must be improved;
- contextual ads must be used instead of individual targeting when the user refuses to be tracked;
- publishers should encourage users to share their data as part of a clearly-explained voluntary procedure;
- publishers should encourage advertisers to target value rather than the price of an ad location;
- users must have the means to refuse and to complain about the ads they receive.

In France, other approaches are underway to reduce advertising pressure and to target users in a more relevant manner. Advertising professionals\(^{12}\) have engaged in a three-pronged approach:

- improving the user experience and the quality of distribution environments (promotion of the Digital Ad Trust and Coalition for Better Ads labels);
- improving quality and security by imposing independent third-party measures based on a tested methodology;
- strengthening the independence of professionals with respect to the global Internet companies concerning data. Data, which are needed for relevant targeting, are pooled within platforms that bring together the main media companies (Gravity and Skyline).

---


\(^{12}\) Syndicat des Régies Internet (SRI), Union des Entreprises de Conseil et Achat Média (UDECAM)
Should it continue, the rise of ad blocking will constitute an economic threat to advertisers. It should not be confused with economic issues linked to the implementation of the proposed Regulation. The task force considers that more effective self-regulation is the correct response to the rise of ad blockers.

### 2.4 Accept advertising or pay: new uses still face this dilemma

Are Internet users willing to pay for access to content and services? This question has been around since the Internet began. While The New York Times, with 1.8 million paying digital-only subscribers (compared with one million subscribers to the printed edition), has shown its capacity to conduct the digital transformation of its editions, most of the press has not reached this stage yet. In France, with the exception of Les Echos whose distribution is half digital publishing, digital circulation remains marginal in terms of revenues, despite a high growth rate (+ 30% in 2017 for national newspapers). The main reason is the appetite for the free Internet, also largely funded by advertising.

According to a study by the Internet Advisory Board\(^\text{[13]}\), “The European online experience is essentially free and ad-supported, with two-thirds of users never paying for services or content”. According to the IAB, nine in ten online users would stop using the services of a site if they had to pay for it. **People with “lower income”\(^\text{[14]}\) would be the first to give up these services**: only 5% of them would be willing to pay, against 12% for high-income users\(^\text{[15]}\). Although many European internet users value their personal data, **two-thirds of them would be willing to share data to access content or services**\(^\text{[16]}\) and more than eight in ten would prefer access to free sites with advertising rather than pay for content.

There is in fact no paradox between a desire to protect one’s privacy and the acceptance of data sharing. What Internet users refuse is not advertising or the creation of databases of which they are the raw material but the fact that they are not informed about the harvesting and use of such data. According to the Internet Advisory Board, they would prefer to obtain detailed information on how their data is used, including the reasons why they see a particular ad, to know who can access it and to be able to adjust or stop that use, rather than being presented with multiple cookie acceptance banners (67% vs.50%).

### 3 Four case studies

Whereas the range of electronic communications services covered by the proposed ePrivacy Regulation is extremely broad, the attention paid to Articles 8, 9 and 10 focuses on a long-standing feature of browsers (the distinction between first- and third-party cookies). To avoid this pitfall and extend our approach, we briefly review the internet browsers, mobile applications (apps), personal digital assistants (PDAs) and connected vehicles. This review allows us to highlight the diversity of issues and of proposed solutions to strengthen privacy protection.

\(^{13}\) Europe on line: an experience driven by advertising, Internet Advisory Board, 2017

\(^{14}\) People whose income is in the first three deciles

\(^{15}\) People whose income is in the last three deciles

\(^{16}\) Figure corroborated by the "Données personnelles et confiance : quelle stratégie pour les citoyens-consommateurs en 2017 ? report", see previous footnote
3.1 Browsers

In October 2017, all terminal equipment taken together, the French market shares of the main browsers, expressed in number of page views, were 48.9% for Chrome, 22.2% for Safari, 13% for Firefox, 4.9% for Internet Explorer and 3.4% for Edge.

The publishers of these browsers are companies and one foundation (Mozilla), whose headquarters are all in the United States. European publishers are barely represented: the market share of Opera, from the Norwegian company Opera Software, which is the most used European browser, is around 2.6% in Europe.

Cookies are files that can be stored on the browser and read by websites. Storage of cookies required for the provision of a service, such as session and load-balancing cookies, does not require the user’s consent. According to the proposed Regulation, the same applies to audience cookies. An extension of the scope of these exceptions was proposed by the European Parliament (see Annex 4, Article 8.1.d, 8.1.d bis, and 8.1.d ter). Other cookies may be classified according to different purposes:

- to improve browsing fluidity or the quality of user experience, customise access to the website pages (preferred pages), propose services (recommendation) and more generally to manage the service offering and the customer relationship (CRM);
- to meet the needs of advertising, according to technical parameters (limitation of the number of times a banner is seen, tags, etc.), or for behavioural targeting (which does not permit the direct identification of the user) or for customised targeting.

There are also other trackers that, like cookies, are based on the registering or reading of information on browsers or on the characteristics of the browser or of the terminal, such as web beacons, tags or fingerprinting. A web beacon, generally invisible, is used on web pages or in emails to verify that a user has accessed certain content. They are currently used to monitor e-mails and web pages. Browser fingerprinting is aggregated information (e.g. regarding the size and resolution of the screen, the fonts used, etc.) which can be used to partly or fully identify a user.

Whether cookies, beacons or tags, Internet users rarely make the distinction between a technical means required to update a shopping cart on an e-commerce site, for example, from means used for targeting or profiling.

There are techniques to monitor the use of cookies by websites. These techniques include:

- the Do Not Track signal, by which the browsers may request remote sites not to track the internet user;
- blocking all cookies;
- blocking third-party cookies;
- private browsing;
- blocking cookies from domains listed in blacklists;
- allowing cookies from domains listed in a whitelist.

It is also possible, using blacklists, to restrict access to sites or vice versa, to unlock access to a site when it appears on a white list.

---

17 Tablets, smartphones and computers
18 Source : Statcounter
The variety of solutions available to internet users to set protection parameters goes well beyond the distinction between first- and third-party cookies. In section 5, we review the means used by Internet Explorer, Chrome, Firefox and Safari to protect privacy. To supplement the overview of existing technical solutions, we also examine complementary tools such as ad blockers. Most of these solutions are recent and are evolving. The review in section 5 highlights the need for a technologically-neutral regulatory approach.

3.2 The universe of apps

Mobile devices now account for a growing share of audience and the majority of digital advertising investments: the turnover of mobile advertising is expected to exceed that of fixed services in 2019 (see § 6.1).

There are more than 2 million apps available on the Apple Store and about 2,8 million on the Google Play Store. These apps generate significant income: for Q3 2017, it totalled $11bn for the Apple Store and $8bn for the Google Play Store. Both stores show a strong increase of downloads: between June and September 2017, 8 billion apps were downloaded from the Apple Store (+8%) and 18 billion from the Google Play Store (+10%).

In France, users have an average of 90 apps installed on their smartphone. Thirty are used each month and 9 every day. The time spent on these applications is approximately 100 minutes (195 minutes per day in South Korea).

To contrast with this profusion, in China, the WeChat platform from Tencent claims to have more than 900 million users and is a service portal. Initially a mobile platform for sending messages, phoning, texting or organising a meeting, it has diversified. It is now used for shopping or buying services, booking train and cinema tickets, etc.

A user who wants to use an application goes through a voluntary procedure, downloads the application and accepts the General Terms and Conditions of Use (TCU). Under the GDPR, where consent is the legal basis for processing personal data, the app publisher must also specifically request it. Several studies show (this is the paradox of privacy), that Internet users are more easily inclined to give their consent in such a context than when they are browsing freely on the web.

The format of advertisement for mobile apps has been adapted for this environment. Cookies have been replaced by a unique identifier specific to the terminal and to the advertising: IDFA for Apple smartphones and tablets and AAID for Android devices. This identifier, renewable at any time at the request of the user (for Android and iOS versions), can be accessed via an application. It is used to design profiles, to determine whether an advertising announcement has already been shown to a specific user or to limit its transmission frequency. One advantage of the identifier is that it can be managed separately from the device’s other parameters, and can, for example, be updated at the user’s request, without obliging him or her to reset the apps s/he uses. This function allows the

---

19 Source : Statistica
21 Decoding consumer usage patterns, App Annie, May 2017
22 An advertising ID could be created for other devices, as Microsoft did for Windows 10
management of advertising pressure separately from other parameters providing access to the user data.

**Mobile devices present specific challenges.** These include the possibility to geolocate users via GPS or networks to which they may connect (telecom networks or open Wi-Fi networks). Geolocation information, combined with other metadata such as the MAC address or the advertising identifier can, for example, allow monitoring the time spent in a shop, knowing the number of visitors or identifying the busiest areas.

Apple activates geolocation by default but does not authorise apps to access it. To do so, the user must specifically authorise each application. For Android devices, data access authorisations are granted to the app upon installation.

In the universe of smartphone apps, a particular challenge for privacy is the management of authorisations granted to each application to access the smartphone's resources (identifiers, Wi-Fi location, address book, etc.).

### 3.3 Personal digital assistants

Configuration of access to users' personal data can be set separately from apps. It should be noted that, with Windows 10, Microsoft currently provides a configuration of the main categories of information gathered: geographical position (affects all applications and web pages), voice recognition when using Cortana, diagnostic data (uses of application and software, web history, data related to keyboard use), personalisation of user experience through use of this data and personalised advertising. Privacy protection parameters are set at the level of the operating system itself. The situation is similar to iOS (see § 4.2.2).

A milestone is reached with technologies that use artificial intelligence to process Internet users' requests and offer a reply or a service without needing navigation or the use of multiple applications that communicate poorly with each other.

This need for an intermediary that manages a navigation seen as too complex explains the popularity of digital assistants. According to Tractica, 500 million people were using a form of digital personal assistant in 2016, a number that could rise to 1.8 billion by 2021 (excluding the professional market). SIRI (Apple), S-voice (Samsung), Cortana (Microsoft), Alexa (Amazon) and Hey Google are available on all terminals, which they can link up via dedicated equipment (connected speakers or pod) such as Google Home or Amazon Echo. They have an interface allowing a natural language conversation by text or by voice (chatbots), and use algorithms capable of mobilising all the resources of the back office net. With the growth of their use, they become intermediaries between consumers and businesses. Their advantage will be, for example, to organise a trip including several transport services, accommodation offers, suggestions for restaurants and a cultural programme.

---

23 It is the case for IDFA, it depends on versions of Android for AAID

24 This is the level 2 address (“the physical network layer”) of the Wifi components. Each Wifi terminal, whatever it is, is identified by a unique MAC address

25 This results from a formal notice procedure by the CNIL


27 Livre blanc "Les assistants virtuels réorganisent nos vies et redéfinissent le marketing numérique", Bing et iProspect
With such assistants, particularly when they provide voice interface, browsers and applications tend to disappear from the visible universe of the Internet user who uses them.

**To be effective, assistants must learn.** It is therefore necessary to let them use the data generated by the user in his interactions, which is essential for AI learning: search histories, contacts, locations, etc. which is usually done by creating an account. Data are sent to online service providers which the assistant uses. The providers store and process this data. This requires a robust technology, but also balanced rules to manage relations between the assistant and the services. The use of assistants illustrates the privacy paradox: despite having reservations as a matter of principle, users agree to entrust them with their data in exchange for service quality.

But assistants could also provide tailored protection, through dialogue with the users, by enabling them to adapt the configuration of authorisations for access to their personal data, in particular on the basis of preferences that change over time.

Personal assistants, particularly those operating via a voice interface, are a new generation of software for accessing electronic communications services, providing an interface with browsers and applications, so that these could disappear from the Internet user's visible universe.

For personal assistants, that have access to certain personal data for learning purposes and to provide services, the challenge is in controlling information that is:

- captured by the device when the listening mode is enabled;
- disseminated in the cloud and used by third-party apps activated by the assistant.

### 3.4 Connected vehicles

Thanks to data exchanged with other vehicles, road infrastructure and the Internet, connected vehicles will be able to offer more and more security, traffic management and entertainment information services. For example, an automatic emergency call system will be implemented in all vehicles sold in the European Union from 31 March 2018, as part of the European Commission's eCall initiative.

Several studies estimate that new vehicles will increasingly be equipped with connected, standard or optional features:

- for A.T. Kearney, by 2020, 75% of the fleet will have some form of connectivity;
- for Accenture Strategy, by 2025, all new vehicles will be equipped with connected features;
- for NTT DATA, 90% of vehicles will have on-board connectivity by 2020.

With the increase in the number of connected vehicles, the data market will constitute an important source of added value. Much of this data is by nature personal data, and therefore falls within the scope of the GDPR and the proposed ePrivacy Regulation. This includes the following data and metadata from the vehicle:

- “customer” data (name, surname, address, telephone numbers, e-mail addresses, etc.);

---

28 Privacy? I Can’t Even! Making a Case for User-Tailored Privacy Bart P. Knijnenburg | Clemson University
30 Accenture Strategy, "Connected vehicle, Succeeding with a disruptive technology", 2015
31 NTT Data, "Connected Car Report", 2015
- geo-location data;
- technical data relating to the condition of the vehicle and parts;
- the serial number of the vehicle or any unique identifier of the vehicle or part;
- vehicle usage data related to the activity of the driver or vehicle occupants (e.g. data on driving style, life on board, etc.).

In terms of security and traffic, it is possible to anonymise useful data. This is the case, for example, of information relating to traffic jams, the presence of roadworks, or available parking spaces. However, certain safety or traffic data may not be convertible into anonymous data: this is particularly the case when a vehicle sends information, for example to an infrastructure, and the latter has to answer directly to it.

Directive 2015/962 on the development of intelligent transport systems encourages the use of anonymous data: "in order to ensure privacy, the use of anonymous data shall be encouraged, where appropriate, for the performance of the ITS applications and services". The Commission Delegated Regulation further states, in recital 6, that "Where the information service relies on the collection of data, including geo-location, end users should be clearly informed about the collection of such data, the arrangements for data collection and potential tracking, and the periods for which such data are kept. Appropriate technical measures (including privacy by design and data protection by design features) should be deployed by public and private data collectors [...] to ensure pseudonymisation of the data received from end users.” Pseudonymisation constitutes personal data processing, which must therefore comply with the conditions detailed in Article 6 (1) of the GDPR.

The C-ITS platform went even further by offering an infrastructure for managing public key certificates, enabling the identity of the vehicle to be protected over time in its exchanges with other vehicles and road infrastructure, replacing it with a frequently renewed alias. This technique is called pseudonymisation. However, it should be noted that the G29 group has published a relatively critical opinion of this mechanism.

Services provided as part of a maintenance service, for example information given by a vehicle that a faulty component needs to be replaced, have a different logic: the driver of the vehicle must give his or her consent for the data to be sent.

The example of the connected car shows the advantages of implementing techniques such as anonymisation and pseudonymisation.

---

32 Intelligent transport system
33 “Cooperative, Connected and Automated Mobility” platform of the European Commission
34 However, it is possible to waive this anonymisation in case of theft or judicial requisition
4 HOW PRIVACY CONCERNS ARE TACKLED IN THE US

In the United States, several unsuccessful attempts have been made to regulate for a better protection of privacy on the Internet, similar to the European approach. Some companies have now taken up the torch and are taking a more active approach.

4.1 The US regulatory approach or the temptation of emptiness?

Several bills were tabled in 2011 and 2012 to require the implementation of a Do Not Track protocol in relation to Internet sites, to give users the possibility to choose whether or not to be tracked by third-party sites when browsing the Internet. These bills failed to pass. In 2012, the Federal Trade Commission (FTC) published a report entitled "Protecting consumer privacy in an era of rapid change" recommending that browsers include an opt-out that allows Internet users not to be tracked.

In 2014, the FTC launched an investigation into US operator Verizon, which used "supercookies" that could not be deleted. The investigation was concluded in March 2016 with Verizon agreeing to pay a fine of $1.35 million and to change their practices; the company must now obtain the consent of the Internet user and allow him or her to withdraw it. In October 2016, Congress adopted regulatory measures proposed by the FCC, including a requirement that Internet users must consent to the resale of their data by telecom operators.

In March 2017, Donald Trump signed the withdrawal of these decisions. The dossier has now been referred to the Federal Trade Commission (FTC).

These measures had been countered by telecom operators and the advertising sector, because they believed that they were advantageous to the net’s major platforms. AT&T, Comcast and Verizon state that they do not plan to sell the browsing history of Internet users and recommend regulations centred on the sensitivity of data rather than on the stakeholders who gather it.

It should be noted, however, that the US regulations provide sectoral frameworks for data use, for example in the areas of health, finance and for companies targeting children. There is also state-level legislation: California law requires companies that advertise online to declare whether or not they comply with Do Not Track.

Finally, several privacy issues35 were under consideration by the US Supreme Court at the end of 2017.

In America, the economic role of advertising is not called into question, even though, in the face of the increasing use of ad blockers, some are calling for better advertising practices that are less intrusive and more respectful of the privacy of Internet users (see for example the IAB’s LEAN advertising initiative or the work of the Coalition for Better Ads).

In the US, some believe that regulations can quickly become economically counterproductive. This is the criticism they have been making against European regulations since 2002.

---

Advertising has become less effective in Europe as a result of regulations

Goldfarb Avi, Catherine E. Tucker “Privacy Regulation and Online Advertising” Management Science 57.1 (2011): 57-71

Abstract: We use the responses of 3.3 million survey-takers who had been randomly exposed to 9,596 online display (banner) advertising campaigns to explore how privacy regulation in the European Union has influenced advertising effectiveness. This privacy regulation restricted advertisers’ ability to collect data on web users in order to target ad campaigns. **We find that on average, display advertising became far less effective at changing stated purchase intent after the EU laws were enacted, relative to display advertising in other countries.** The loss in effectiveness was more pronounced for websites that had general content (such as news sites), where non-data-driven targeting is particularly hard to do ...

One potential asymmetry is across the breadth of content provided by a website. For example, the use of web bugs and cookies is more important for websites that aim for a general or mainstream audience that is not connected with a specific type of product. Someone visiting www.cruise.com is more likely to be interested in purchasing cruises and can be targeted accordingly, but a portal or a news website cannot be sure whether someone visiting its main page is in the market for cruises unless they track whether that consumer is also reading news features on cruises. This means that general or less product-specific websites could find consumer tracking technologies relatively more useful for targeting ads than product-specific websites is supported by external empirical evidence. For example, the E-Soft annual survey (Reinke, 2007) documents that the 100 websites that use the most web bugs have consistently been general interest websites, like Information.com, photobucket.com, flickr.com, and YouTube, as well as various ad networks.

At the heart of the American model is also the belief that the changing needs of users are better served by a variety of innovative solutions offered by competing players, than by a regulatory framework. This is particularly obvious with the Apple approach.

### 4.2 When Apple arises as a ePrivacy champion

In recent years, particularly with the launch of the iOS 11 mobile operating system, in September 2017, eprivacy is an important component of the strategy of Apple.

#### 4.2.1 Data collection, “differential privacy”: a strong but fairly opaque policy

Tags placed in advertising messages sent by Apple are used to find out if these messages have been opened. URLs referring to an Apple site tell you whether the targeted user has expressed interest in the message by logging into the URL.

With regard to **tracking technologies (cookies, web beacons and pixel tags), the company collects cookies to measure the effectiveness of its advertising** and to know which parts of its websites are most commonly used. The **data collected is then considered as non-personal data except for the following two cases:**

a) when the IP address is considered by local law as personal data (which is the case in the countries of the European Union);

b) when non-personal data and personal data are associated in which case the whole is considered as personal data.
Apple uses personal data for marketing purposes\textsuperscript{36} (developing and improving its products, services, content and advertising), logistics (product delivery), security (loss prevention, fraud prevention), communication (significant notifications, changes in terms and conditions, and charters), auditing and analysis in connection with the company's products and services. It also gathers and discloses data, considered in their document as non-personal, such as occupation, language, postal code, unique device identifier, location and time zone. Information gathered on the company's websites can be combined with metadata such as IP addresses to ensure the quality of online services.

Apple shares personal data with companies that provide services such as information processing, credit extension, product delivery and processing of orders, customer data management and development, customer satisfaction surveys. With the express consent of the user, the company may collect information about the use of the device and applications to help developers improve their applications. Apple also undertakes to disclose any personal information requested by law enforcement in connection with legal proceedings.

To process this data by making it anonymous without compromising its value, Apple uses an obfuscation technology called differential privacy, which consists of adding random noise to information about users and their uses before it is sent to the company's servers. In this way, Apple can build databases of information without revealing person-specific information.

Ideally, private data on servers should be protected from attack. But according to a study by the online magazine \textit{Wired}\textsuperscript{37}, the effectiveness of the differential privacy technique depends on a variable called the "privacy loss parameter", which is said to be low at Apple. In addition, the code and values of these parameters are not public and can be changed at any time, making the privacy policy totally opaque with regard to these criteria.

The iPhone's operating system makes it possible to prevent applications from accessing the user's personal data. By means of an adapted setting, the user can grant or refuse access authorizations to the following personal data: contacts, calendars, reminders, photos, movements and physical activities, geolocation service, multimedia library, social network accounts such as Twitter and Facebook. Access to the following components and services is also controlled by the operating system under the same conditions: microphone, camera, homekit, voice recognition, Bluetooth sharing. By default, these parameters are in the "OFF" position (no access). In addition, if the user synchronizes their data in Apple's cloud, called iCloud, they can allow third parties to access it.

\subsection*{4.2.2 iOS 11 and intelligent tracking prevention: an enhanced protection of private life}

Prior to the current version of the mobile operating system (iOS 11), the user could decide to (a) block all cookies, (b) always allow and (c) only allow "first-party" cookies from the sites visited. The new Apple mobile OS makes profound changes to the use of cookies. If it is still possible to use them to record login information on the most frequently visited sites, their use to track from site to site ("cross-site") will be limited or impossible. Indeed, with the limitation of the lifetime of third-party cookies to 24 hours, Apple is implementing, through the "Intelligent Tracking Prevention"

\footnote{36 The entire analysis is based on the documents published by Apple, “Privacy Statement of September 19, 2017” and "Security iOS 10" of March 2017}

\footnote{37 Wired, How One of Apple’s Key Privacy Safeguards Falls Short, 15 September 2017, \url{https://www.wired.com/story/apple-differential-privacy-shortcomings}. This article builds on the work of several academics (University of Southern California, Indiana University, Tsinghua University).}
feature, the possibility of strongly limiting the targeting (or retargeting) by merchant sites. This feature is enabled by default.

The following example illustrates the dynamics of this functionality: if an Internet user visits the example.com site that uses multi-site tracking, the cookies of this site will be deleted if, after 30 days, the Internet user has not revisited this site. Third-party cookies are deleted the next day. In summary:

- J0: third-party cookies are allowed (cross-site tracking is allowed);
- D+1: third-party cookies can no longer be used;
- D+30: first cookies are purged.

If the user visits example.com again, intelligent tracking prevention considers that s/he is interested in this site and keeps first-party cookies for a further 30 days. Intelligent tracking prevention does not block the use of third-party cookies immediately after a visit because they can be used to connect to another site (typically a Facebook, Twitter or Google account).

The announcement of these new features elicited strong reactions from advertising professionals. They point out that Apple did not seek consensus or a solution built on a standard, but invented its own rules. In their words, "machine-driven cookie choices do not represent user choice; they represent browser-manufacturer choice". Their fear is that the Safari browser, which accounts for one-third of the mobile traffic on the Internet, will contribute to increasing the attractiveness of platforms with connections (Google and Facebook in particular) to the detriment of content publishers.

Apple’s policy strengthens the protection of access to the user’s personal data, but it has a significant impact on the digital advertising market and on the players in that market. In addition, Apple can modulate this impact according to the technical specifications it retains and which will continue to evolve so that intelligent tracking remains efficient.

Such an approach cannot be viewed from the perspective of personal data protection alone. It is also necessary to assess whether its effect on the market presents a risk under competition rules.

### 4.3 The privacy paradox seen from a US perspective

The privacy paradox is illustrated by a study of undergraduate students at MIT. This study finds that despite preferences for privacy protection, students readily agree to transmit private data if prompted to do so, and that they quickly surrender their concern for privacy if this concern makes browsing become less easy. “Consumers say they care about privacy, but at multiple points in the process end up making choices that are inconsistent with their stated preferences”.

The authors conclude their study with remarks for public authorities: “On the one hand it might lead policy makers to question the value of stated preferences for privacy when determining privacy policy. On the other hand, it might suggest the need for more extensive privacy protections, from the standpoint that people need to be protected from their willingness to share data in exchange for relatively small monetary incentives”.

---

38 An Open Letter from the Digital Advertising Community, September 14, 2017

They add that, in all cases, we must be wary of regulations that would require an effort on the part of
the Internet user or that would make navigation more difficult, because it would be rejected by
users.

5 WHAT ARE THE TECHNICAL OPTIONS?

The aim here is to review the advanced settings of computer browsers, the extensions associated
with them (also called "add-ons" or modules) and to examine the possibilities offered by several
types of filtering: list filtering, filtering according to purpose (audience measurement, sending
advertisements, personalisation of the route, etc.), filtering according to plotting techniques and the
nature of the trackers and filtering according to site category. This analysis makes it possible to
identify, in a typology of possible solutions, those proposed by publishers who have taken into
account ergonomic constraints and users’ expectations.

For all of these means, the issues fall into the following categories:

- the quality of protection;
- the impact on economic stakeholders;
- user friendliness and fluidity of the implementation, including the possibility to revert to
  previous choices.

The tests are performed with the latest versions of browsers by downloading the homepage of the
New York Times. A summary of the results is proposed for these different tools, according to the
previously mentioned categories.

5.1 Filtering through black/white lists

5.1.1 Mozilla Firefox V 57, a protection by exclusion list with the possibility of exceptions

Firefox proposes a separate management of cookies or Firefox offers cookie management, JavaScript
enabling/disabling and tracking protection. Tracking protection is based on the use of exclusion lists:

- a basic protection list that blocks "elements commonly referred to as analytical tracking,
  social sharing and advertising";
- a strict protection list that blocks "all known tracking elements, including analytics, social
  and advertising sharing and content tracking elements".

Users have three options for tracking protection: private browsing, always or never. Cookies can also
be viewed and deleted individually. This feature does not delete all cookies; some cookies (e.g.
audience cookies) continue to be posted. Advertising trackers are blocked, but not contextual ads
that continue to be served. The robustness of this feature, based on the ability of lists to filter
cookies, is in fact entirely left to the initiative of Mozilla, the Firefox publisher. The ability to add a
customised list to the two existing lists does not exist, but there is a possibility to disable session
protection. This functionality is easy to implement (a simple click on an icon next to the menu bar).

Functional evaluation

- Quality of protection: depends on the lists of sites used;
- User friendliness and simplicity of implementation of the protection: good fluidity, few
  clicks;
• Impact on the economic players: the transition from a blocking situation to a tracking acceptance situation is achieved with only one click. The site visited does not seem to be notified of acceptance or prohibition.

5.1.2 Ghostery, protection through personalised exclusion lists

Ghostery is an extension, i.e. browser companion software that adds new functionalities to a browser. Ghostery aims to add a level of security to the protection of the user’s personal data by filtering the elements that web sites can deposit and read on their terminal. To do this, Ghostery lists these elements (tags, cookies, tags, etc.) and compares them with lists of “prohibited” elements. These lists include eight categories of items: advertising, site analysis, consumer interactions, social media, essential, audio/video player, adult advertising and commentary. The user can enable or disable each list, and within a list, prohibit or authorize a site, either beforehand or while browsing. For each site visited, Ghostery displays in a dedicated window the number of elements detected and details the elements it has blocked. Ghostery is interactive but requires a certain level of attention.

Functional evaluation

• Protection: depends on the lists used but theoretically strong. Ability to customise lists;
• User friendliness: good;
• Impact on economic players: the transition from a blocking situation to a tracing acceptance situation is achieved with a single click. The site visited does not seem to be notified of acceptance of prohibition. Only when reloading the page is the change taken into account.
uBlock Origin, an extension which filters trackers and blocks advertising banners

uBlock Origin is an add-on that is based, like Ghostery, on lists of known ad trackers. A graphical interface allows, by designating a location on a page, to accept blocked elements pointing to that location. This is a very effective device that not only filters ad trackers but also blocks ad banners.
Functional evaluation

- Protection: depends on the lists used, theoretically better than those of Firefox and Ghostery, possibility to customise the lists;
- User friendliness: good;
- Impact on the economic stakeholders: possibility to "unblock" the elements pointing to a location in a page. However, the site visited does not seem to be notified of acceptance or prohibition, so that it is necessary to reload the page for the choice made to become active.

5.2 Filtering according to the purpose of targeting

5.2.1 The Do Not Track protocol

Browsers implement a special protocol called "Do Not Track". It includes a header field in each HTTP request message that indicates that the user does not want to be tracked. In theory, advertisers and their technical intermediaries must react to this signal by refraining from targeting the user. The latter will continue to receive advertisements but they will no longer be targeted, due to the absence of behavioural data.

The difficulty in applying this protocol is that it is non-binding. Respecting the "Do Not Track" indication and not tracking the user is voluntary. Today, companies such as Microsoft, Google, Facebook and Critéo have declared that they do not take "Do Not Track" into account (this is an obligation under the laws of the State of California).
The Do Not Track protocol has been in the process of standardisation within W3C for many years. It became a candidate recommendation in October 2017. The lack of progress on this issue partly explains the success of browser add-ons and the decision taken by some publishers, Firefox in particular, to adopt other ways of controlling advertising flows.

The Working Party On the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, also known as “Article 29 Data Protection Working Party” encourages browser publishers to implement the “Do Not Track” protocol. The objective is to achieve the standardisation of a protocol within the W3C to collect the user's consent not in a binary way ("Acceptance" or "Refusal" of ad trackers) but in a granular way (domain by domain). This would fine-tune exceptions and record user preferences for a particular domain, thus meeting publisher demand.

**Functional evaluation**

- Protection: depends on the compliance of the receiving website with the "Do Not Track" protocol;
- User friendliness: good;
- Impact on economic stakeholders: depends on whether or not a granular "Do Not Track" protocol is implemented.

5.2.2 Filtering according to the purpose of trackers

An attractive idea, as reflected in many reactions to the proposed ePrivacy Regulation, would be to **classify trackers into categories according to their purpose**, allowing a finer distinction than first-/third-party cookies. Ghostery, for example, classifies cookies into 8 categories (see 5.1.2). These categories should be described in simple terms, making it easier for everyone to choose an option (accept or not).

A classification by purpose would be particularly interesting to create a category of trackers which, although useful for the development of a service, would not present any problem with regard to the protection of personal data (non-tracking cookies). PageFair, for example, suggests that these trackers be treated differently from others and gives a series of examples such as:

- allowing a website to change its appearance each time a user visits it, convert prices into the visitor's original currency and more generally customise its home page;
- recording players' progress without requiring them to identify themselves;
- performing the test campaign of a configuration (A / B testing);
- limiting the number of times an ad is presented to a user (frequency capping).

The implementation of this solution is based on complex choices that are difficult to adapt to a regulatory definition:

- characterisation of categories, their evolution over time according to practices and technologies;
- how to assign a tracker to a category and how to control it.

---

40 It was the conclusion drawn from a brainstorming session organized by the cluster Cap Digital for the taskforce, on 8 November 2017, with around 30 of its members

41 https://pagefair.com/blog/2017/non-tracking-cookies

42 Today, the Regulation mentions only trackers necessary for the service or to measure the audience
As in the case of whitelists, for example, the implementation of this solution would be based either on an open procedure or on choices made by the software manager who would propose this option.

5.3 Filtering according to the tracking techniques or the nature of the tracker

5.3.1 Google Chrome (V 62.0.3202.89), three levels of configuration

Chrome offers three levels of settings: "Block/Allow sites to save and read cookie data" and "Block third-party cookies". There is also a possibility of private browsing after which cookies are deleted (in addition to browsing history, site data and information entered into forms). Chrome does not allow, during a private browsing, to consent by exception, by means of a simple action, to the saving and reading of cookies.

It is possible to enable or disable JavaScript and manage application access to the computer's accessories (microphone, camera). There is also protection against malicious access.

The list of cookies present on the terminal is accessible but is not dynamically updated. This is an important shortcoming of this tool. In practice, not all cookies are blocked during private browsing, but the task force did not have the means to determine which ones or why. On the other hand, some banners do appear to be blocked.

Configuring Chrome requires that users know how to define settings. The majority of them use default settings: cookies are allowed for all sites. There is no way to interact simply and dynamically with the user.

Google has announced that a version of Chrome allowing the user to block ads that do not comply with the good practice rules of the Coalition for Better Ads will be published in 2018.

Functional evaluation

- Protection: based on the acceptance or refusal of cookies. Theoretically less detailed than protection based on exclusion lists.
- User friendliness: parameters can be modified by using the menus of the navigator. This operation is less fluid (several clicks) than that allowed by Firefox.
- Impact on economic stakeholders: no change - acceptance or blocking of elements "on the fly". Return to the browser settings menu is necessary.
CGE taskforce on the proposed ePrivacy Regulation
5.3.2 Apple Safari Version 11.0.1

Safari offers personal data protection based on the management of cookies by nature (first/third parties) or the "Do Not Track" protocol. Options are:

- prevent tracking across multiple domains (regularly delete third-party cookies);
- request websites not to follow me (Do Not Track);
- block all cookies;
- to accept everything, you have to uncheck all the boxes.

In addition, it is proposed to enable or disable JavaScript. The effect of these options varies: when all options are chosen, only caches are present; when JavaScript is activated, the list of caches present widens and includes in particular caches to monitor the audience. When the saving of cookies is authorised, the list of data stored is enlarged by a large number of trackers. Finally, when tracking is allowed across several domains, the ad targeting of users is significantly enhanced.

Safari also offers a version of private browsing where once the window is closed, cookies, page views, auto-fill information and search history will not be saved. Contextual advertising banners are served during browsing, provided that the JavaScript option has been enabled.

As Chrome, Safari does not have a simple way to accept or decline cookies "on the fly" during private browsing. For this, it is necessary to reconfigure the privacy settings via the dashboard.

Safari in open navigation mode: inter-site tracking allowed, cookies allowed
Functional evaluation

- Protection: based on the activation of one of three options (erase third-party cookies, Do Not Track, block all cookies). Theoretically less refined than a protection based on exclusion lists.
- User friendliness: parameters can be modified by using. This operation is less fluid (several clicks) than that allowed by Firefox.
- Impact on the economic stakeholders: no modification - acceptance or blocking of elements "on the fly". Return to the browser settings menu is necessary.

5.4 Filtering according to the nature of sites

INRIA, the French National Institute for Computer Science and Applied Mathematics, has developed a different filtering approach from those previously described. It targets users who are not against advertisements but who block them for privacy reasons. It is based on the assumption that Internet users do not want to be tracked on "sensitive" websites (for example sites related to religion or health), but agree to be tracked and receive ads on less sensitive sites. In practice, this means providing users with the ability to specify the categories of web pages on which they do not want to be tracked and receive third-party cookies.

The project strives to find a compromise between privacy and the needs of the Web economy. To do this, INRIA has developed an add-on for Google Chrome called "MyTrackingChoices". While users are browsing the Web, the extension categorises Web pages visited and, depending on the user’s choice, blocks network connections from undesirable third-party domains on the page. In addition to the tracking that is prevented, ads from third-party sites are not displayed. The add-on is very sophisticated as it works on the basis of the pages visited and not the whole site.
It should be noted that, unlike other ad blockers, this add-on does not block ads served directly from the publisher.

This is a research project that was the subject of a publication in 2016.

Conclusion: Software is evolving and offers privacy features that go beyond the distinction between third-party cookies and first-party cookies. These are based on:

- exclusion lists. These lists pose the problem of their governance. The most sophisticated allow a site by site setting or/and the unlocking of a site on the fly;
- the “Do Not Track” protocol which today is based on a commitment to compliance by the web publishers;
- filtering of trackers according to their purpose, the technical specifications of which have yet to be defined, and which would raise governance issues similar to exclusion lists;
- a tailor-made solution (Apple). Based on its understanding of how ad targeting works, Apple editor offers an optimised protection solution that is a commercial differentiator.

5.5 Consent Managers: BayCloud and TartAuCitron

5.5.1 The BayCloud solution

BayCloud is a publisher providing businesses with privacy protection software. In particular, it markets a so-called "CookieQ" solution that allows site publishers to collect user consent prior to depositing, processing or reading cookies using the “Do Not Track” protocol.

Consent applies to all domains (host and third-party) so that once explicit consent has been given to a set of domains, there is no need to reapply for it. The sites may propose to the user to limit the duration of consent and to revoke it at any time by clicking on the appropriate icon. Consent may be recorded for certain categories of cookies, such as “functional” or “analytical”.

CookieQ can be configured to automatically delete first- and third-party cookies as well as storage items for which consent has not been given or revoked.
5.5.2 The TartAuCitron solution

The centralised collection of consent for various functionalities (deposit of cookies, social buttons, videos, other modules inserted on the pages of the site) takes place at once for the duration envisaged by the site.

**Réseaux sociaux**

Les réseaux sociaux permettent d’améliorer la convivialité du site et aident à sa promotion via les partages.

Facebook

> En savoir plus  > Voir le site officiel

Autoriser  Interdire

Twitter

> En savoir plus  > Voir le site officiel

Autoriser  Interdire

Twitter (cards)

> En savoir plus  > Voir le site officiel

Autoriser  Interdire

Twitter (timelines)

> En savoir plus  > Voir le site officiel

Autoriser  Interdire

*TartAuCitron: a centralised consent management solution*

**Conclusion:** Consent management, using tags, on a site-by-site basis, meets the provisions of the RGPD and also covers the proposed ePrivacy Regulation. More importantly, it makes it possible to collect users’ preferences in a dialogue where the site can explain its economic model. This answers the need for transparency and respect (cf. § 2.2) expressed by Internet users: what data is collected, for which processing and use, and in return for which service? Unlike centralised management at the browser level, a genuine dialogue is initiated whereby the site manager can explain to the user the economic effect of his or her choices.

6 The economic impact of the European proposed regulation

The analysis of the economic impact of the proposed ePrivacy Regulation, limited in the case of our study to Articles 8, 9 and 10, should make it possible to estimate the additional impact that they will have in relation to the current regulations and the entry into force of the GDPR in May 2018. The assessment carried out for the European Commission provides an estimate of compliance costs according to different scenarios of regulatory proposals. During the task force’s interviews, three other economic impacts were highlighted:

- impact on the digital advertising market;
- impact on e-commerce, marketing and customer relations (CRM));
- impact on the competitive position of companies, particularly vis-à-vis large Internet platforms.

---

44 Evaluation and review of Directive 2002/58 on privacy and electronic communications
6.1 Impact on the digital advertising market

According to the SRI - UDECAM - PWC digital advertising barometer\textsuperscript{45}, digital advertising has, since 2016, become the leading advertising sector in terms of media investment (33%), ahead of television. This growth continued (+9.8%) in the first half of 2017. PWC provided the task force with a market estimate for 2021, as shown in the table below. The GDPR and its implementation date were known when it was established, but ePrivacy was only a project at this stage.

<table>
<thead>
<tr>
<th>Internet advertising in France (US dollar millions) - Source PWC</th>
<th>2016</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile internet advertising</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile video Internet advertising in France</td>
<td>316</td>
<td>560</td>
<td>617</td>
<td>672</td>
</tr>
<tr>
<td>Mobile paid Search Internet advertising in France</td>
<td>175</td>
<td>445</td>
<td>503</td>
<td>560</td>
</tr>
<tr>
<td>Mobile paid Search Internet advertising in France</td>
<td>908</td>
<td>1 709</td>
<td>1 897</td>
<td>2 011</td>
</tr>
<tr>
<td>Total Mobile internet advertising in France</td>
<td>1 399</td>
<td>2 713</td>
<td>3 017</td>
<td>3 243</td>
</tr>
<tr>
<td>Wired internet advertising</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classified Internet advertising in France</td>
<td>495</td>
<td>584</td>
<td>612</td>
<td>638</td>
</tr>
<tr>
<td>Other Display Internet advertising in France</td>
<td>554</td>
<td>463</td>
<td>455</td>
<td>451</td>
</tr>
<tr>
<td>Video Internet advertising in France</td>
<td>288</td>
<td>390</td>
<td>414</td>
<td>438</td>
</tr>
<tr>
<td>Paid Search Internet advertising in France</td>
<td>1 186</td>
<td>796</td>
<td>765</td>
<td>757</td>
</tr>
<tr>
<td>Total Wired internet advertising in France</td>
<td>2 522</td>
<td>2 232</td>
<td>2 247</td>
<td>2 283</td>
</tr>
<tr>
<td>Total Internet advertising in France</td>
<td>3 922</td>
<td>4 946</td>
<td>5 264</td>
<td>5 526</td>
</tr>
</tbody>
</table>

According to this forecast, the growth of the French digital advertising market is expected to be driven by the mobile market. Parallel developments are also expected in Europe and the United States.

The success of digital advertising stems from the fact that it has allowed advertisers to switch from media planning to audience planning, i.e. campaigns designed according to the profile of the individuals to whom the advertising message will be sent. This trend continues with personalisation, which aims to deliver an individualised message or offer, adapted to a specific user or group. It also refers to online behavioural advertising (OBA), built on the profile of an individual or a group according to their location, their search history, and more generally the collection and treatment of their browsing activity. Since, on the Internet, all major brands have become media (via their sites, social media, etc.); advertising then becomes part of their customer relations management (CRM).

However, in the analyses, it is not always possible to clearly distinguish between cases where digital advertising relies on uses of data regulated by GDPR or ePrivacy (such as OBA) and cases where such use is not regulated (e.g. some contextual advertisements).

\textsuperscript{45} Obsepub, (SRI, PWC, Udecam), 17th edition and 18th edition of July 2017
Effectiveness of recommendations based on behavioural analysis

Quoted during a hearing conducted by the task force, the following example illustrates the effectiveness of behavioural targeting in making recommendations:

On a media site, a test was conducted in the summer of 2016 to compare the performance of an internally produced recommendation for news articles (contextual, based on simple rules of semantic proximity between the tags used to qualify articles) with that of a recommendation for articles calculated by a third-party, based on the users’ behaviour (and thus using third-party cookies and algorithms).

Over the test period (one month and a half) and in equivalent context (same location, same block design), were observed:

- A click-through rate of 1.3% for contextual suggestions (i.e. without third-party cookies)
- A click-through rate of 2% on algorithmic recommendations (with third-party cookies).

These are averages over a short period of time. Nevertheless, throughout the period there was a widening gap between the two solutions. In conclusion, the use of an actor specialised in video recommendation, based on user behaviour and the use of algorithms, improves the performance obtained, compared to the current rules of content suggestion.

The two main markets for digital advertising are Search (search engines) and Display (banners or videos, on all sites including social media). According to the studies, the scope of the other levers (affiliation, comparators, e-mailing, classified ads) can vary, but represents only 10% to 15% of the market.

6.1.1 Search switches over to mobile and makes increasing use of artificial intelligence

Search (paid search engine links) should continue to account for half of the digital advertising market. It is becoming predominantly mobile and increasingly local. According to the e-pub observatory, local search (information related to the site of the research) accounted for one-third (32%) of mobile search revenues in France in the first half of 2017.

Since people use their smartphones dozens of times per day, most of the time for a few seconds, browsing must be sped up. Google is promoting a standard, "Accelerated Mobile Pages (AMP)”, for "lighter" pages, especially in advertising: sites that meet this standard are better ranked in mobile search results.

In addition, following a search, the optimised extract, a short paragraph placed at the top of the results (known as the zero position), uses artificial intelligence to understand the meaning of the user’s query and propose the most explicit excerpts from the pages found. If the answer is sufficient for the Internet user, the search engine no longer refers to opening a new web page.

Google dominates the French search engine market with a 92.04% share (reference StatsCounter, October 2017) ahead of Bing (4.99%), Yahoo (2.11%), DuckDuckGo (0.68%) and 0.12% for the other search engines (MSN, Yandex Ru, Qwant, Ecosia,...).

Search advertising targeting is based on the data collected by the search engine: contextualisation of the search but also the search history and, for local searches, geolocation (fixed or mobile). Search engines display their privacy rules, and already provide for asking the consent of the Internet user to
the processing of certain data. The collection of this consent will in future be better supervised by the GDPR. It is possible that privacy concerns may lead a growing number of Internet users to limit the collection of their data. This is the challenge met by Qwant, a French search engine that does not deposit cookies or collect any personal information.

However, every Internet user regularly uses a small number of search engines that provide an essential service free of charge.

**In the context of such a relationship, it will be easier to acquire the user’s consent.**

6.1.2 **The growth of Display (banners) is driven by social media**

Display (advertising banners) is growing faster than Search, but this growth is almost exclusively driven by social media.

The advertising offer on social media is targeted on the profile of Internet users who have opened an account: advertisers have access to a selection of parameters that can allow very precise targeting. They have no access to the data of Internet users, but the company that manages the network guarantees that the advertisements will be served only to the users corresponding to the parameters that advertisers have chosen.

It should be noted, however, that the system’s lack of transparency is currently widely criticised.

Internet users access social media through their personal accounts. The acquisition of consent on the use of personal data of the Internet user is done today at the time of the creation of the account, via the acceptance of the general conditions of use. With the GDPR, the publisher of the application will have to request specific consent for the use of personal data. However, every Internet user who chooses to become a member of a social network receives a free service (excluding premium packages).

**In the context of such a relationship, it will be easier to acquire the user’s consent.**

In order to analyse the situation of the advertising market for banners outside social media, we must distinguish between direct purchases from the site selling these advertising spaces and so-called "programmatic" purchases. Programmatic advertising (see Appendix 3) is a technical tool for managing advertising campaigns that allows ads to be served “impression by impression”. It is capturing a growing share of the Display market. Advertising on social media is programmatic, as well as a large part of the video.

Programmatic advertising can be used for direct space purchases (presale of ad space by contract) or for auctions (RTB, real time bidding) on an open platform. According to the IHS, RTB’s share of programmatic advertising, which has grown very strongly, should peak (to less than half of the programmatic). The same trend is estimated in the United States (44% of RTB in 2017 according to e-Marketer).

---

46 Categories are powered automatically from what users post about themselves

47 When a page is displayed, the programmatic technical channel selects which advertisement is displayed, in particular according to data available on the user who calls this impression

48 European Programmatic Market Sizing 2015 (September 2016)
Within the Display, according to an IHS Markit study\textsuperscript{49}, 86% of programmatic advertising uses behavioural data, as well as 24% of non-programmatic advertising. Advertising using the data would thus represent €10.6 billion out of a €16 billion display market in Europe. With programmatic growth, these figures should rise to €21.4 billion from a market of €23.5 billion in 2020. These figures are consistent with those of the American market: in the United States, programmatic advertising represented 73% of the Display in 2016 and should grow to 85% in 2019 (source: eMarketer, April 2017). However, the impact of programmatic advertising is less important on Display outside social media. This is particularly the case in France, as is shown in the table below.

<table>
<thead>
<tr>
<th>Zenith Study : advertising expenditure forecast France - September 2017 - M€</th>
<th>2016</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>1204</td>
<td>1922</td>
</tr>
<tr>
<td>Including social media (100% programmatic)</td>
<td>453</td>
<td>1193</td>
</tr>
<tr>
<td>Display excluding social media</td>
<td>751</td>
<td>729</td>
</tr>
<tr>
<td>Programmatic Display</td>
<td>639</td>
<td>1468</td>
</tr>
<tr>
<td>Share of programmatic within Display</td>
<td>53%</td>
<td>76%</td>
</tr>
<tr>
<td>Programmatic Display excluding social media</td>
<td>186</td>
<td>275</td>
</tr>
<tr>
<td>Share of programmatic within Display excluding social media</td>
<td>25%</td>
<td>38%</td>
</tr>
</tbody>
</table>

According to this forecast, by 2019, content sites, excluding search engines and social media, are expected to sell on average less than half of their advertising space via programmatic channels, and within them, less than half by real-time auctions. A site that sells half of its spaces through programmatic channels (of which 85% is using behavioural targeting, according to IHS data) and the other half live (24% using behavioural targeting, IHS data), would then have 50% of its advertising space sold using targeting data. However, it should be pointed out that this type of average calculation covers a great heterogeneity according to the nature of the sites.

---

\textbf{The value of advertising space increases with accompanying data}

For an advertiser, an important parameter to measure a banner’s effectiveness is the click-through rate. According to the above-mentioned IHS study, these rates are very different: 0.7% for pre-sold campaigns, 3.8% (5 times more) with behavioural data, 6.9% (10 times more) for retargeting. Naturally, this difference in click-through rates translates into different advertising space price ranges: CPM (cost per thousand) from 0.4€ to 8€ without behavioural targeting, CPM from 1.8€ to 25€ with targeting.

Other studies report a lower price differential. A 2014 study\textsuperscript{50} estimates that an impression accompanied by a cookie can be worth 60% to 200% more, depending on the age of the cookie (a recent cookie giving less information).

Since 2010, it has been possible to refuse (opt-out via an AdChoice icon) targeted advertising. A recent US study\textsuperscript{51} analyses the value of ads served to Internet users using this possibility. Only 0.23% of impressions are served to American Internet users who use this opt-out, but the corresponding ads are 59.2% cheaper.

---

\textsuperscript{49} The economic value of behavioural targeting in digital advertising HIS Markit 2017

\textsuperscript{50} An empirical analysis of the value of information sharing in the market for online content, J.H. Beales and J.A. Eisenach

The individuals interviewed by the task force provided analyses confirming the order of magnitude of these figures. On a mobile advertising platform, an analysis of programmatic purchases was carried out from 19/09/2017 to 03/10/2017 to estimate the effect of the new iOS 11 version of Apple on advertising prices. During this period, the average purchase price of mobile web impressions on Safari iOS11 decreased by 25% (paved format), 33% (interstitial format) and 50% (banner format) compared to purchases made on previous versions of Safari.

Programmatic advertising and targeting have a cost: it is estimated that for every €100 spent by an advertiser, €40 goes to the site displaying the ad and €60 to technical intermediaries (source: WFA / UDA).

It should also be noted that targeting makes it possible to reach Internet users by following them in their navigation on "inland pages" or on sites of low notoriety, whose price of ad space is less expensive, in order to provide for targeted advertising at a lower cost.

A large part of the value provided by targeted advertising is thus captured by the advertiser (best click-through rate) or by technical intermediaries, but the difference in revenue for content sites remains significant. The people audited during the task force's remit confirmed that, once the cost of technical intermediaries has been deducted, the price paid to the publisher increases with the data, sometimes citing a 20 to 30% increase in the CPM, sometimes a factor of 2 (from 0.5 € to 1 € for the CPM).

Apart from the major market players and some companies created using digital technology, content sites need to call on specialised sub-contractors who deposit third-party cookies that enable them to offer targeted advertising on their pages. If these cookies are refused by Internet users, this can produce two effects: a loss of value for "premium" spaces pre-sold directly to advertisers (programmatic or not), and the risk of no longer finding advertisers for other spaces, which are often sold at auction on an open platform (RTB). It can be estimated that for a site that sells half of its spaces accompanied by behavioural targeting, half of them in RTB, a quarter of these spaces would remain unsold and the rest would be devalued by a third, leading to a drop in total revenues of nearly 25%.

It should not be forgotten that such a site could not compensate for the decline in the value of its ad spaces by increasing the advertising pressure on its premium pages, as this would lead to a decrease in audience. An example of this was provided to the task force by an advertising agency. Following a malfunction in 2017 leading to an increase in advertising pressure, the drop in audience, accompanied by an increase in ad blocks, led to a halving of the volume of advertising served!

The evolution of the digital advertising market is determined by the advertisers and ecosystems of large digital platforms, who play a leading role as technical prescribers. Other players, in particular newspaper publishers, do not have sufficient weight and expertise to influence the market. They must follow its evolution, by grouping together and relying on specialised third parties if they want to maintain their autonomy, or by joining the ecosystem of the major platforms.

The risk of exclusion from the market is high: advertisers need audience segmentation to limit advertising pressure. As a targeted offer will remain abundant via the large platforms, ad space without data will be devalued more and more.

---

52 Large digital platforms occupy a large share of this market, but there is a dynamic alternative offering that allows content publishers to diversify their subcontractors.
6.1.1 Advertising plays a special role in the economic viability of the press

The study of the economic models of the press is beyond the scope of this study. For the publishers interviewed during the task force, in particular for the traditional press, the advertising market is not a solution on its own: the objective is to preserve the initial business of selling content by convincing part of the online audience to take up a subscription. This transition is difficult: digital revenues do not generally offset the decline in revenues from paper, subscriptions and advertising.

The prospects for the digital press advertising market are not negative, as this market should experience some growth, even if it is less important than that of search engines or social media, as shown in the table below.

<table>
<thead>
<tr>
<th>PWC GEMO Study 2016 (in millions of €)</th>
<th>2016</th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital newspaper advertising</td>
<td>199</td>
<td>233</td>
<td>245</td>
</tr>
<tr>
<td>Advertisements in digital general-interest magazines</td>
<td>423</td>
<td>590</td>
<td>653</td>
</tr>
<tr>
<td>Digital advertising in professional journals</td>
<td>169</td>
<td>213</td>
<td>227</td>
</tr>
<tr>
<td><strong>Total digital advertising in the press (Display incl. video)</strong></td>
<td><strong>791</strong></td>
<td><strong>1036</strong></td>
<td><strong>1125</strong></td>
</tr>
</tbody>
</table>

There is a large audience for press sites. Facebook (Facebook Connect) or Google (Insights engine project) regularly develop new offers for content publishers. For their part, to maintain independent access to advertisers in programmatic channels, French newspaper publishers are developing a cooperative approach (La Place Média, Audience Square, Gravity) alongside the world’s major digital platforms.

Traditionally, an advertising agency presells the spaces of press companies to advertisers or their agents by contract (often through a "programmatic" channel) and offers unsold items at auctions via an open platform (RTB). Press publishers generally use specialised third parties to manage audience tracking and targeting. Therefore, they nowadays largely use third-party cookies.

According to a study conducted by Monitor Deloitte for the National Daily Press Union (SPQN), 52% of national daily press revenues (£377 million) will come from digital media by 2020. The study assumes that by 2020, 100% of advertising revenues will come from ads linked to data that requires third-party cookies. It is also based on a survey conducted by Deloitte among 6,000 Internet users in 3 countries (England, France, Germany, 2000 people in each country), which estimates that the acceptance rate of third-party cookies (88% today) would only be 13% if the question were explicitly asked. On this basis, the SPQN study concluded that two-thirds of digital revenues could be lost. This is clearly a breakthrough scenario based on the assumption that the virtual disappearance of third-party cookies as a result of the ePrivacy Regulation would lead to the collapse of online press advertising revenues.

---

53 https://marketingland.com/google-publishers-user-data-insights-engine-project-225452
54 Monitor Deloitte Etude d’impact du projet de règlement ePrivacy 27 Juillet 2017
We can temper this scenario:

- the current acceptance rate of third-party cookies on the websites of the national daily press is 95%, based on the information provided by these websites. This is higher than the Deloitte survey’s 88%. As part of a dialogue with their readers, press sites could continue to achieve a higher acceptance rate. A study by the GFK also predicts an acceptance rate for targeted advertisement of 20% in Europe;
- without data, the premium advertising space of the press will retain a certain value, even reduced (see last § of the insert on page 40). On the other hand, the other ad spaces will have much more difficulty to find takers.

With these assumptions, it can be considered that the loss in the value of advertising space would be less significant. If it were in the order of 25% (see § 6.1.2) it would, however, cancel the prospect for growth in the press’s advertising revenues.

As we pointed out at the outset, for many newspaper publishers, the advertising market alone is not a solution to ensure economic viability. A significant part of the anticipated loss of growth revenue is not related to advertising, but to the reduced possibility of following readers’ practices in order to offer them suitable subscription offers. Readers’ knowledge is a strategic subject for the development of the press, as is the knowledge of its customers for any company. Since only a small minority of readers is currently subscribing, on the internet, this knowledge is based on targeting techniques. This is targeting for a purpose which is separate from advertising.

Content publishers need a technique for the individual tracking of their readers, to serve them content or offer tailored subscription packages.

6.1.2 Advertisers call for more transparency

On the advertisers' side, there is a strong demand for improved transparency of the digital advertising channels.

The cost of technical intermediaries in the advertising chain is high, 60% according to figures communicated to the task force by the Union of Advertisers (source: WFA / UDA). It is also the estimate published in the United States by the ANA (Association of National Advertisers) in 2014. A more recent ANA study shows that the share of intermediaries can drop to 42% on a sample of campaigns, using direct programmatic purchasing, that are well managed by advertisers. The study points out that the advertisers should make an effort to gain more transparency: “it is therefore recommended that advertisers demand and secure a source of independent transactional information for their buys. One recommended approach is to access and control your programmatic transaction level data - winning bid log data and metadata - to serve as the advertiser's record of transaction (e.g. "programmatic invoices")”. In August 2016, the ANA launched a working group on transparency, which concluded a year later that transparency issues do exist, which must be resolved through improved controls by advertisers.

56 https://pagefair.com/blog/2017/new-research-how-many-consent-to-tracking/
57 Programmatic: Seeing Through the Financial Fog, May 2017
58 http://www.ana.net/miccontent/show?id=ii-production-transparency-2017
The French advertisers grouped in the UDA regularly echoed this concern for transparency and in its editorial of October 2017, the president of the UDA made it a high priority of the association's action for 2018.

This need for transparency translates into the need to collect data to better measure the effectiveness and efficiency of a campaign.

In conclusion, the development of the advertising market on the Internet is driven by audience growth and the performance of targeted advertisements (behavioural advertising). Content sites do not play a prescriptive role for advertisers and must adapt to enhance their audience, or run the risk of seeing their advertising space devalued. Search engines and social media (Facebook, Twitter, LinkedIn) are used for free by a large majority of Internet users. They are well placed to obtain the consent of their users, and will be able to continue to sell their advertising space via programmatic channels with their own targeting data. They will therefore be little affected by the proposed ePrivacy Regulation and will be able to continue to offer advertisers effective behavioural advertising. On the other hand, content sites will have much more difficulty in achieving this.

6.2 E-commerce, online marketing and customer relation management

Privacy protection is an important dimension of trust in the digital economy. Furthermore, regulatory differences between European countries are considered as one of the main barriers to the development of cross-border e-commerce. Therefore, the European Commission's decision to legislate by regulation for the protection of privacy, because it allows harmonisation, was initially welcomed by e-commerce specialists.

Since then, there has been a growing concern about the future of the use of technologies to monitor Internet users. According to the European e-commerce association EMOTA, trackers are used:

- for technical management: 77% of e-commerce sites use cookies, firstly for shopping cart management, the user's language and payment settings;
- for marketing: 72% of sites use customer data (largely collected via cookies) for marketing purposes;
- for advertising: one site out of two generates more than 20% of its turnover by hosting third-party advertising.

The first point (technical management) is particularly important for the fluidity of navigation and the execution of an act of purchase. Websites on which Internet users register can more easily offer fluid navigation (which can end with a one-click payment), which increases the competitive advantage linked to the size of e-commerce platforms. As of Q1 2017, 10 of the top 15 e-commerce sites in France are marketplaces, i.e. platforms that put buyers in contact with third-party sellers (source: Fevad - Médiamétrie). On Amazon, for example, for 288 million references, only 2.8 million are Amazon products, the others come from the marketplace (figures published at IRCE 2016).

In addition, online marketing is largely based on personalisation. All e-commerce sites, as well as content sites, use the data available to them on Internet users to personalise their offer, i.e. to offer a product, service or content that is adapted to a customer's specific preferences. Personalisation

59 EMOTA press release, 28 August 2017
begins as soon as you browse the site, optimizing the itinerary offered to Internet users. Whether it’s
browsing through a database of millions of product references, navigating through a content site, or
displaying targeted advertising, the techniques are essentially the same. The site carries out an
automated management of what is displayed on the page according to data collected on the user.

This is particularly the case for recommendations, which have become widespread, both on content
sites and e-commerce sites, to suggest a continuation of the course of his navigation to an Internet
user. In any case, it is a question of predicting a score of interest of the user for a series of
propositions and to take into account this score in what is presented to him.

For the revenues that e-commerce sites derive from advertising resources, the issue is the same as
that mentioned in point 6.1 above.

Platforms that benefit from a regular customer base will find it easier to obtain the consent of their
customers. This will be more difficult for e-commerce sites that serve more occasional customers.

In the absence of a simple and fluid solution, the impact of large platforms, on which a large number
of Internet users are registered, will continue to increase.

### 6.3 Impacts on the competitive position of stakeholders

In early 2017, the acceptance of Article 10 of the ePrivacy project was often favourable, for example:
"Ecommerce Europe also welcomes the fact that the proposed Regulation will allow consent to be
given by browser settings when technically possible, because this will reduce the consumer’s consent
fatigue and make it easier for online merchants to seek the consumer’s consent."

However, this initial favourable reception did not last, with the realisation, as early as the summer of
2017, that "The major developers of browsing software (Google Chrome, Microsoft Internet Explorer,
Apple Safari) – all based outside of the European Union – would be able to regulate standard access
to the terminal equipment by browser setting consent systems, not only for themselves but also for
their competitors."

A clear distinction must be drawn, in the settings of software giving access to
electronic communication services, between what is covered by the trackers used
by the software publisher for its own purposes and what is covered by the
trackers used for the services to which it gives access.

This distinction is all the more important because, if these software programs appear to the public as
 guaranteeing the respect of the privacy choices made by the Internet user, they will be in a position
of privileged trust. There may then be a potential conflict of interest between their role as
"custodians" and their own activities.

In order to lay the groundwork for a more concrete analysis, the task force undertook an
examination of the issues according to the 3 main technical options identified in Chapter 5: filter the
trackers according to white or black lists, according to the purpose of tracking, or according to the

---

nature or techniques of tracking. These options concern the trackers used by the services to which the software gives access, not those that can be used by the editor of the software for its own needs.

6.3.1 Filtering according to black/white lists

Nowadays, publishers who offer list filtering use lists that have already been created. These are not empty, because it would be an ineffective solution for the Internet user, who would need to invest too much time to constitute them. The exclusion lists of intrusive or dangerous sites are drawn up on the basis of knowledge that the Internet user does not have. Even if the lists can be individually modified at the user's request, which is desirable, their economic impact is important. It is in fact likely that belonging to a list will have an immediate effect for a site or an application, and that the operator may have difficulty in having this modified by the Internet user.

The first question is therefore the governance of the list and the transparency of this governance:

- publication of the lists, which can include thousands of items;
- whether or not it is possible to contest or request inclusion in a list;
- protection against conflicts of interest of the list manager;
- how updates are carried out.

To be effective, this governance can only be conceived within the framework of a reactive and agile system. Depending on the options, it may be more or less shared according to processes open to third parties.

The governance of lists gives economic power to those who exercise it.

6.3.2 Filtering according to the purposes of tracking

This is the request of many stakeholders, who hope to enable Internet users to make informed choices. By selecting a reasonable number of categories (8 in the case of Ghostery), the Internet user could be offered a choice related to his perception of the more or less acceptable or intrusive nature of the proposed purpose.

The implementation of such a solution must solve two problems. The first is the difficulty in defining the content of categories. The practice of A/B testing, for example, is considered by many digital players as a natural asset of the net and a harmless practice if it is well supervised. For others, it is based on the constitution of control samples that require specific prior consent. To the best of the task force's knowledge, there is currently no recognised standard that would make it possible to define categories that would be consensual. The second problem is the difficulty of assigning a specific tracker to a category, which would require qualification of the tracker's purpose, display of that purpose and control.

In the end, except a governance of categories giving guarantees of independence is conceived and implemented, the editor of the filtering software would exercise an economic power analogous to what is detailed in the previous case.

6.3.3 Filtering according to the nature or the techniques of tracking

The distinction between first- and third-party cookies has made it possible to set up a first browser configuration solution, which has been in existence for several years. It has the advantage of being both simple and objective, but it is now widely considered too rudimentary to be effective, as shown by the example of Apple's solutions. But this example also shows that we are rapidly losing transparency and efficiency gains! Not to mention that the technical specifications are not fixed: we assume that the solution proposed by Apple (particularly the configuration of the Intelligent Tracking...
System) is destined to evolve according to the technical tricks that will be found by the stakeholders of digital advertising to slip through the cracks of the system.

As we can already see from the reactions towards Apple, any "proprietary" solution will have to be examined in terms of its real effect, in practice, on market players. In particular, it will be necessary to verify that if some stakeholders are less penalised than others, this will be done under good conditions of transparency and fair commercial practices.

This rapid analysis shows that the setting up of a software for access to communication services, for the protection of privacy, bears the character of a service to users, which falls under the responsibility of the editor of this software.

Such access or access control software may be used to record specific consents given by the user of the terminal for a particular domain or service, but they do not currently have any legal obligation to ask for consent, and will not be required to do so under the GDPR, for the processing of data that the software publisher does not carry out itself, or that is not carried out on its behalf. This consent must be requested by the operator responsible for data processing directly to the Internet user.

If the management of consent becomes a legal obligation of access control software for communication services, and if this is accompanied by an obligation to offer a default setting denying consent, questions arise concerning consent given on a case-by-case basis by the Internet user:

- as far as browsers are concerned, the solutions chosen today by the editors, who have chosen these options for their ergonomics, their simplicity of implementation and who integrate an expertise in security that the user does not have, would become obsolete. Is it desirable to impose a single system?
- Operating systems are also access software. But Windows 10, for example, does not allow the user to control the settings of a browser that is not Microsoft-dependent. More generally, when access to an electronic communication service depends on a chain of several software packages controlling access, as is the case for personal assistants, how is the responsibility shared?

7 Proposals

In light of the foregoing analyses, we believe that beyond implementation of the GDPR, the proposed ePrivacy Regulation, as it stands, could bolster the position of the major internet platforms that have regular users, many of whom have opened a private account. On the other hand, it may undercut those stakeholders that operate services and sites that cater to less regular customers. Were it to introduce mandatory settings for software used to access electronic communications services, this move could be rejected by users, as the user-friendliness has not been tested and it is not known whether these settings meet users' needs.

We are putting forward four principles that could inform both discussions and the French position when the text of the Regulation is being discussed.
7.1 To ensure sustainable protection of privacy, the Regulation must be technology neutral

The brief overview of the access software and possible solutions described in the report shows the complexity and highly-evolving nature of the ecosystem.

The example of Safari/iOS 11 shows the richness and complexity of a privacy protection system, which will also have to evolve. More generally, the diversity of markets (fixed, mobile electronic communications services, the Internet of Things - from watches to connected vehicles) and, for each market, the variety of options (access software settings or options, installation of extensions such as tracking protection software, ad-blockers or anti-viruses) mean that it is impossible to define technical specifications covering such a broad field.

In addition, new responses to bolster privacy protection are emerging through anonymisation techniques (see the example of connected vehicles), the development of “privacy by design” or data processing technologies (differential privacy).

To ensure that access to electronic communications services respects privacy in a sustainable manner in an ever-changing environment, the drafting of the Regulation must be technologically neutral. This should apply to both its articles and recitals, as highlighted, for instance, by the Mozilla Foundation in its position paper\(^\text{62}\) on recitals 22 to 24. Although successive versions of the proposed Regulation have tended to become more technology neutral, this remains an imperative.

Proposal n° 1. The proposed Regulation should be technology neutral, throughout the text including the recitals.

7.2 The privacy protection software offering must continue to diversify and develop

The ability to prevent third parties from storing information on terminal equipment, or processing information already stored, may be a functionality proposed by the publisher of access software for electronic communications services, or of an add-on of such software, which may be provided by another company.

The best way to ensure that the solutions offered meet different user expectations and their desire for user-friendly applications is for the range of privacy protection software to continue to diversify and develop. This would involve the various access control software, in particular extensions, being considered at the same level as access software for electronic communications services.

Publishers’ know-how is reflected by the scenarios put forward for protecting Internet users’ data, by explaining the parameters of these scenarios and their consequences and giving Internet users the opportunity of choosing between them. Publishers must be able to freely choose the parameters of these scenarios, especially for the default option. This is a service offered to users.

---

\(^{62}\) https://blog.mozilla.org/netpolicy/files/2017/10/ePrivacy-position-paper_-FINAL.pdf
Such access or access control software may record the consent given by the user of the terminal, but must not seek this consent (within the meaning of Article 9(2)), which in any event must be requested by the data processing manager directly from the Internet user.

**Proposal n° 2.** The privacy protection software offering must continue to diversify and develop. The Regulation should not provide certain software with a privileged “gatekeeper” role. Access or access control software for electronic communications services must offer several protection scenarios, clearly explain the implications of these different options and provide a simple procedure for accepting the default settings, reinforcing them or making them more flexible.

As regards the settings of software giving access to electronic communications services, a clear distinction must be drawn between what is covered by the trackers used by the software publisher for its own purposes and what is covered by the trackers used for the services to which it gives access. These publishers would be in an unusual position as they have to obtain the consent of Internet users for the data they use for their own purposes whilst being seen to uphold these users’ privacy with regard to third-party services. Care should be taken to ensure that this situation does not give rise to a conflict of interests, in particular as regards the commercial activity of these publishers.

This is particularly important when the publisher occupies a dominant position in its market.

**Proposal n° 3.** Competition law enforcement authorities need to consider the impact of the options (including default settings) offered by software providing access to communications services, when their publishers hold a dominant market position.

### 7.3 To maintain an open Internet, a “feedback channel” is required

Services or websites catering for occasional users need to establish direct contact with them in order to be able, on one hand, to customise their offering, which is one of the advantages of online services and, on the other, to propose the financial terms of the service, including funding through advertising.

This dialogue with the Internet user, which is used to approach him/her, to obtain his/her consent and, if necessary, to amend, for this specific site, the configuration of the control software that allowed access to the service in question, represents a “feedback channel”.

One solution would be to define the functional specifications of this “feedback channel” and to begin an international standardisation process to define the functionalities that should be provided by software for access to electronic communications services. This process should involve all stakeholders and inspire confidence on the part of the service providers that are reliant on this access software.
The example of the failure of the P3P protocol\textsuperscript{63} in 2006 and the slow progress of attempts to standardise the Do Not Track header within the W3C show the difficulty of this type of approach, whose success within a timeframe compatible with the implementation of the ePrivacy Regulation is not guaranteed.

For this reason, the proposed Regulation must mention the need for access software to propose a simple and ergonomic procedure for correcting its settings to include the consent given by an Internet user for a particular site or service.

\begin{quote}
\textbf{Proposal n° 4.} Access or access control software for electronic communications services must propose a simple procedure for correcting its settings to include the consent given by an Internet user for a particular site or service.
\end{quote}

The so-called tracking wall issue must be addressed. A company must be able to make access to its services contingent on the acceptance of various terms and conditions (subscription, advertising, etc.). The aim is to ensure continuous dialogue between the supplier and its customer on the financial terms of the service, and to offer, for example, a subscription, a premium service with acceptance of targeted advertisements, or a basic service (freemium) with no targeted advertising, or any other option compatible with the GDPR.

The Commission’s proposed ePrivacy Regulation did not explicitly rule out these options. As the European Parliament’s proposal seems to be looking to exclude them, we believe it is important to reassert that they are necessary to ensure the economic equilibrium of many sites or services.

\begin{quote}
\textbf{Proposal n° 5.} If a service provider wishes to use, for commercial or service development purposes which are not strictly necessary for the provision of that service, terminal equipment processing or storage capacities, it must be able to offer the user several options for accessing the service, depending on whether the user has given his/her consent or not.
\end{quote}

One feature of digital technology is the “long tail”. This means the ability to offer a very large number of small and medium-sized stakeholders access to Internet users. With the development of large international platforms, which are capturing a growing share of value, the relative market share that can be captured by small and medium-sized players is becoming marginal.

The ePrivacy Regulation may be an opportunity to promote the development of digital markets that protect personal data. As a result, it should not hamper the expansion of European players, be they digital players or traditional companies in transition, in relation to the major international digital platforms, none of which are European. Nor should they be pushed into the arms of these platforms, as this could strengthen the latter’s oligopolistic position. As the transformation of the music market shows, players need time and resources to adapt their business models. These players rely on the

\textsuperscript{63} http://www.allaboutcookies.org/p3p-cookies/index.html
support of specialised third parties for a successful transition, which must not be endangered by an all-too-hasty implementation of the ePrivacy Regulation.

**Proposal n° 6.** The deadlines for the implementation of the ePrivacy Regulation must be adjusted, particularly after the Regulation has been adopted, to allow the most vulnerable stakeholders to adapt themselves.

### 7.4 Regulating advertising pressure on the Internet

The rapid growth of the digital advertising market is not without its downside. Advertising pressure is sometimes poorly controlled, and this has been reflected by the rise in the use of ad-blockers. The market is not always transparent for professionals and this causes malfunctioning or fraud (high rate of clicks on ads by robots, measurement errors on the number of ads served or seen, etc.).

Part of the perception of advertising pressure stems from the reaction of Internet users to ads that are considered invasive, some of which, such as targeted ads, use personal data. However, the regulation of advertising pressure is not primarily to be governed by the ePrivacy Regulation. It is up to companies to organise themselves in response to the rise of ad-blockers and in a bid to improve the user experience.

This is an issue that has already been taken up by the whole of the advertising industry, particularly through the ARPP (a French self-regulatory body for the advertising industry) and its members. This goes beyond e-privacy, but improving the image of advertising among Internet users would make it easier to obtain their consent for targeted advertising.

**Proposal n° 7.** Initiatives for the self-regulation of advertising by professionals should be encouraged by the public authorities.

**Proposal n° 8.** A programme to monitor the transparency of the advertising chain should be implemented by the public oversight authorities.
ANNEXES
Annexe 1 : Lettre de mission

LE MINISTRE DE L’ÉCONOMIE ET DES FINANCES

LE SECRÉTAIRE D’ÉTAT AUPRÈS DU PREMIER MINISTRE, CHARGÉ DU NUMÉRIQUE

LA MINISTRE DE LA CULTURE

Monsieur Luc ROUSSEAU
Vice-président
Conseil général de l’économie
Ministère de l’Économie et des Finances
139, rue de Bercy
75572 PARIS Cedex 12

Paris, le 23 OCT. 2017

Nos réf. : TR/2017/P/25529/CMA

Monsieur le Vice-président,

La Commission européenne a présenté le 10 janvier 2017 une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (ci-après « le règlement e-privacy »), présenté comme une lex specialis du Règlement général sur la protection des données personnelles (RGPD) adopté en avril 2016 et entrant en vigueur le 25 mai 2018.

Ce projet de texte est en cours d’examen par le Conseil des ministres de l’Union européenne (UE), dans sa formation « Transports, télécommunications et énergie ». Au départ, la Commission a affiché son souhait de finaliser les échanges au plus vite pour que ce texte, d’application immédiate dans tous les États membres, entre en vigueur dès le 25 mai 2018, soit en même temps que le RGPD. Les articles 8 à 10 du projet de règlement e-privacy, relatifs à l’encadrement des cookies, à la définition du consentement et à son recueil via le paramétrage du navigateur suscitent de vives inquiétudes tant parmi les représentants de la presse et des médias en ligne que parmi les acteurs de la publicité digitale.

En effet, l’encadrement renforcé prévu dans le projet de règlement pourrait conduire une part significative, voire majoritaire, des internautes à refuser a priori certains cookies. Or ces derniers sont utilisés aujourd’hui pour la personnalisation du contenu des sites, qui constitue un important facteur d’attractivité du service pour les utilisateurs, et pour la publicité ciblée, dont le développement, conjugué aux progrès techniques dans la gestion des données, laisse présumer une amélioration à court terme du modèle économique encore déséquilibré des éditeurs de services en ligne.
Nous vous serions reconnaissants de nous fournir des éléments d'analyse qui permettraient d’apprécier plus précisément l’impact des mesures envisagées dans le projet de règlement sur les acteurs concernés à la fois sur le plan économique (marque à gagner, investissement pour se maintenir ou s’adapter...) et sur le plan technologique, à travers la description des solutions d’adaptations qui pourraient être mises en œuvre, en tenant compte de leur acceptabilité sociale (caractère intrusif ou répétitif) et de leur ergonomie (facilité d’usage).

En outre, vous pourriez notamment éclairer le gouvernement sur :

- le risque de renforcement de la position dominante des acteurs dominants (Facebook, Google) sur le marché de la publicité ciblée;
- les alternatives techniques (ex. extension URL) dont disposent les acteurs pour procéder à de la publicité ciblée sans recours à des cookies tiers ;
- l’opportunité d’imposer des obligations différenciées suivant la finalité des cookies ; à cette fin, le « filtrage » effectué par les navigateurs des cookies selon leur finalité vous paraît-il souhaitable et possible ? ;
- l’intérêt d’une promotion voire d’une généralisation sur le territoire de l’Union de la fonctionnalité « Do Not Track » du protocole HTTP afin de permettre de recueillir le consentement de l’utilisateur, non pas de manière binaire (« pour » ou « contre » les traceurs) mais granulaire (site par site) ;
- l’identification de mesures techniques alternatives à celles proposées par la Commission européenne, permettant de concilier le respect de la vie privée des internautes et l’intérêt économique des acteurs en ligne.

Compte-tenu du calendrier de la négociation, vous travaillerez en étroite liaison avec les directions de l’administration chargées de l’élaboration des positions françaises, en particulier avec la direction générale des entreprises et le SGAE. Nous vous saurons gré de nous remettre vos principales conclusions d’ici deux mois. Selon ces conclusions, vos travaux pourront faire l’objet d’un rapport publié en français et en anglais.

Nous vous prions d'agréer, Monsieur le Vice-président, l'expression de notre considération distinguée.

Bruno LE MAIRE  Moufdir MAHJOUBI  Françoise NYSSSEN
Annexe 2 : Liste des personnes rencontrées ou interrogées

Organismes publics et parapublics

Ministère de la Justice
- Mme Aurélia Schaff, conseillère chargée de l'Europe et des relations internationales
- Mme Pauline Dubarry, bureau de la négociation pénale européenne et internationale, cheffe de bureau
- M. Corentin Hellendorff, direction des affaires civiles et du sceau, rédacteur expert

Secrétariat d'État auprès du Premier ministre, chargé du Numérique
- M. Côme Berbain, Conseiller auprès du secrétaire d’Etat

Secrétariat général aux affaires européennes
- M. Francesco Gaeta, secrétaire général adjoint
- Mme Christine Cabuzel-Duvallon, secteur numérique politique industrielle (ITEC), ajointe au chef de secteur
- M. Loic Agnès, chef du secteur ITEC

Direction générale des médias et des industries culturelles
- Mme Elizabeth Le Hot, sous-direction du développement de l'économie culturelle, sous-directrice
- Mme Victoire Citroën, bureau des affaires européennes internationales, cheffe de bureau
- Mme Laura Desille, bureau des affaires européennes internationales, chargée de mission
- Mme Joanna Chansel
- Mme Sophie Bouquet, secrétariat général, service des affaires juridiques et internationales, chargée de mission

Direction générale des entreprises
- M. Olivier Corolleur, sous-direction des communications électroniques et des postes, sous-directeur
- M. Jean-Pierre Labe, bureau de la réglementation des communications électroniques, chef de bureau
- Mme Mélanie Przyrowski, bureau de la réglementation des communications électroniques, chargée de mission

Direction générale de la concurrence, de la consommation et de la répression des fraudes
- Mme Joanna Ghorayeb, sous-direction des affaires juridiques, des politiques de la concurrence et de la consommation, sous-directrice
- M. Philippe Guillermin, bureau Politique de protection des consommateurs et loyauté, chef de bureau
- M. Hugo Bruel, bureau Politique de protection des consommateurs et loyauté, adjoint au chef de bureau

Autorité de régulation des communications électroniques et des postes (ARCEP)
- M. Zacharia Alahyane, Direction « Internet et Utilisateurs », directeur
- M. Olivier Delclos, Direction « Internet et Utilisateurs », unité opérateurs et obligations légales, chef d’unité
- Mme Jennifer Siroteau, Direction « Economie, marchés et numérique », unité analyse économique et intelligence numérique, cheffe d’unité
- M. Vincent Toubiana, Direction « Economie, marchés et numérique », unité analyse économique et intelligence numérique, chargé de mission
- Mme Annabel Gandar, Direction « Affaires juridiques », unité Infrastructures et réseaux ouverts, chargée de mission
- Mme Clara Hanot, Direction « Europe et international », unité Europe, chargée de mission

**Commission Nationale de l’informatique et des libertés (CNIL)**
- M. Jean Lessi, secrétaire général
- Mme Clémence Scottez, service du secteur économique, chef de service
- M. Brice Bastié, service des affaires économiques, juriste
- M. Heslot, service de l’expertise technologique, ingénieur

**Conseil National du Numérique (CNN)**
- M. Rand Hindi, membre du CNN, fondateur de Snips
- M. Charly Berthet, responsable juridique et des relations institutionnelles

**Organisation professionnelles**

**Fédération e-commerce et vente à distance (fevad)**
- M. Marc Lolivier, délégué général

**Fédération nationale de la presse spécialisée (FNPS)**
- M. Laurent Bérard-Quelin, président
- Mme Catherine Chagniot, directrice déléguée
- Mme Aurélie Petit, responsable juridique et économique

**France digitale**
- M Nicolas Brienne, directeur général

**Groupement des éditeurs de contenus et de services en ligne (Geste)**
- Mme Corinne Denis, Directrice du Numérique et du Développement des revenus, Lagardère Active, et Vice-Présidente du GESTE
- M. Emmanuel Parody, Associé et Directeur des rédactions, Mind Media, et Secrétaire Général du GESTE
- Maître Etienne Drouard, Président de la Commission Enjeux Réglementaires du GESTE
- M. Amélien Delahaie, Juriste au GESTE
- Mme Louise Durand, Responsable des Affaires Juridiques et Réglementaires du GESTE

**Syndicat de la presse indépendante d'information en ligne (SPIIL)**
- Mme Karen Autret, directrice
- M. David Legrand, membre du bureau

**Syndicat de la presse quotidienne nationale (SPQN)**
CGE taskforce on the proposed ePrivacy Regulation

- M. Denis Bouchez, directeur
- M. Samir Ouachtati, responsable des affaires juridiques et sociales
- Mme Béatrice Lhopitallier, Groupe Les Echos, directrice data
- M. Samuel Profumo, lefigaro.fr, directeur data & CRM

Syndicat des régies internet (SRI)
- Mme Hélène Chartier, directrice générale

Tech’in France
- M. Loïc Rivière, délégué général
- Mme Alice Garza, chargée de mission affaires publiques

Union des annonceurs (UDA)
- M. Jean-Luc Chetrit, directeur général
- Mme Laureline Frossard, responsable juridique
- Mme Laura Boulet, directrice affaires publiques, juridiques & éthiques

Union des entreprises de conseil et achat média (UDECAM)
- Mme Françoise Chambre, déléguée générale

Union de la presse en région (UPREG)
- Mme Maud Grillard, directrice
- M. Bruno Ricard, traitement des questions publicitaires

Association

La Quadrature du Net
- M. Arthur Messaud, juriste

Entreprises

Criteo
- M. Guillaume Marcerou, senior counsel Global Privacy Product
- M. François Costa de Beauregard, directeur général adjoint France

Google
- Rita Balogh, Public Policy and Government Relations Manager, Bruxelles
- M. Olivier Esper, directeur des relations institutionnelles
- M. Thibault Guiray, affaires publiques et relations institutionnelles
- Lanah Kammourieh Donnelly, Public Policy and Government Relations Manager, Londres

Lysios
- M. Jean-Luc Archambault, président

Next Radio TV
- Mme Stéphanie Corbière, responsable juridique groupe
Orange
- M. Pierre Petillault, directeur adjoint des affaires publiques
- Mme Sophie Poncin, Orange advertising, directrice régie
- Mme Luisa Rossi, direction de la réglementation
- Anne Derouin, Responsable du Département Publicité, Services, Portails web et mobile

Qwant
- M. Léonard Cox, vice-président Affaires Publiques et RSE
- M. Guillaume Champeau, directeur Ethique et Relations Publiques

SFR
- Mme Marie-Georges Boulay, directrice des affaires réglementaires, concurrence, contrats opérateurs et fréquences
- M. Marc Jossermoz, directeur business development big data
- Mme Estelle Chevalier, responsable affaires européennes

S4M
- M. Nicolas Rieul, vice-président stratégie EMEA et administrateur responsable de l’international de la Mobile Marketing Association France

TF1
- M. Antony Level, directeur des affaires réglementaires numériques groupe
- M. Pierre Renaldo, expert data
- M. Ribadeau-Dumas, directeur-adjoint marketing digital

Groupe Vivendi
- Mme Chantal Andriotti, Canal+, responsable juridique Concurrence, Marketing de l’Offre, Données personnelles, NTIC
- M. Clément Reix, Dailymotion, directeur de projet « Affaires Publiques »
- M. Christophe Roy, Canal+, directeur des affaires européennes
- Mme Marie Sellier, Vivendi, directrice des Affaires Publiques
- M. Arnaud Schmite, havas media, secrétaire général

Wavestone
- M. Gabriel Amirault, senior consultant
- Mme Mathilde Bouget, stagiaire de Toulouse Business School

Personnes qualifiées
- M. Claude Castellucia, INRIA, directeur de recherche
- Mme Maryline Laurent, professeur, Telecom SudParis
- M. Daniel le Metayer, INRIA, directeur de recherche
- M. Patrick Waelbroeck, professeur, Telecom ParisTech

Cap Digital a organisé pour la mission le 8 novembre une discussion-débat sur le projet de règlement e-privacy, à laquelle a pris part une trentaine de membres du pôle de compétitivité.
Annex 3: the operation of programmatic advertising

For a targeted advertising campaign, the advertiser seeks to define a group of people who may be interested in a product or service. The analysis is essentially probabilistic: it is about predicting a score of interest for the product or service, from people who may belong to certain segments of different categories of data: sociodemographic segmentation (gender, ages, with or without children, socio-demographic profiles), segmentation of intentions to buy a good or service (inferred from a browsing history), segmentation of interests or hobbies, possession of certain types of products, ... There is therefore a definition of the target (the profile of Internet users likely to be interested) and then, when a user calls a page, a calculation to match or not this user to that target, based on the data available on his own profile.

The advertiser relies on an agency or an internal marketing team, which will use a terminal linked to a DSP (demand side platform) to buy spaces on pages (impressions) called by Internet users who match the targeted profile. These ads spaces are marketed by SSP (supply side platforms) via Ad exchanges. This sale circuit of the spaces is completed by a data sales circuit (data first party, second party or third party), and by a circuit which allows to serve ads (adservers).

In the case of re-targeting, it is the interest expressed by the Internet user for a product or service that leads to propose it to him again during a subsequent browsing.

The methods that lead to offering advertising to an Internet user are similar to those used to make a recommendation: the data collected on an Internet user can be used to calculate matches from other recorded transaction data. In many tests, these methods have proved to be more efficient than contextual analysis methods (prediction of the interests of the Internet user based on what he/she is doing).

For Internet users, the steps are as follows:

1. The Internet user accesses a web page. A query is generated to serve an ad that will appear on this page. This request is processed with data about the user. These data may be known from the site, or have been compiled by a data management platform on the basis of cookies (data 3rd party).
2. The request is addressed to the ad server of the website, which serves in priority the displays corresponding to direct sales (presales), corresponding to contracts entered into by the publisher (or its advertising agency) with advertisers (or their agencies).
3. If there are no presales, or if they pass through the "programmatic" channel, the request is transmitted to an ad exchange via an SSP. This ad exchange communicates with many servers (DSP) that may be interested in buying the ad space. The ad exchange can:
   a. Place ads on pre-sold spaces, called "premium" when it uses to the best advertising space, such as home pages. For the advertiser, the advantage of going through the ad exchange for direct contracts is to automate his purchase campaign.
   b. Serve as a private market place (only certain buyers selected by the publisher participate in the sale).
   c. Serve as an open market place (Real Time Bidding, RTB). Any DSP connected to the platform can participate.

---

64 See, for example, the categories of data identified in the Eyeota H1 2017 Index Report
4. The ad space is sold after auction to third parties (case b. and c.). The auction is won (usually by the highest bidder, but for the price of the 2nd bid). Those who participate in auctions can use data accompanying the request, but also on their own database (e.g., for retargeting).

5. The ad is served to the user (impression).

The attractiveness of the programmatic channel lies in its technical efficiency and flexibility. Its limitations come from the difficulty, on the one hand, to control the quality of the data and, on the other hand, to measure the visibility of the advertisement (partial or complete display time, machine-generated displays, sometimes fraudulent). In addition, the buyer does not know on which site he buys ad space, he can only set up lists of sites, white or black. From his side, in RTB, the publisher can only set a minimum floor price and define a list of undesirable advertisers. Direct purchases or private sales are reputed to offer a better guarantee of visibility than RTB. Within the programmatic channels, the share taken by direct or private sales, which have been growing since 2010, is therefore linked to advertisers' desire to buy quality spaces and control better the visibility of ads.
**Annex 4: text of articles 8,9 et 10**

**Text proposed by the Commission**

Protection of information stored in and related to *end-users’* terminal equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users’ terminal equipment, including about its software and hardware, other than by the *end-user* concerned shall be prohibited, except on the following grounds:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the *end-user* has given his or her consent; or

(c) it is necessary for providing an information society service requested by the *end-user*; or

**Amendment by the European parliament**

Protection of information transmitted to, stored in and related to *processed by and collected from users’* terminal equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from *end-users’* terminal equipment, including about its software and hardware, other than by the *user* concerned shall be prohibited, except on the following grounds:

(a) it is *strictly* necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the *user* has given his or her *specific* consent; or

(c) it is *strictly technically* necessary for providing an information society service specifically requested by the *user*; or
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.

(d) if it is technically necessary for measuring the reach of an information society service requested by the user, provided that such measurement is carried out by the provider, or on behalf of the provider, or by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or

(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:

(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;

(ii) the user is informed in advance each time an update is being installed; and

(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;

(d b) in the context of employment relationships, it is strictly technically necessary for the execution of an employee’s task, where:

(i) the employer provides and/or is the user of the terminal equipment;

(ii) the employee is the user of the terminal equipment; and

(iii) it is not further used for monitoring the employee.

1a. No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal
2. The **collection** of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

2a. For the purpose of points (d) of paragraph 1 and (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:

(b) the processing shall be limited in time and space to the extent strictly necessary for this purpose; and

(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and

(d) the users shall be given effective possibilities to object that do not affect the functionality of the terminal equipment.

2b. The information referred to in points (aa) and (ab) of paragraph 2 shall be conveyed in a clear and prominent notice setting out, at the least, details of how the information will be collected, the purpose of
Article 9

1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.

2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.

3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

3 a. Any processing based on consent must not adversely affect the rights and processing, the person responsible for it and other information required under Article 13 of Regulation (EU) 2016/679, where personal data are collected. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679.

3. The information to be provided pursuant to paragraph 2b may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.
freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and the protection of personal data.

Article 10

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall:

(a) by default, have privacy protective settings activated to prevent other parties from transmitting to or storing information on the terminal equipment of a user and from processing information already stored on or collected from that equipment, except for the purposes laid down by Article 8(1), points (a) and (c);

(b) upon installation, inform and offer the user the possibility to change or confirm the privacy settings options defined in point (a) by requiring the user's consent to a setting and offer the option to prevent other parties from processing information transmitted to, already stored on or collected from the terminal equipment for the purposes laid down by Article 8(1) points (a), (c), (d) and (da);

(c) offer the user the possibility to express specific consent through the settings after the installation of the software.

Before the first use of the software, the software shall inform the user about the privacy settings and the available granular setting options according to the information society service accessed. These settings shall be easily accessible during the use of the software and presented in a manner that gives the user the possibility for making an informed decision.

1a. For the purpose of:

(a) points (a) and (b) of paragraph 1,

(b) giving or withdrawing consent pursuant to Article 9(2) of this Regulation, and

(c) objecting to the processing of personal data pursuant to Article 21(5) of Regulation
(EU) 2017/679,

the settings shall lead to a signal based on technical specifications which is sent to the other parties to inform them about the user’s intentions with regard to consent or objection. This signal shall be legally valid and be binding on, and enforceable against, any other party.

1b. In accordance with Article 9 paragraph 2, such software shall ensure that a specific information society service may allow the user to express specific consent. A specific consent given by a user pursuant to point (b) of Article 8(1) shall prevail over the existing privacy settings for that particular information society service. Without prejudice to paragraph 1, where a specified technology has been authorised by the data protection board for the purposes of point (b) of Article 8(1), consent may be expressed or withdrawn at any time both from within the terminal equipment and by using procedures provided by the specific information society service.

deleted

2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.

3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.

3. In the case of software which has already been installed on [xx.xx.xxxx], the requirements under paragraphs 1, 1a and 1b shall be complied with at the time of the first update of the software, but no later than six months after [the date of entry into force of this Regulation].