WIK • Report

Study for the Bundesministerium für Wirtschaft und Energie

Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Models

Authors:
Christian Hildebrandt
Dr René Arnold

WIK Wissenschaftliches Institut für Infrastruktur
und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany

Bad Honnef, November 2017
Translation to English in December 2017

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Imprint

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
Email: info(at)wik.org
www.wik.org

Persons authorised to sign on behalf of the organisation

General Manager and Director	Dr Iris Henseler-Unger
Director Head of Department Postal Services and Logistics	Alex Kalevi Dieke
Director Head of Department Networks and Costs	Dr Thomas Plückebaum
Head of Administration	Karl-Hubert Strüver
Chairman of the Supervisory Board	Winfried Ulmen
Registered at	Amtsgericht Siegburg, HRB 7225
Tax No.	222/5751/0722
VAT ID	DE 123 383 795

Executive Summary

The results of this study show that the ePrivacy Regulation is likely to jeopardise large parts of the online advertising industry and ad-based digital business models. Specifically, six questions are addressed in the study:

Question 1: What would the ePrivacy Regulation mean for specific business models if the European Commission's estimate is correct that around 11% of users agree to accept cookies?

In Germany, the **total digital advertising budget is expected to reduce by about one-third** in the short term. Display and affiliate advertising will primarily be affected. The short-term effect on search engine advertising (in Germany mainly Google) and advertising on social networks (in Germany mainly Facebook) is likely to be relatively small. Structurally similar effects are expected to occur in other European countries.

The consequences of this short-term withdrawal of capital will initially accelerate **the decoupling of the European online advertising market from the growth of the US market**, which has been ongoing since 2014. In the US, the money from online advertising is increasingly being invested in the development of new business models and technologies such as autonomous driving and artificial intelligence. With the ePrivacy Regulation, Europe is ultimately at risk of being excluded from crucial innovations that are relevant for the future of the digital economy.

In the medium to long term, it is anticipated that advertising budgets will migrate to closed log-in systems (where the user experience is largely unaffected by the ePrivacy Regulation) and these systems are expected to win over an even greater proportion of the time users spend online. If this happens, it is likely that even high-quality content will follow the eyeballs and the advertising budgets to large online platforms. In particular, online log-in based platforms that already have a large number of users will likely benefit from such a development. Ultimately, the ePrivacy Regulation can provide the impetus for a European internet characterised by log-in and paywall-restricted online services.

Question 2: Is the assessment by the European Commission correct that only 11% of users will accept cookies? Is there an alternative estimate?

A clear statement about future consumer behaviour is not as easy to deduce as that done by the European Commission with its survey-based impact assessment. Too many details of the actual implementation are still unclear. Privacy-by-Design/Default configured operating systems, web browsers and apps presume that consumers have the necessary technical understanding to assess which function has what purpose and which setting is required to enable this, for example the specific configuration required to enjoy a particular online video. In addition, the consumer must be able to (intuitively) understand which services or applications are fully or partially blocked (by default) due

to the software design or the default configuration and how this can be easily changed manually without allowing an unnecessary flow of information. **It is doubtful whether these propositions by the European Commission are correct, because it cannot be assumed that consumers will engage in such complex technical and organisational measures before using the internet.** Thus, the outlined implementation ultimately **does not create any new transparency for consumers**. Instead, many consumers will be overwhelmed by the need to make fundamental choices. As a result, consumers will likely sway towards opting to block cookies without being aware of the consequences for their user experience. In essence, this can be seen as a **barrier for the transmission of cookie-based targeted advertising based on the ePrivacy Regulation.** As a consequence of poor user experience, consumers may switch to services that (for whatever reason) can still deliver the usual level of ease of use.

Question 3: Can we expect different user behaviour depending on the business model of specific services?

It is possible that, after the ePrivacy Regulation has come into force, user behaviour may differ across business models. Due to the high degree of heterogeneity of both internet users and online services, it is currently not possible to make a reliable forecast in this respect. Decisions depend, among other things, on consumer confidence in a particular service, on the individual utility a specific service offers to the consumer, and on the possible alternatives of economic compensation.

Question 4: What is the revenue loss that may occur if the transmission of targeted advertising is no longer possible in the future because only a few users give their consent?

An analysis by IAB Europe generally supports the results of this study, which expects **a short-term reduction in the advertising budget for online advertising in Germany of about one-third.** The IAB study outlines three specific scenarios that predict **a reduction in advertising budgets for display advertising by 2020 between 45% and 70%** as a combined effect of the General Data Protection Regulation (GDPR) and the ePrivacy Regulation. Since the vast majority of current display advertising is programmatic advertising, this estimate seems rather conservative.

Question 5: Can revenue losses be compensated for by other forms of non-targeted advertising or payment models and if not, why not?

In principle, advertisers and media professionals in the digital economy have limited opportunities to compensate for revenue losses in other ways, as the internet economy traditionally has no alternative to the three options: (1) paying attention to advertising content; (2) collecting and using personal data; (3) payment models. Another reason is that internet users expect to enjoy the majority of online content free of charge, thereby habitually accepting advertisements as part of the online content.

There is no comparable system that allows such a granular allocation of funding as targeted online advertising. In most cases, the monetary sum that a content provider receives for a single visit or click amounts to a fraction of a euro cent. The cost of paying such sums through another payment system is prohibitive, in particular with transaction costs of implementation and the payment process that the consumer would have to go through on a regular basis.

Again, log-in systems are a possible solution. They allow billing and appropriate allocation of funds. However, a proliferation of log-in systems would ensure that the **ePrivacy Regulation misses its most central objective: a higher level of data protection**. Log-in systems provide much more direct access to personal data and effectively reduce data protection compared to today's level of protection and the prevailing open system of ad allocations using pseudonymised data.

Question 6: What proportion of online services may be discontinued due to revenue losses?

The expected loss of revenue can threaten the existence of service providers that are mainly financed by display advertising. This applies in particular to publishers and other (high-quality) content providers. The smaller providers who do not have a strong brand will likely suffer the most.

Focusing on the benefit of the individual citizens may entail the risk of collective public welfare losses in the digital economy and society. Overall, it is clear **that a balance of interests between consumers and the digital economy** is imperative. Furthermore, the present study shows that an effective ban on an entire class of technologies without a balanced examination of their effects runs the risk of causing substantial collateral damage.

Table of Contents

1 Introduction

The ePrivacy Directive for Electronic Communications (2002/58/EC) is a European Community Directive that was adopted in 2002, which sets binding minimum requirements for data protection in telecommunications for all Member States. In 2009, the so-called Cookie Directive (2009/136/EC), which requires the explicit consent of users of websites and apps to accept cookies, was added to the directive. Cookies produce a small text file in which a series of numbers is generated to identify, among other things, an internet-enabled device, operating system and the web browser or app. This enables advertisers and other service providers to follow users through the internet when they visit different websites (online tracking) and to use the generated information for advertising purposes.

Currently, there is an amendment that will transform the ePrivacy directive into a regulation on the protection of privacy and confidentiality in electronic communications. The aim of this process is to harmonise regulatory frameworks across the EU not only for telecommunications services but also for Over-The-Top (OTT) services. In addition, the new regulation should complement and ensure coherence with the European General Data Protection Regulation (GDPR) (EU) 2016/679, which will come into force in May 2018 but does not cover all areas of processing personal data. The European Commission's current proposal – COM (2017)10 final – aims for a uniform level of protection for telecommunications and internet services, irrespective of the device.

A public consultation took place from April to July 2016; the results were published in August 2016. As a result of this, the European Commission has opted for a regulation. In line with their Better Regulation Guidelines, they carried out an impact assessment. On 13 December 2016, a first draft of the regulation was leaked. The official (updated) draft was presented by the European Commission on 10 January 2017. It is intended that the ePrivacy Regulation will come into effect at the same time as the GDPR on 25 May 2018.[1]

The current draft (COM (2017) 10 final) is classified as a threat by actors within the digital economy, as well as by those working in the advertising industry, and contains many concerning elements. The aim of this study is to address problematic areas and related aspects of the draft and to provide a critical opinion on the future of online advertising and ad-based digital business models in Germany.

The study is structured as follows. A brief summary of the public stakeholder consultation and the impact assessment by the European Commission is given in section 2, before the current discussion on the ePrivacy Regulation with the key findings of the interviews with various stakeholders is documented in section 3. Section 4 addresses key issues of the draft regulation from a scientific point of view, and section 5 gives details on the possible implications for online advertising and digital business models. The study concludes with a summary and outlook in section 6.

1 It is currently expected that this will not happen. Negotiations are likely to continue until summer 2018.

2 Analysis of the public consultation and impact assessment by the European Commission

In line with their Better Regulation Guidelines, the European Commission has established a standardised process with a view to amending directives and regulations. This includes a public consultation, impact assessment and a trialogue procedure with the European Council and the European Parliament to finalise a set of rules. In the period from April to July 2016, a public consultation was held by the European Commission, the results of which were published on 4 August 2016. The stakeholders who were involved in the survey can be divided into three groups:

1. Citizens and civil society watchdogs
2. Industrial companies and associations
3. Data protection and consumer protection organisations

1: Individual citizens and civil society watchdogs see themselves in an ambivalent relationship with the use of internet services and applications. They want to maintain the protection of their own privacy, but take comparatively few (or no) measures to increase privacy and confidentiality in electronic communications (privacy paradox).[2] On the one hand, they feel unsettled by the massive expansion of various forms of online and offline tracking and feel that there is an implicit and creeping process of losing control; on the other hand, relatively few citizens are well informed about internet reality and are not in a position to use technical measures to increase their privacy protection. They call for extensive and comprehensive data protection for both telecommunication and internet services in order to safeguard their fundamental right to informational self-determination.

2: Industrial companies and associations see a development in which consumers have had little or no monetary willingness to pay for internet services since the commercialisation of the internet, with the result that new forms of non-monetary prices such as advertising (attention) and personal data have emerged endogenously on various digital markets. Therefore, they see ad-financed and data-based digital business models as legitimate and believe that all interventions in digital markets must be justified. They consider the protection of privacy and confidentiality in electronic communications to be worth protecting but they want balanced solutions that do not jeopardise other legitimate legal interests such as freedom of contracting or media diversity. This balance of economic and consumer interests is lacking in the current draft of the regulation. Industrial companies and associations also call for reasonable consideration of the complexity of the internet ecosystem in order to avoid losing traction in the global competitive arena by additional regulation.

2 For a detailed discussion see Arnold, R., M. Waldburger & A. Hillebrand. 2015. Personal Data and Privacy – WIK Study for Ofcom, Bad Honnef.

3: Data and consumer protection organisations consider the draft to be progressive and consider the principles of confidentiality of communications and enhanced privacy to be important enough to extend them to internet services and terminal equipment. They call for an end to all offline and online tracking activities unless the consumer has given his or her explicit consent. To achieve this, the consumer is to be empowered to comprehensively restore or secure his/her sovereignty with regard to personal and non-personal data through appropriate technical mechanisms.

All groups of participants considered the period for public consultation to be too short due to the breadth and depth of the issues. Many companies were not previously aware that they will soon be directly or indirectly assigned to the field of electronic communications, for example if they previously regarded themselves as food producers, car manufacturers or mechanical engineers.

The impact assessment of the envisaged ePrivacy Regulation was carried out after the public consultation by the European Commission and consists of the following elements: identification of the problems; reasons and objectives for an amendment; and assessment of five identified policy options based on the criteria of relevance, effectiveness, coherence, efficiency and added value for the EU. The following policy options were considered:

1. No legislative measures
2. Limited strengthening of privacy/confidentiality and simplification of the regulatory framework
3. Specific strengthening of privacy/confidentiality and simplification of the regulatory framework
4. Extensive strengthening of privacy/confidentiality and simplification of the regulatory framework
5. Removal of the ePrivacy Directive

The result of the analysis was to opt for option 3: instead of a directive, a regulation has been chosen that once passed will take immediate effect in all EU Member States. All in all, three goals are to be achieved:

- Protection of privacy and confidentiality in electronic communications
- Uniform level of data protection in Europe
- Promotion of the digital single market through the free flow of (non-) personal data, terminal equipment and services

The intention is to achieve harmonisation in the following five main fields: (1) security in electronic communication; (2) confidentiality of communications and traffic data; (3) confidentiality of information stored on terminal equipment; (4) protection of users' privacy; and (5) other legitimate interests of users.

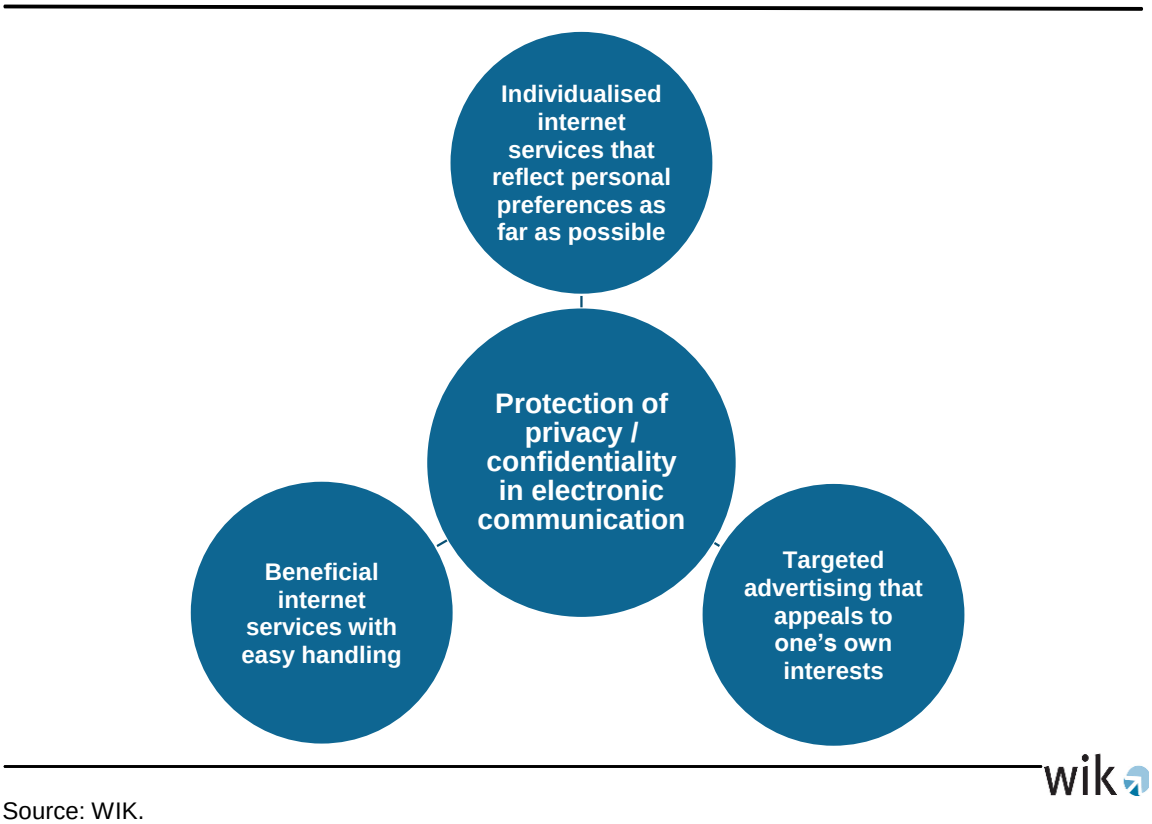
The approach taken in the impact assessment should be viewed critically, as from a scientific point of view, different effects must always be assessed and weighed up in order to achieve a valid decision based on an overall view of all essential aspects. For example, the impact assessment carried out by the European Commission has highlighted the advantages of technology neutrality, increased user control and transparency, the opt-in for marketing measures, and simplification through harmonisation and clarification of the rules. However, it has neglected to explain the resulting disadvantages; for example, the interventions in established business models required by the regulations are only mentioned briefly and their possible economic and societal effects are not examined in sufficient detail.

The impact assessment carried out by the European Commission includes the following weaknesses:

- Very narrow data protection view; no trade-offs for consumers considered/requested
- Further effects on the economy not estimated (e.g. impact on competition, innovation and investment)
- Further effects of a technical nature not estimated (e.g. effects on the internet ecosystem)
- Consistency in the overall structure of European law not examined

Consideration should be given to numerous trade-offs for consumers (as shown in Figure 1) which could have been determined via an intelligent consumer survey with appropriate framing of the questions.

Figure 1: Trade-offs for consumers



Source: WIK.

When consumers are asked about the protection of privacy, they say it is important to them. They want internet services that generate benefits and are characterised by technical and intuitive handling; they also want internet services that reflect their own preferences as far as possible. Advertising measures should also match their interests in a way that suits them perfectly. Finally, it is also important to consumers that internet services are free of charge. In this context, a legitimate question about possible forms of economic compensation for internet services arises but is not addressed by the impact assessment.

Overall, the European Commission's impact assessment is inadequate. It should be noted that a more comprehensive investigation and impact assessment should have been done, especially because of the very far-reaching regulations and the associated interventions in established business models. In view of the self-imposed objectives of the envisaged ePrivacy Regulation, the impact assessment on data protection and the promotion of the "free flow of data" to achieve a digital single market remains vague. The impact assessment also does not investigate the chances of possible alternatives through self-regulatory approaches by the industry and co-regulation concepts. In this context, an agreement on necessary technical standards could in principle provide an opportunity to maintain a complex internet ecosystem that enables privacy and confidentiality in electronic communications while maintaining established digital business models.

3 Assessments by relevant stakeholders

3.1 The current status of the discussion on the ePrivacy Regulation

Currently, the European Parliament is preparing their position on the ePrivacy Regulation, and following this the European Council of Ministers will do the same. These positions are finally coordinated with the European Commission in the so-called trialogue procedure and formally confirmed by the EU Parliament and the EU Council of Ministers.

In the European Parliament, three committees have issued opinions on the ePrivacy draft regulation:

- Committee on Industry, Research and Energy with the rapporteur Kaja Kallas – Opinion of 4.10.2017
- Committee on Legal Affairs with the rapporteur Pavel Svoboda – Opinion of 5.10.2017
- Committee on the Internal Market and Consumer Protection with the rapporteur Eva Maydell – Opinion of 6.10.2017

The parliamentary committee, chaired by Marju Lauristin, the rapporteur, voted on 20 October 2017 on the LIBE report and voted by a narrow majority (31 to 24 votes, one abstention) in favour of its adoption. The compromise text, which consists of 827 amendments and has been pre-negotiated by various political groups in the European Parliament, advocates a one-year transitional period from the date of entry into force of the ePrivacy Regulation.

The high number of amendments clearly highlights just how controversial the discussion between advocates of data protection and representatives of the interests of the digital economy is.

Telecommunications regulation includes sector-specific data protection, which will also include internet services in the future.[3] With regard to confidentiality in electronic communications and the protection of privacy, this is generally considered appropriate by all representatives, provided that the implementation of the regulation is proportionate and reconciles different interests.

3 On a national level, this implies that the provisions of the Telecommunications Act (TKG) and the Telemedia Act (TMG), which are based on the previous ePrivacy directive, will be replaced by the new ePrivacy Regulation, as long as they cover the processing of personal data. In addition, the possibilities of addressing the law against unfair competition (especially section 7 UWG) by means of advertising measures (telephone, email, fax, SMS, etc.) are also suppressed by the new ordinance, as long as they include the processing of personal data.

For the digital economy, and especially for the online advertising industry, Articles 8, 9 and 10 (Protection of terminal equipment) of the ePrivacy Regulation present a threat. In some cases, Articles 6 and 7 (Confidentiality and Permissions) are viewed critically with regard to metadata regulations.

Article 8 deals with the protection of stored information on terminal equipment and the collection of data. It does not permit the processing of data on terminal equipment, unless this is necessary. Neither the ePrivacy Regulation nor Article 6 of the GDPR specify when data processing is “necessary”. Thus, the digital economy has considerable problems of interpretation and implementation. Article 10 (Privacy-by-Design/Default) concerns software but it is unclear which types of software fall under the regulation. Thus, in principle, any software that connects to the internet will have to enable a default option that prevents all (first- and third-party) cookies from using the device’s storage and processing capacity without explicit consent. For content providers and advertisers, this imposes noticeable limitations on their business models.

In connection with Article 9 of the ePrivacy Regulation, consent shall be granted in accordance with Articles 4 and 7 of the GDPR. However, it is questionable whether it is possible in the case of globally active internet companies for users to give informed and voluntary consent that meets the requirements of the fundamental right to informational self-determination. Article 7(1) of the GDPR stipulates that in the assessment of voluntariness, the coupling of consent to data processing that is not required and the conclusion of a contract must be taken into account (prohibition of coupling). This raises an economic question when it comes to the consumption of internet services and the possible forms of economic returns. A reconciliation of interests between industry and the consumer is therefore imperative.

3.2 Stakeholder interview results

3.2.1 Documentation and methodology

In addition to the secondary research conducted, interviews with relevant stakeholders are the main source of information for this WIK study. The main purpose of the interviews was to identify what impact the various stakeholder groups expected the ePrivacy Regulation to have on their respective business models. In order to gather this information, an interview guide was developed, the topics of which are presented below.

1. The EU Commission's ePrivacy Regulation concerns various services
   a. How do you generally assess the influence of the regulation on your business model?
   b. Do you share the European Commission's view that OTT providers who already work on a "consent basis" will not be substantially affected?
2. Enquiries about the individual services
   a. Browser
   b. OTT communication services
   c. Email services
   d. Online advertisement
3. Significant ways to implement tracking
   a. What is the current role of tracking technologies?
   b. Which of them will still be usable and which will not be usable under the regulation?
   c. Are there alternative ways to legally continue tracking customers?
   d. What consequences do you expect for your (business) customers?
4. Consequences of the ePrivacy Regulation
   a. How do you assess the impact of the regulation on the entire online advertising market in the EU and especially in Germany?
   b. Who will have (dis-) advantages?
   c. Is there a realistic threat to certain business models?
5. Impact assessment of the effects of the ePrivacy Regulation
   a. How do you assess the new position of web browser providers to protect privacy by default?
   b. What are the effects on apps?
6. Impact assessment of the European Commission

   In its impact assessment, the European Commission estimates savings of around EUR 950 million.

   a. What do you think of this figure?
   b. Has the European Commission duly considered all aspects?
7. Consumer perspective
   a. How do you expect consumers to react?
   b. Which setting options are consumers likely going to choose in their browsers (other software)?
   c. How can first- or third-party tracking technologies ask for consumers' consent? How can this be technically implemented? How do you expect consumers to react?
8. Transitional period until the entry into force of the ePrivacy Regulation
   a. How long will the entire transition take?
   b. What are the plans to convert "legacy systems"? Is that even possible?
9. Internet experience and usability
   a. How do you think the customer experience will change when the new web browser settings are implemented?
10. Achieving the objectives of the ePrivacy Regulation
    a. Do you think that the regulation will achieve its objectives?

The interviews were conducted as semi-structured interviews. This means that we developed an interview guide to ensure a balance of good comparability across the interviews while allowing for some variation for individual requirements of the interviewee/interviewer on each occasion. In concrete terms, we left enough room in the interviews to explore particularly interesting questions and answers in additional detail. Depending on the interviewee, certain topics were prioritised.

All interviews were conducted in October 2017 and relate to the state of discussion of the ePrivacy Regulation at that time. The interviews typically lasted 60 minutes. They were conducted by Dr René Arnold and Christian Hildebrandt. Some interviews were done in person but the majority were conducted over the phone.

Interviews were conducted with the following companies/institutions (in alphabetical order):

- AGOF (Working Group for Online Media Research)
- BITKOM (Federal Association for Information Technology, Telecommunications and New Media)
- BVDW (German Association of Digital Economy)
- CCIA (Computer & Communications Industry Association)
- Facebook
- Ferrero Group
- Google
- IVW (German Audit Bureau of Circulation)
- L'Oreal Group
- RTL Group
- The Nielsen Company
- Oath (Inc.)
- OMG-Mediaagenturen
- OWM (German Advertisers Association)
- ProSiebenSat1 Group
- Symantec
- VDZ (Association of German Magazine Publishers)
- VPRT (Association of Private Broadcasting and Telemedia)
- ZAW (The German Advertising Federation)
- ZEIT-Online

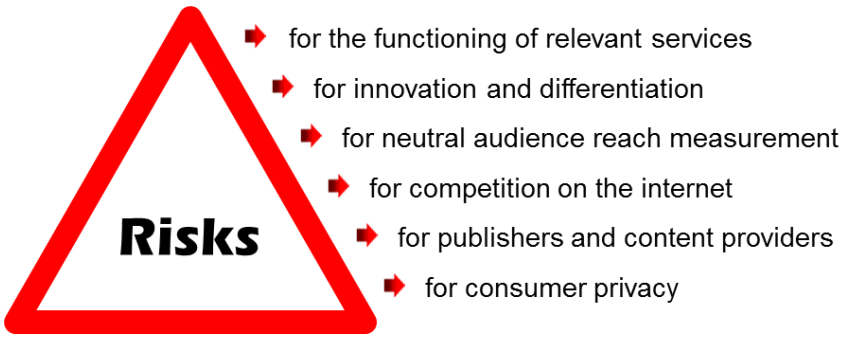
This meant that a broad spectrum of stakeholder assessments could be captured. These focused on the possible effects of Articles 8, 9 and 10 of the ePrivacy Regulation, in line with the selection of stakeholders. The following section summarises the main results of the stakeholder interviews.

3.2.2 Key results

Across all interviews, the interviewees consider the ePrivacy Regulation to be dangerous for their business model or at least for a large number of the services they offer in view of the current draft. Since the text of the regulation has not yet been finalised, we can only talk about risks perceived by the various stakeholders. However, these are considerable, as confirmed by all interview partners. The interview partners struggled to assess the concrete financial risks.[4] It is certain though that all stakeholders in the online advertising value chain expect significant losses, changes and uncertainties due to the ePrivacy Regulation, all of which will be looked at in more detail in this section.

The following sections describe more specifically the expected impact should the ePrivacy Regulation enter into force in the form that is discussed at the moment. The following figure provides an initial overview of the losses, changes and uncertainties as mentioned by the interviewees.

Figure 2: Risks from interviewed stakeholders' perspectives



Source: WIK.

Stakeholders consider Article 8(1) and Article 10(1) of the ePrivacy Regulation an effective prohibition of measures necessary for targeting, service optimisation and audience reach measurement.[5] From the stakeholders' point of view, this not only calls into question the provision of numerous services on the internet, but also effectively

4 In section 5, potential economic impacts are assessed in more detail on the basis of interviews and secondary research.

5 Specifically, the wording in Article 8(1) prohibiting any access to the processor and storage capacity of the terminal device and any use of the information on the terminal device makes it impossible to use cookies and other technical solutions to identify the terminal device, the software used, the online behaviour, etc. In particular, the wording prohibits the use of cookies and other technical solutions. The wording of Article 10(1) stipulates that any software must have a default setting which allows the user to prevent any exchange of information with third parties. While other gradations of the privacy preferences are not defined in more detail (they are only roughly outlined in recital 23), it is determined that the user should be asked to select a certain default setting when installing or updating the software. It is assumed that the vast majority of users will exclude all third parties.

threatens online advertising in Europe as such and in turn advertising-financed business models and the business success of advertisers. In particular, it is noted that there is no passage in the regulation covering the legitimate use of cookies and other measures that can ensure at least the basic functioning of advertising-financed services, but also of numerous non-ad-based websites.[6] Depending on how Article 8(1)(c) is construed, it is possible that even simple applications such as email services, online shopping or cloud services are affected. In addition, the regulation questions whether it is still possible to ensure that content, including advertising, can be played out correctly. This includes, for instance, the correct reaction to filters that protect children from potentially hazardous or inappropriate content. Identifying fake clicks,[7] malware and other IT security applications also requires access to processor and storage capacity. This would no longer be possible under the regulation, or only with major restrictions.

Regardless of whether and how a distinction can be made between actually necessary usage of the device's storage and processing capacity, all interviewees note that it is precisely the "unnecessary" interactions with one's devices that make it possible to offer (innovative) individual services with added value. Accordingly, the regulation would remove the main differentiation instrument for market participants by preventing the introduction of such differentiation possibilities within an already used service by creating new barriers such as requiring additional user consent. This was seen as hostile to innovation and thus a threat to the competitiveness of European market participants. In addition, European consumers may also be prevented from accessing innovative online services or functions, because global software and hardware suppliers may introduce certain functions in Europe later or not at all.[8] This may result in a loss of consumer surplus.[9] Furthermore, the postponed or non-implementation of innovative services may also indirectly harm the European economy and consumers, as relevant platforms may not be available or only with limited functionality.[10]

---

6 In Article 8(1), a number of exceptions are defined which legitimise measures under section c which are "necessary for providing an information society service requested by the end user". However, it is left open which measures are to be considered "necessary" in each case.

7 For example by so-called click farms.

8 Certainly, the European market is important for numerous global players due to the high average income compared to many other regions of the world. However, it should be remembered that, for example, around 100 million new internet connections were added in India alone between the first quarter of 2016 and the first quarter of 2017 (TRAI 2016 and 2017). This corresponds to about a quarter of the approximately 434 million internet users in the EU28 (Internet World Stats 2017). According to the same source, more Indians than Europeans already use the internet (462 million).See Telecom Regulatory Authority of India. 2016. The Indian Telecom Services Performance Indicator Report for the Quarter ending March 2016. New Delhi. and Telecom Regulatory Authority of India. 2017. The Indian Telecom Services Performance Indicator - January - March, 2017. New Delhi, India. and http://www.internetworldstats.com/

9 Arnold, R., C. Hildebrandt, P. Kroon, & S. Tas. 2017. "The Economic and Societal Value of Rich Interaction Applications." Study for the Computer & Communications Industry Association; McKinsey. 2010. "Consumers Driving the Digital Uptake: The Economic Value of Online-Advertising-based Services for Consumers." Study for IAB Europe.

10 Arnold, R. & C. Hildebrandt. 2017. "The Socio-Economic Impact of Online Platforms." WIK Study, June 2017, Bad Honnef.

Although the regulation does not explicitly mandate preferential treatment of first-party service providers, it transpires from the wording of the recitals (cf. 14, 15, 17, 18, 20, 21, 22) that a distinction is made implicitly between first-party and third-party service providers, where third-party cookies are judged to be significantly more harmful than first-party cookies. This is also described in Article 8(1)(d), which states that audience reach measurements are only exempt from the prohibition if they are carried out directly by the provider of the information society service. The stakeholders interviewed criticise this implicit and explicit preference for several reasons.

First, they note that the restriction in Article 8(1)(d) simply does not do justice to the reality of audience reach measurement. Today, this is typically carried out by third-party providers who can accumulate the necessary skills on the one hand and can ensure a (neutral) comparison of the data on the other. Audience reach measurement by an individual provider of an information society service is effectively worthless, since it does not allow for comparability and thus no neutral assessment of the advertising effectiveness for advertisers.

Considerably more serious are the possible effects of the implicit preferred treatment of first-party providers within the regulation on the competitive situation in the online advertising market.[11] Many interviewees noted that in particular this distinction favours those providers who already rely mainly on log-in systems and thus have significantly more direct access to consumers than providers who operate without or only optionally with log-in systems.[12] In concrete terms, numerous stakeholders fear a clear preference for large US companies such as Google, Facebook, Apple, Amazon or Microsoft.

In addition to better access to consumers and the associated high probability of consent, the numerous stakeholders' assessments are based on the provisions in Article 10, which reinforce the gatekeeper position of the web browsers,[13] whose settings determine access to the processor and storage capacities of the mobile device.

The stakeholders interviewed agree that globally active companies are better able to cope with the effects of the regulation than national suppliers or those that concentrate on the European market. Global companies can better absorb the potential loss of sales in Europe. They can also continue to use data from other regions of the world to optimise their services and innovate. This would especially harm small and medium-

11 It should be noted that this statement is not to be interpreted as meaning that first-party providers are not affected by the regulation.

12 It should be noted that log-in systems are necessary in essential areas and fall within the category of learned consumer behaviour. These include social networks where it is necessary to ensure a clear assignment to a profile. The same applies to numerous other online services such as games, marketplaces, messenger services, cloud applications, sharing economy applications or email services. Essential online services such as search engines or e-commerce providers often offer optional log-in systems to provide users with an optimised service. Numerous and especially information-related services such as newspapers, video platforms or comparison portals offer their services mostly without (or only with optional) log-in.

13 The provisions in Article 10 include any access software. However, the example of the browser is repeatedly cited as an essential one both in the recitals and in the interviews. Therefore, the explanations here follow this logic in the form of an illustrative example.

sized enterprises in Europe. It is expected that many of these companies will no longer be able to operate profitably if the regulation enters into force as discussed here. This applies in particular to providers who monetise journalistic or other particularly high-quality and thus expensive content. Stakeholders agree that this will hit publishers and other media particularly hard.

With regard to possible effects on competition and the financing of content through advertising, the stakeholders interviewed also see a significant influence of Article 8. Restricting access to the processor and storage capacity of any terminal equipment connected to the internet can substantially change market conditions. First of all, stakeholders note that targeting serves many positive purposes. This includes the technically correct presentation of content and advertising, for example the differentiation between mobile and stationary devices, the screen resolution and the (probably) preferred language.[14] For example, cookies ensure that the same advertisement is not shown too often on the same device (frequency capping). If this and comparable technical control options are no longer available, it can be assumed that online advertising outside of closed systems and search advertising[15] will lose much of its effectiveness and attractiveness for advertisers. Some stakeholders therefore expect a shift in advertising budgets to log-in systems and search engine advertising. Such a shift would give major online platforms an additional competitive advantage in Europe.

Furthermore, virtually all stakeholders regard so-called Online Behavioural Advertising (OBA) as indispensable. Contextual or semantic targeting cannot offer the same effectiveness. The elimination of OBA is therefore expected to result in a price decline for online advertising and at the same time in a noticeable increase in the number of online advertisements as the effectiveness of the individual ad decreases. This would not be in the interest of advertisers, content providers or consumers.

The stakeholders interviewed also question whether the regulation, as drafted, can actually improve consumers' level of privacy protection and whether this will be the case with regard to the GDPR. Should the regulation actually result in a proliferation of log-in systems, the connection between the data a service receives through interaction with a user and an individual consumer could be established directly. The segmentation of consumers typically used today with completely pseudonymised data and the playout of OBA based on segments is specific to target groups and not individually linked to a single consumer.

The stakeholders interviewed, who themselves offer a service on the internet, also point out that there is already competition between the various web browsers and additional software for the best protection of consumers' privacy. In this respect, the question

14 Based on the settings of the mobile device.
15 See Google AdWords, AdSense, Bing Ads, Yahoo!, Gemini and ad.net.

arises as to whether intervention in the market at this point is necessary at all and if so whether the possible collateral effects described above are proportionate.

All stakeholders interviewed clearly deny that the regulation can achieve its intended objectives. Obvious conflicts with the GDPR, the “Free Flow of Data” Regulation[16] and the Digital Single Market are also mentioned here, in addition to the likely worse position of the consumer.

The following section reflects on these core results on the basis of accessible secondary data and relevant literature. First, there is a general assessment as to which essential areas of the internet can be affected by the regulation and in which form. Secondly, the following section focuses on the importance of online advertising and digital ad-based business models.

16 COM(2017) 495 final

4 What is at stake?

The internet is a network of networks and integrates an ecosystem of providers of services, content and applications as well as different user groups. The evolution of the internet has been observable for decades and is a continuing success story due to a protocol-based technology (TCP/IP).[17] The resulting decentralised ecosystem, which generates much economic, technical and societal added value, is essentially based on an unchanged end-to-end network architecture.[18]

Data protection versus data economy

Users currently have access to a virtually open internet in which they can consume all kinds of content, services and applications at any time. When such information services are provided by commercial enterprises, the refinancing of these services often takes place through advertising. The users' acceptance of the advertising content is usually in exchange for the processing of their data. Users then pay for private-sector offers on the internet by looking at advertising content or by giving access to their data (e.g. by accepting general terms and conditions and data protection declarations).[19] As Figure 3 shows, a further differentiation of all actors reveals a highly complex and interdependent system of today's globally active data economy.

It is expected that the ePrivacy Regulation will change the effects of user behaviour in such a way that this complex ecosystem will no longer be able to function as before. The consequence could be a fragmentation of the internet through a multitude of closed log-in systems and payment-barrier solutions. When users are faced with the choice of either paying money for high-quality content and services on the internet or making themselves identifiable in log-in systems, the possibilities of extensive data collection at the individual level and data-based monetisation channels are created, where consumers ultimately achieve a lower degree of protection of privacy than before.[20]

17 Greenstein, S. 2015. How the Internet became Commercial: Innovation, Privatization, and the Birth of a New Network. New Jersey: Princeton University Press.

18 Van Schewick, B. 2010. Internet Architecture and Innovation: The Role of the End-to-End Arguments in the Original Internet. Cambridge: The MIT Press.

19 Hildebrandt, C. & R. Arnold. 2017. "Solving the Online Platform Puzzle." InterMedia 45 (1):23–26.

20 Goldfarb, A., & C. E. Tucker. 2012. "Shifts in Privacy Concerns." American Economic Review 102 (3):349–353; Farrell, J. 2012. "Can Privacy Be Just Another Good." Journal on Telecommunications & High Technology Law 10:251–265; Acquisti, A., C. R. Taylor, & L. Wagman. 2016. "The Economics of Privacy." Journal of Economic Literature 52 (2):442–492.

Figure 3: Overview of actors in the global data economy

Source: FirstMark Capital (2017) and Big Data Landscape (2017).

According to the current draft ePrivacy Regulation, the chosen web browser must allow the user to configure the privacy settings in a sufficiently transparent and simple manner (Privacy-by-Design/Default) so that it corresponds to the user's actual willingness if he or she agrees to the setting of third-party or tracking cookies.[21] In the context of big data and data-driven business models on the internet, consent cannot be regarded as a suitable means of protecting consumers' self-determination.[22] The guarantee of informational self-determination must therefore be structured differently in the context of digital markets. It should be noted that consent to processing of data cannot be considered separately from the requests for offers, as the use of internet services of any kind is associated with the processing of personal data. Informed consent requires the necessary information to be easily accessible, clear and understandable.

Data protection versus competition

A significant effect is to be seen in the split between first-party providers and third-party providers, which is intended by the ePrivacy Regulation.[23] The economic opportunities for participation in the competitive process are likely to shift in favour of a few large players (e.g. log-in-based online platforms) and to the detriment of many small players (e.g. online news providers) in the digital economy. As a result of the ePrivacy Regulation, third parties will hardly be able to collect user data due to the foreseeable lack of critical mass of consent and the new Privacy-by-Design/Default such that (high-quality) content providers will have the following three alternatives for commercial internet activity. They can

1. finance themselves directly via monetary payment systems (change of user habits required),
2. establish a first-party log-in system on their own (cost structures with high fixed costs and low variable costs are likely to exclude small and medium-sized companies), and
3. integrate into existing closed first-party log-in systems, within which performance measurement in the form of user data or user-group-specific advertising is still possible.

The shift towards first-party providers induced by the ePrivacy Regulation is preventing fair competition and diversity in the internet ecosystem. For example, mergers of start-ups with large internet companies already show a tendency for start-ups to sell their

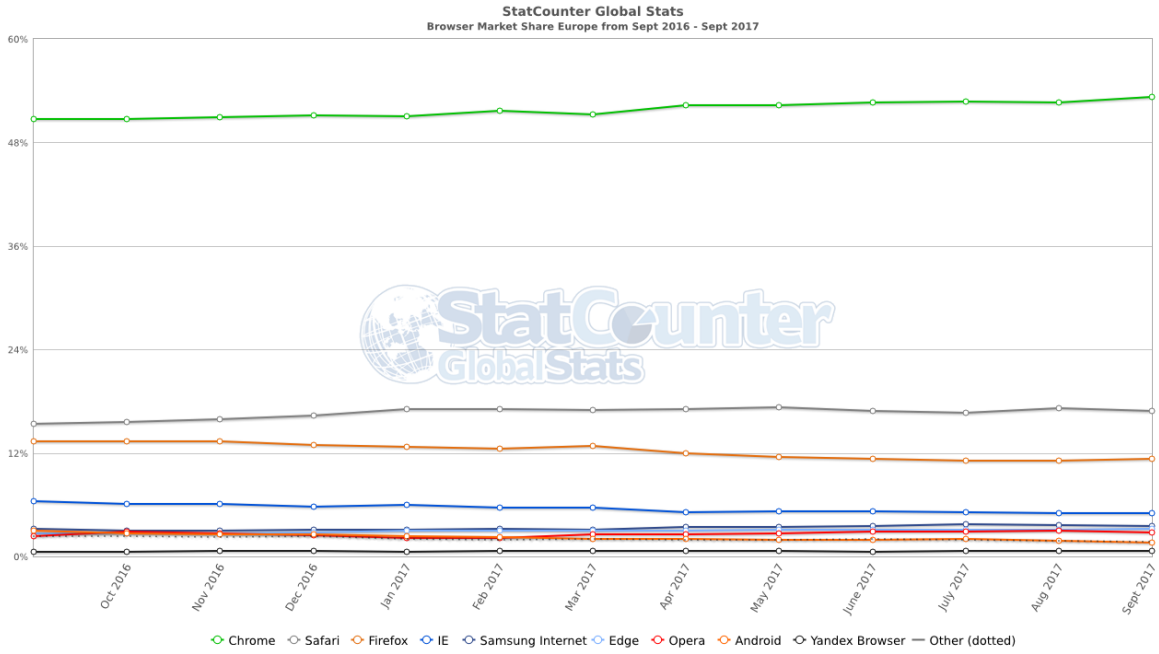
21 Zuiderveen Borgesius, F., J. Van Hoboken, R. Fahy, K. Irion, & M. Rozendaal. 2017. "An Assessment of the Commission's Proposal on Privacy and Electronic Communications" Study for the LIBE Committee of the European Parliament.

22 Hildebrandt, C. & R. Arnold (2016): Big Data und OTT-Geschäftsmodelle sowie daraus resultierende Wettbewerbsprobleme und Herausforderungen bei Datenschutz und Verbraucherschutz, WIK Diskussionsbeitrag Nr. 414, November 2016, Bad Honnef.

23 Engeler, M., & W. Felber. 2017. "Draft of the ePrivacy Regulation from the Perspective of the Regulatory Practice." Zeitschrift für Datenschutz 2017 (5):251–257; De Cornière, A. & R. De Nijs. 2016. "Online Advertising and Privacy." RAND Journal of Economics 47 (1): 48–72.

businesses to those players who offer the most comprehensive user data.[24] These actors are often online platforms, some of which show considerable tendencies towards concentration. The increased acquisition of innovative start-up companies by leading online platforms also risks reducing crucial innovation potential and competition in the digital market.[25]

Figure 4: Market for web browsers in Europe



Source: http://www.gs.statcounter.com/browser-market-share/all/europe

The role assigned to web browsers, apps and operating systems by the envisaged ePrivacy Regulation to implement the requirements regarding Privacy-by-Default/Design does not seem to be effective.

On the supply side, third parties depend on the definitions and regulations of web browsers and operating systems. In Europe, the market for operating systems has been highly concentrated for years and the market for web browsers is also made up of four main providers: Chrome (Google), Safari (Apple), Firefox (Mozilla) and Internet Explorer (Microsoft). All leading offers come from US companies.

24 Lambrecht, A. 2017. "The Relationship between EU e-Privacy Provisions and Venture Capital Investments in the EU." Mimeo.

25 Stucke, M. E. & A. P. Grunes. 2016. Big Data and Competition Policy. New York: Oxford University Press.

On the demand side, this leading position would be further corroborated by a reduction in the multihoming of web browsers in Europe due to the need for individual data protection configurations. However, multihoming, a parallel use of web browsers, would have a negative effect on the concentration tendencies of web browsers. Consumers would have to configure each web browser and each app individually according to their perceptions about the level of data protection, which significantly increases the effort for parallel use of different web browsers and thus increases the tendency towards single-homing. This is problematic from a competition policy perspective.[26]

Behavioural patterns such as whitelisting in the web browser market are known; as a result, their gatekeeper position in data generation or interaction with the user should not be further strengthened.[27] Whitelisting means that web browser extensions (functional extension by plug-ins, for example ad blockers) create a list of web pages and tracking companies that are then blocked when users visit a website. Websites and advertisers on these "black lists" can enter payment agreements with ad blockers (whitelisting) so that their tracking and advertising measures are permitted by the appropriate browser extension – in contrast to the intention of the consumer. This is done by disabling filtering on the whitelist pages so that these websites can display advertisements.

Overall, it becomes clear that a balanced and detailed compromise must be reached on the envisaged ePrivacy Regulation, particularly in order to prevent possible economic and societal collateral damage.

26 Krämer, J., R. Dewenter, D. Zimmer, I. Henseler-Unger, R. Arnold, C. Hildebrandt & G. Knieps. 2016. "Wettbewerbspolitik in der digitalen Wirtschaft." Wirtschaftsdienst 96 (4): 231–248; Doganoglu, T., & J. Wright. 2006. "Multihoming and Compatibility." International Journal of Industrial Organization 24 (1):45–67.

27 Mughees, M. H., Z. Qian & Z. Shafiq. 2017. "Detecting Anti Ad-blockers in the Wild." Proceedings on Privacy Enhancing Technologies 2017 (3):127–142; Sjösten, A., S. Van Acker, & A. Sabelfeld. 2017. "Discovering Browser Extensions via Web Accessible Resources." Proceedings of the Seventh ACM Conference on Data and Application Security and Privacy 2017:329–336.

5 Possible impact on online advertising and digital business models financed by advertising

5.1 Overview of online advertising and digital business models

In order to understand the relevance of the digital advertising industry and ad-based business models on the internet, it is worth taking a brief look at history. The World Wide Web was created at the beginning of the 1990s. At first it consisted of a few websites provided by mostly publicly funded publishers. The Global Network Navigator was created in 1993, when there were only a few hundred websites. The first online advertisement was placed there. As the number of websites grew from about 10,000 in 1994 to about 650,000 in 1997, the desire for a new way of navigating the internet arose. Several search engines were developed at that time. In the early 2000s, Digital Subscriber Line (DSL) speeds and flat-rate tariffs made internet access increasingly affordable and popular. Until then, advertising was the most important source of income for all online content and services. Consumers learned that once they had paid for access to the internet, they were largely free to use the services available. In return, advertisements were displayed. Websites requiring log-in were comparatively rare. These came mainly from new services such as social networking and voice-over-IP services, which required clear user identification, for example for billing purposes. With the market launch of smartphones and affordable data plans for mobile internet access, new services have been developed that focus more on the local and temporal situation of the consumer. The trend towards more log-in systems has been intensified.[28]

On the whole, it can be stated that from a historical point of view, consumers have different behaviours (usage habits) with regard to social networks, mobile apps and comparable applications in contrast to freely available websites, where they do not expect a log-in or a paywall as expected by the stakeholders. Accordingly, it can be expected that these two options for financing publishing and entertainment websites would be particularly difficult to implement.

Given the importance of advertising on the internet, the methods of placing advertisements have evolved alongside. Nowadays, there is rarely a simple (personal) negotiation between advertisers and websites regarding ad placement.[29] Instead, a complex ecosystem of different actors has emerged, and this continuously fills available advertising space on a website by using so-called programmatic advertising. This procedure distributes advertisements in real time, dynamically. Pricing is commonly

28 Arnold, R., & M. Waldburger. 2015. “The Economic Influence of Data and their Impact on Business Models.” In Trends in Telecommunication Reform 2015 – Getting Ready for the Digital Economy, edited by ITU, 153–183. Geneva: International Telecommunication Union.

29 The main pages of particularly high-reach online media are a notable exception. Even today, advertising spaces and types of advertising are partly negotiated directly between advertising agencies or the marketing departments of large brand companies and the operators of media offerings. But even Spiegel-Online has been relying on programmatic advertising since 2015 (see, for example, https://www.wuv.de/digital/premiere_fuer_spiege_titelseite_alle_anzeigen_werden_automatisiert_vertickt).

assigned in largely automated (real-time) auctions. Programmatic advertising is currently used by 87% of online advertisers, 92% of online agencies and 93% of online publishers in Europe.[30] The following figure displays the complexity of the system.

Figure 5: Display advertising ecosystem

Source: LUMA Partners LLC (2017).

In this system, the advertiser (marketer) requests a specific target group or advertising target from the advertising agency. The agency then initiates a process that dynamically optimises the control of the advertising media. Within the scope of an ongoing advertising campaign using creative optimisation, even different variants of advertisements can be imported, tested and evaluated, dynamically and in real time. This means that not only are the advertising spaces and environments dynamically adapted to the advertising objectives, but also the advertising design itself is. At virtually all interaction points, real-time data on reach, represented target audience on a given page, and budgets for each advertising space on any given site decide which advertisement will be shown in a specific spot.

30 IAB Europe. 2016. Attitudes towards Programmatic Advertising. According to Deloitte, Germany still lags behind as regards programmatic advertising. They find the following shares of programmatic ads in the US: 64%, UK: 70%, Germany: 49% see Deloitte. 2016. Closing the programmatic gap. The changing digital advertising in Germany. The Bundesverband Digitale Wirtschaft (BVDW) e.V. estimates that around 32% of the advertising reveneues registered in the Circle of Online Marketers' (OVK) advertising statistics are programmatic ads. See BVDW. 2016. Programmatic Advertising Kompass 2016/2017.

As a result, the vast majority of decisions are made by algorithms and not by people. This makes advertising significantly more effective and efficient. The biggest advantages of programmatic advertising are, however, on the part of the website owners and consumers. With the help of programmatic advertising, website owners such as publishers can market content that would not be monetised in a non-data-based advertising market, due to featuring a too-specific target group or addressing too many different target groups. In this way, the return on investment (ROI) for advertisers and publishers can be improved.[31] For consumers, programmatic advertising ought to result in fewer unsuitable or obviously useless online advertisements.
The following should therefore be noted:

- The refinancing of online services through programmatic advertising is an essential part of the economic activity in the online sector.
- Programmatic advertising only works by processing user data.
- This is done by means of automated procedures for storing on and retrieving information from the end-user's terminal equipment.

According to the ePrivacy Regulation proposed by the European Commission, programmatic advertising is no longer technically feasible and legally permissible. Technical feasibility depends first and foremost on the fact that the software on the end device allows the setting and retrieval of information. The end-user is required to decide on this during installation. In addition, the regulation requires a mandatory update for already installed software. Irrespective of the software settings, the processing of the information is only possible with the end-user's consent. Depending on user behaviour, the ePrivacy Regulation with its proposed rules may jeopardise a significant part of the economic activity in the online sector. In addition to the direct revenue losses in the advertising industry and for content providers, there is another important point to consider: programmatic advertising is one of the main drivers of innovation in the advertising industry. Numerous start-ups from Germany[32] and the rest of Europe[33] are evolving in this area. The expected change in user behaviour under the ePrivacy Regulation may threaten the existence of these companies.

Notably, programmatic advertising is an essential, but by no means the only, type of targeted advertising used on the internet. No matter how well the advertisement fits the interests of the consumer, it has to adjust dynamically to the type of terminal device, screen resolution and language preferences.[34] All information that is pre-defined in

31 BVDW. 2016. Programmatic Advertising Kompass 2016/2017.

32 Examples include AdSquare, Exactag, Remerge, Orbyd, adlicious, Breitengrat, realzeit, Yieldlove, AddApptr, Yieldlab.

33 Examples include Adform (Denmark), AdBrain (UK), Iponweb (UK), Admedo (UK), Axonix (UK) and Choozle (UK).

34 Without such an adjustment, web page loading times would be considerably longer and their presentation would be limited. For example, the ad would occupy the entire screen or a desktop-optimised ad would be displayed on mobile devices. In addition to these and other technical features of the terminal, the user's language preferences, which can be derived from the language settings of the browser or operating system, are also required for the correct display of advertisements. Without data exchange with the end device, it is likely that advertisements will be displayed in the wrong language.

offline advertising based on the surrounding content (e.g. in a magazine) can only be determined for online advertising by exchanging data with the user's terminal device.

Another important difference between online and offline advertising is the frequency of interaction with advertising. While broadcasting law has guidelines for how much advertising may be displayed, there are no such guidelines in online advertising. Also, a specific advertising space on a website can be filled with (almost) any advertising content according to a pre-defined target audience. In order to avoid bothering consumers with the same advertisement over and over again, it is necessary to know how often an advertisement has already shown on a specific device (frequency capping).[35] Data exchange with the terminal device is also necessary for this purpose, which specifically includes tracking of a terminal device. Should frequency capping no longer be possible, a considerable limitation of the user-friendliness (internet experience) is to be expected.

Furthermore, due to the amount of content online, it is necessary to be target-specific to achieve competitive advertising effectiveness.[36] A completely bespoke approach to an individual user is neither technically possible nor in the interest of the advertiser, since there is a decreasing marginal utility accompanied by a significant increase in marginal costs for any additional individualisation. Therefore, it is common practice to segment users (target group definitions). In doing so, groups of users are formed that are as homogeneous as possible and at the same time differ from each other as clearly as possible.[37]

Depending on user behaviour, the ePrivacy Regulation may mean that content providers who use advertising to finance their offers will no longer be able to do so in the future.[38] Information currently available, in particular from small and medium-sized providers, and special interest content could become unavailable as a result.

5.2 Expectations based on existing studies

A study conducted by IHS Markit on behalf of IAB Europe estimates that about two-thirds of the revenue generated by OBA, i.e. information made available from end-user devices.[39] For the year 2020, it is expected that this turnover will increase significantly and that a total of EUR 21.4 billion out of a total turnover of EUR 23.5 billion for display advertising will come from OBA. The study predicts a decrease of up to 70% in display advertising if end-users no longer allow third-party cookies in the future.

35 This leads to a diminishing benefit of advertising insertion or even to a negative benefit as the consumer will be irritated by constant repetition.

36 Reisch, L., D. Büchel, G. Joost & H. Zander-Hayat. 2016. Digitale Welt und Handel: Verbraucher im personalisierten Online-Handel. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) beim Bundesministerium der Justiz und für Verbraucherschutz.

37 Riekhof, H.-C., T. Schäfers, & I. Eiben. 2009. Behavioral Targeting: Ein effizienter Einsatz des Online-Werbebudgets? PFH Forschungspapiere, Private Fachhochschule Göttingen.

38 Individual media services with a particularly high reach can continue to sell individual advertising spaces directly. However, the majority of today's budgets flow into programmatic and targeted advertising.

39 IHS Markit. 2017. The Economic Value of Behavioural Targeting in Digital Advertising.

While the impact on online content and application providers who can use their own user data for advertising purposes is estimated to be rather low, the study assumes that users will primarily not accept cookies from third-party providers in the future. The result would be a reduction of 50% to 70% in advertising revenue for publishers without sufficient data/scalability to differentiate or for ROI reporting to their advertising clients. The redistribution of digital advertising expenditure to market participants with a lot of user data available for this purpose and traditional advertising media would be expected.

The analysis by IHS Markit provides a first clue. However, it deals exclusively with sales for display advertising and is not aimed specifically at the German online advertising market.

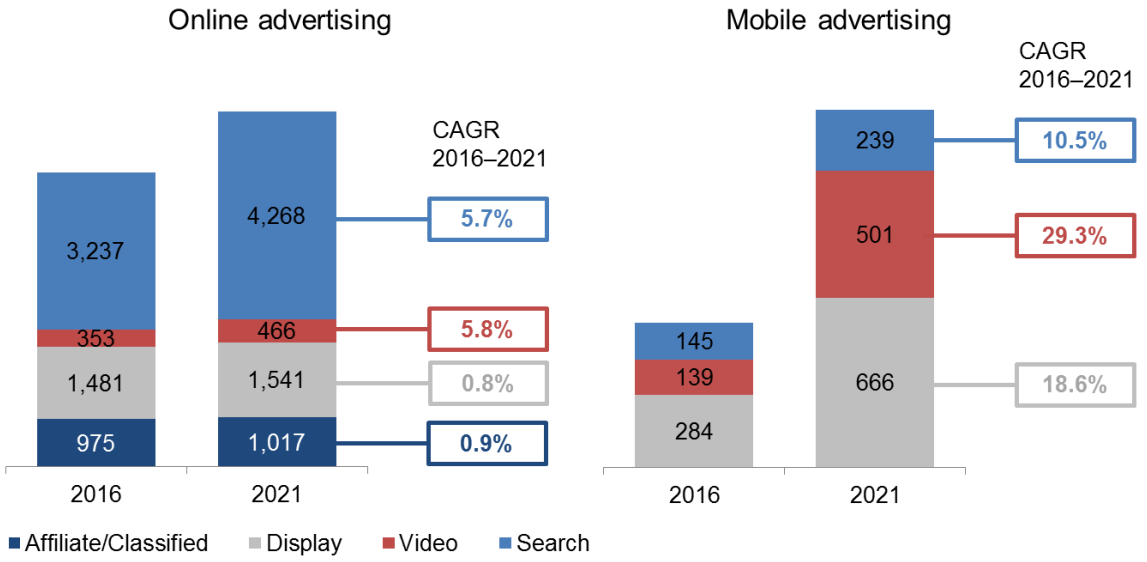
5.3 Assessment of the German online advertising market

Based on the assessments of the stakeholders surveyed and our own research, the following section looks at a probable scenario for the German online advertising market.

Since display advertising not only depends to a large extent on behavioural targeting but also requires access to the processor and storage capacity of the end-user's device, the ePrivacy Regulation makes this practically impossible, because it is expected that end-users will set their browser software in such a way that third-party cookies will no longer be allowed. The German display advertising market is likely to suffer considerably. According to the Online-Vermarkterkreis (OVK), this currently corresponds to a sum of about EUR 1.5 billion.[40] In addition, it can be assumed that affiliate advertising will also come to a halt in the short term. There, click-through tracking is required for billing. PwC currently estimates this to be around EUR 975 million in Germany.[41] Overall, it can therefore be assumed that approximately one-third of the current online advertising revenue in Germany is threatened by the ePrivacy Regulation (see Figure 6).

40 OVK. 2017. Net advertising revenues of recordable advertising media in Germany 2013 to 2016.
41 PwC. 2017. German Entertainment and Media Outlook 2017–2021.

Figure 6: Online advertising turnover in Germany by category (in million €)

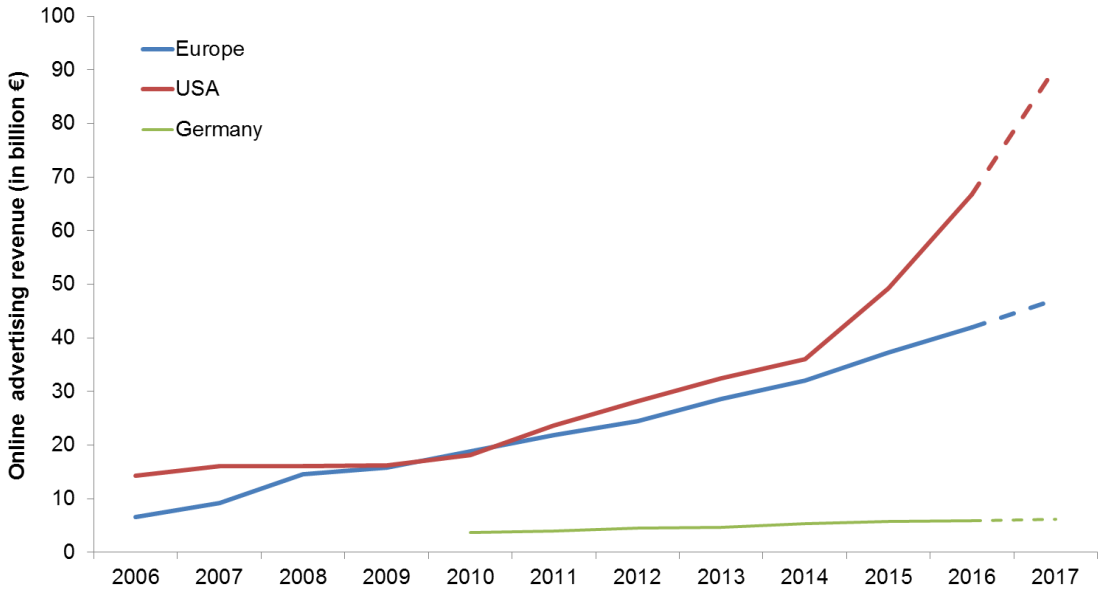


Source: PwC. 2017. German Entertainment and Media Outlook 2017–2021.

For search advertising and social advertising, which form the main formats of the remaining advertising revenue, only minor effects, if any, of the ePrivacy Regulation are to be expected. The decoupling from the growth curve exemplified by the advertising market in the US (see Figure 7) would be intensified.

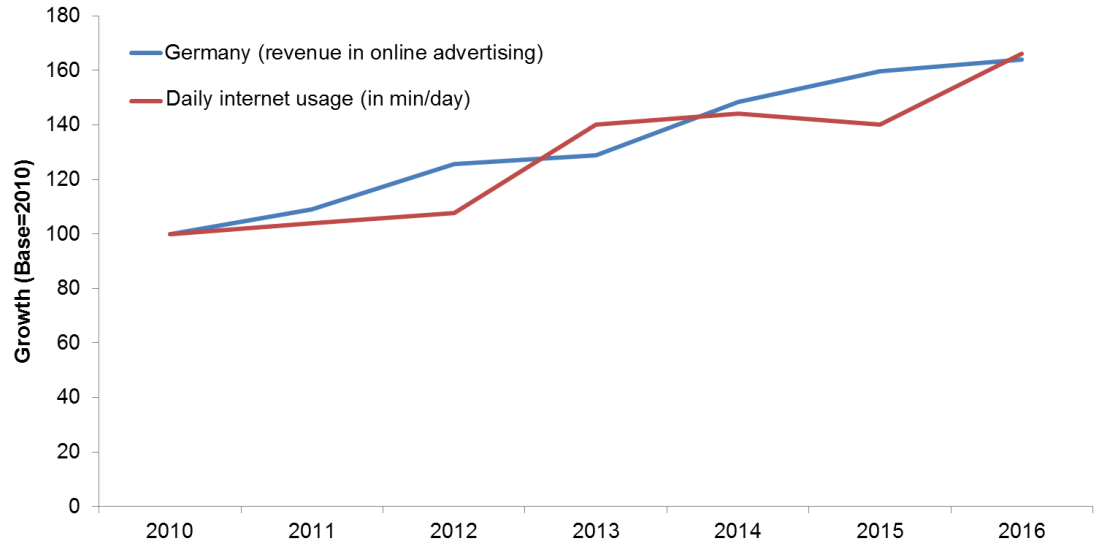
A different development can be expected in the medium to long term. In principle, advertising has so far always followed the attention of consumers. This is illustrated by the close correlation between the growth in daily use of the internet and growth in online advertising revenue in Germany, as shown in Figure 8.

Figure 7: Online advertising revenue in Germany, Europe and the US



Source: IAB and WIK estimates.

Figure 8: Online advertising in Germany and average daily use of the internet (Index 2010 = 100)



Source: IAB, MediaPerspektiven and WIK estimates.

The ePrivacy Regulation, as outlined above, is likely to strengthen the market position of closed (log-in) systems. On the one hand, online services outside of log-in systems become less attractive due to the likely suppression of access to storage and processing capacities of the terminal equipment. Since consumers prefer a simple and intuitive handling of online offers, it can be assumed that only a few will extensively deal with the question of whether and how to configure their software settings in order to maintain the accustomed user-friendliness. Instead, they will prefer online offers which, due to their consent or pre-settings, will give them the accustomed user-friendliness. On the other hand, a large number of independent providers will no longer prevail due to the lack of refinancing of their websites, and as a result there will be little or substantially less choice for end-users.

Finally, consumers will likely accept log-in systems where they are already used to them. This applies in particular to social networks such as Facebook, e-commerce platforms such as Amazon and communication services such as WhatsApp or Instagram. As a result, it seems likely that consumers will use the internet (even) more than ever before within such closed systems. It can be assumed that the advertising material and content will follow this trend as it has to be where the consumers' eyeballs are. In combination with the gatekeeper position of web browsers, it is likely that in the medium to long term, major online platforms such as Facebook and Google, which are heavily financed by advertising, will benefit in comparison with other market participants.[42] The ePrivacy Regulation may therefore trigger the development of a largely proprietary internet, of which the advertising revenues are generated almost entirely outside of Europe.

42 The ePrivacy Regulation also has a negative impact on Facebook, Google and other large platforms.

6 Summary and outlook

The amendment of the protection of privacy and confidentiality in electronic communications is currently leading to controversial discussions between consumer watchdogs, data protectors and representatives of the digital economy. While the first two groups emphasise a necessary improvement in how data is treated by online content and application providers, the latter group insists that the innovative momentum of the digital economy should not be brought to a halt by regulation.

From an economic point of view, it is important to understand the basic trade-offs in a highly complex and interdependent internet ecosystem before setting the political course.

Data protection versus data economy

- The ePrivacy Regulation is intended to contribute to a successful European data economy, but excludes the consideration of legitimate economic interests.
- The ePrivacy Regulation is likely to shift the added value generated by the digital economy to large market players even more than before.
- Providers of high-quality content on the internet who are reliant on refinancing through advertising see their business model threatened by the draft regulation. These fears are to be taken seriously. The loss of these offers would be a significant limitation of media diversity.
- Consent as the primary benchmark, as stipulated in the ePrivacy Regulation, is not an appropriate instrument to protect consumer data sovereignty. This requires a holistic concept of digital sovereignty in combination with new technical implementation possibilities of data sovereignty for consumers.

Data protection versus competition

- The protection of privacy and confidentiality in electronic communications is generally supported by all stakeholders, but distortions of competition must be avoided.
- Operating systems and web browsers must not be strengthened in their role as gatekeepers by implementing data protection by default/design.
- Self- and co-regulatory approaches may be superior to regulation.
- The regulations of the ePrivacy Regulation may in the long-term benefit leading US service providers when compared to small and medium-sized providers such as those based primarily in the EU.
- Generating a proprietary internet based on log-in systems and payment barriers is no more in the interests of consumers than in the interests of the European economy.

While the draft ePrivacy Regulation was ignored by many at the beginning, it is now attracting the attention of numerous stakeholders. The interviews conducted show that the upcoming ePrivacy Regulation is accompanied by significant concerns for the digital economy in general and the online advertising industry in particular. Based on the information available on the current share of online advertising in the digital value chain and the ideas on better protection of privacy expressed in the draft ePrivacy Regulation, these concerns are to be taken seriously. Considerable disadvantages for Europe's innovation potential and economic development can be expected.

The exact extent of the possible effects could not be fully assessed in this study. This would require a much more comprehensive study (using primary and secondary data) to determine both the direct and indirect effects. This would also enable a macroeconomic analysis to be carried out.

Furthermore, the present study lacks a detailed assessment of the possible effects of the ePrivacy Regulation on consumers in Germany and the rest of Europe. As other WIK studies have shown, consumers benefit to a considerable extent from ad-based digital business models. This benefit goes far beyond the revenues at stake. Such a consideration would illustrate the scope of the impact in social, cultural and technical dimensions.

Ultimately, the question of long-term development of the internet ecosystem remains largely unanswered. A more detailed analysis could provide information on the extent to which the newly created market conditions will be either positive or negative from a macroeconomic point of view.