More data sovereignty, fewer barriers to digitalization

How the proposed ePrivacy Regulation will affect competition and growth in Europe

Policy Paper

Preface

The European Internet economy stands at a crossroads. In May 2018, Europe's landmark General Data Protection Regulation (GDPR) will take effect, ushering in a new era of standardized rules for the processing of consumer data in all 28 EU nations. Besides strengthening data protection and consumer choice, it represents a major step toward the creation of an effective Digital Single Market.

However, this vision of potential progress is muddled, ironically, by another piece of legislation proposed by the European Commission: the so-called ePrivacy Regulation. Initially intended as a complementary regulation to clarify the GDPR's privacy rules for personal electronic communications data, the regulation as discussed today goes beyond the provisions of the GDPR and creates further barriers to the processing of personal data. While it lacks clarity in decisive areas, the scope of its validity is now so broad that virtually every European company would be affected by it.

Hence, the current proposal would have serious – and presumably unintentional – consequences for the European economy as a whole and hinder the development of European digital companies. We therefore call for a revision of the regulation in order to establish a fair balance between data protection and data processing guided by the principle of data sovereignty.

This paper builds on a statement that the Internet Economy Foundation released in July 2017. Since then, consensus among digital ventures all across Europe – start-ups, more mature Internet companies as well as digitalizing players in the old economy – has formed around the fact that the proposed plans threaten a successful European digital future. Various players have encouraged us to speak on their behalf and echo these concerns. This paper gathers those stories, examines the economic context, presents many real-world case studies, and demonstrates what is at stake. We hope that this paper will serve as a helpful addition to the current debate, and that we can play our part in strengthening Europe's digital future.

Friedbert Pflüger
Chairman
Internet Economy
Foundation

Clark Parsons
Managing Director
Internet Economy
Foundation

Three key points for effective privacy and fair competition:

1. Maintain flexibility regarding data processing
2. Keep digital services independent of browsers
3. Allow transitional periods for the implementation of new rules

Contents

1
WHAT WE ARE DISCUSSING:
The draft proposal for an ePrivacy Regulation

Effective and fair forms of privacy reconcile the interests of citizens with those of the economy. They enable businesses to offer customers a broad spectrum of digital products. They also safeguard citizens' sovereignty over their data: Thanks to transparent rules, people are clear about what happens to their personal data and how these are processed. To date, however, this kind of privacy has been implemented only partially at the European level. True, the General Data Protection Regulation (GDPR) ratified by the EU in 2016 does harmonize data protection across Europe, and it also strengthens the rights of consumers. Yet it also limits the ways in which companies can process personal data, and that creates huge challenges to the realization of data-driven business models.

In January 2017, the European Commission submitted its draft proposal for an ePrivacy Regulation[1] to replace the 2002 ePrivacy Directive.[2] On June 21, Marju Lauristin, rapporteur for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), released a draft report on the proposed ePrivacy Regulation.

The proposed regulation is intended to establish consistent data protection rules within the sphere of electronic communications throughout Europe. It is designed as a *lex specialis* to complement the GDPR, clarifying and supplementing the rules enshrined in the latter with regard to electronic communications data. In the view of the European Commission, that explains why it primarily addresses providers of electronic communications services. As digitalization and convergence advance, however, the proposed ePrivacy Regulation put forward by the Commission would also have serious – and presumably unintentional – consequences for the European economy as a whole.

At its meeting on October 11 and 12, 2017, the LIBE committee is scheduled to discuss and ratify the draft, clearing the way for the plenary session to consult on the proposed regulation before the month is out. In parallel, the EU member states are currently debating the Commission's proposal within the framework of the EU Council and are seeking to establish a common position. As things stand, there is no way of knowing whether the Council will reach agreement this year or not until 2018. The regulation cannot become law until the Parliament, the Council and the Commission reach a compromise regarding the Commission's proposal on which they all agree. Once this hurdle has been cleared, however, the Commission intends to move fast: The plan is for the ePrivacy Regulation to take effect – with no transitional period – as early as May 25, 2018. It is therefore high time to take a closer look at how the proposed ePrivacy Regulation will impact the European economy and the competitiveness of data-driven business models that are "made in Europe".

Considerable uncertainty surrounds the concrete effects of the planned ePrivacy Regulation. One reason is that many of the provisions set out in the draft regulation differ from those of the GDPR and therefore create significant legal uncertainty. Another is that the draft

1 Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation)
2 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive)

Europe's data protection rules would do well to champion data sovereignty rather than tread the ill-advised path of data minimalism.

regulation is still in the middle of the legislative process, in the course of which numerous amendments are still to be expected. The huge importance of personal data to the European economy and widespread criticism of the draft ePrivacy Regulation call for a thorough investigation of the effects, both intentional and unintentional, of the Commission's proposal.

The belief that the ePrivacy Regulation in its current form would have a negative impact on Europe's economy is based on two main arguments. First, the draft goes beyond the provisions of the GDPR and creates further barriers to the processing of personal data. Second, the scope of validity is so broad that virtually every European company would be affected by it.

For these reasons, the ePrivacy Regulation threatens to make digital value creation grind to a halt across the whole of Europe. At the same time, the current draft of the regulation would further strengthen the position of the dominant Internet platforms. Within their vast digital ecosystems, the latter have the capability to market a large number of digital services and bundle the necessary declarations of user consent in a customer-friendly form. The planned ePrivacy Regulation could thus trigger a further concentration of personal data in the hands of a small number of market-dominating companies, ultimately – and paradoxically – weakening privacy in Europe. That would run counter to the European Commission's stated aim of promoting digital innovation on the basis of a Digital Single Market and establishing Europe as the leading region in the global Internet economy.

If the European economy is not to fall behind in the digital race, the planned ePrivacy Regulation must, together with its negative effects (including the unintentional ones), be subjected to a thorough review. Europe's data protection rules would do well to champion data sovereignty rather than tread the ill-advised path of data minimalism. Its people should be able to make their own informed decisions about which services and functions they wish to use and the kinds of data processing to which they thus give their consent. This perspective avoids creating a fictitious "dualism" between the interests of users on the one hand and the interests of businesses on the other. Instead, it accommodates the fact that data-driven products generate substantial benefits for customers, and that data processing by companies is therefore also in the interests of users.

2 WHAT IS AT STAKE:

Data as the bedrock of sustainable economic activity

As digitalization gains ground, data are moving center-stage in all areas of society and all sectors of the economy. Data's importance to the workings of modern societies is often likened to the role of oil in the 20th century. As was the case with oil, all kinds of products today are no longer conceivable without data. Companies also need data to get their products to the customers. We have reached a point where it is easier to deliver a product without using fossil fuels than without using data. Digital business models are based on connectivity between selected data points which allows them to generate extra benefits for customers. The speed at which and the extent to which digitalization is transforming the economy is shown by a glance at the sectors in which the world's ten most valuable companies operate. →A

In 2006, manufacturing and natural resource companies accounted for 64% of the market capitalization of the world's ten most valuable enterprises.[3] Microsoft was the only technology company that made it onto this elite list. Ten years later, however, the ratio had almost been reversed: Manufacturers now comprise only a quarter of the market capitalization of the ten most valuable companies[4] – compared to 59% for tech firms.[5]

That, however, is only the tip of the iceberg, and it should not obscure the fact that data are becoming a central factor of production for practically every company. Businesses have to reach out to their customers via digital interfaces and offer them solutions that are rigorously customer-centric. If they don't, the big Internet platforms threaten to claim the customer interface with their digital ecosystems and render conventional business models obsolete. A prime example of such verticalization is the way Alphabet (Google) has penetrated a varied assortment of digital and industrial sectors (operating systems, browsers, messaging, logistics, smart metering, and so on).

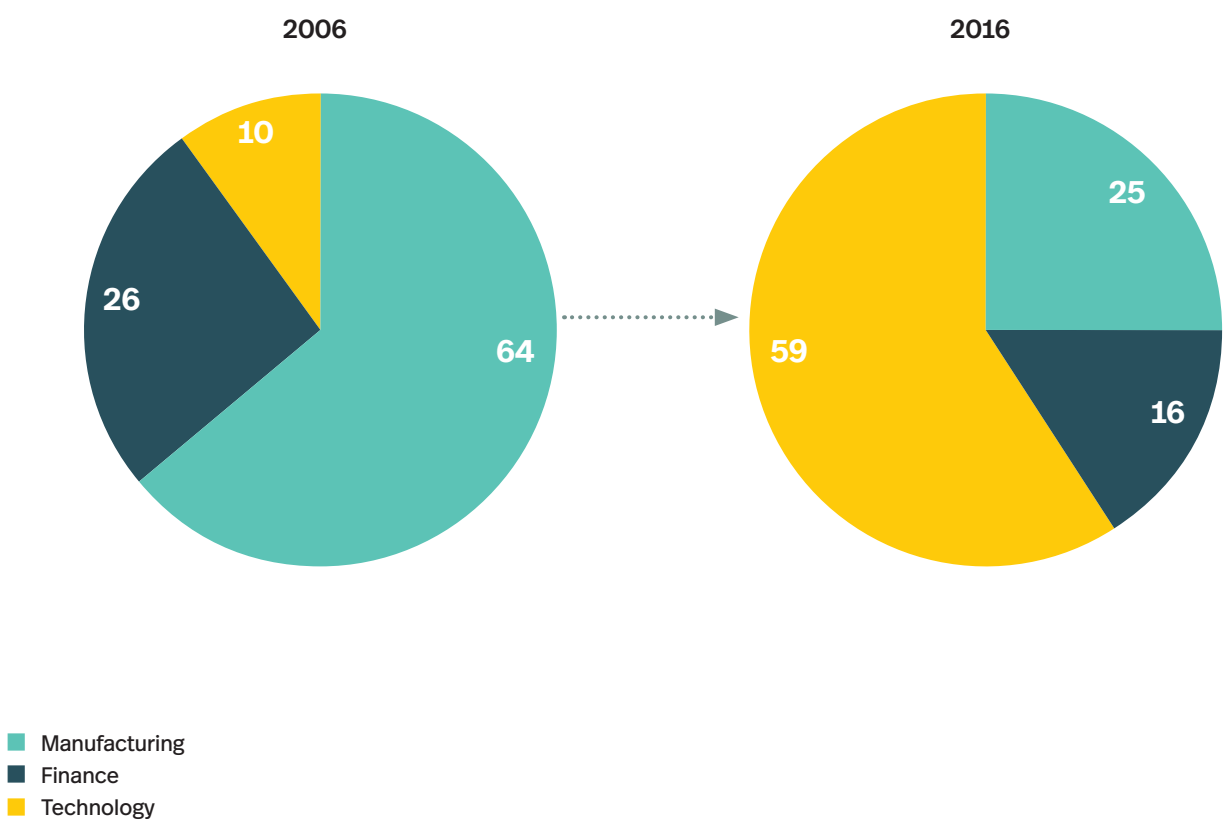
If Europe's economy is to stay competitive as digital platforms make inroads into established sectors of services and industry, modern data processing and innovative analytics must become core elements of their business models. The development and intelligent use of extensive databases is becoming a crucial factor of competition. Carefully and selectively linking individual data points facilitates the development of modern business models and personalized offerings for customers. Huge demand exists for the latter, as such offerings generate considerable customer benefits.

Personal data are only one aspect of the data that companies process, and electronic communications data in the sense used in the planned ePrivacy Regulation are only a subset of personal data. That said, electronic communications data occupy pride of place in data-driven business models. They can be compared to the steering system in a vehicle: Though it is only one of many elements of a vehicle, it is indispensable to getting from Point A to B in a sensible way. That is why European companies need a reliable legal framework that lets them make use of electronic communications data in the

3 ExxonMobil, General Electric, Gazprom, BP, Royal Dutch Shell, Toyota
4 ExxonMobil, Johnson & Johnson, General Electric
5 Apple, **Alphabet (Google)**, Microsoft, Facebook, Amazon

A New world: In just ten years, the lion's share of the market capitalization of the world's ten most valuable companies has shifted from manufacturing to the technology sector

Annual average [%]



Sources: Bloomberg; Roland Berger

manner required by the modern digital world. If the government raises the barriers to the processing of these data too high, the economy loses its access to the digital world's most important raw material – to the detriment of companies, employees and consumers alike.

What is at stake is readily apparent from a study[6] commissioned by the European Commission. Published in February 2017, the study examined issues such as how the European data economy will develop between now and 2020. Taking account of direct, indirect and secondary effects, it focuses on how the market for data-related services and products will impact the economy as a whole.[7] The study put the value of the European data economy at an estimated EUR 300 billion in 2016 – equivalent to roughly 2% of total European GDP. If the conditions within which the European data market operates were to improve, the value of the whole of Europe's data economy could rise to EUR 739 billion – or nearly 5% of GDP[8] – by 2020. That would equate to annual growth of 25%. Whether or not the European economy can realize this growth potential, however, depends in part on the precise form taken by the proposed ePrivacy Regulation.

The European economy could lose its access to the digital world's most important raw material.

6 European Data Market – Final Report, February 2017. The study was produced by IDC and Open Evidence on behalf of the European Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT).

7 Direct effects result from revenue generated with data-related services and products. Indirect effects comprise the additional revenues of supplier (upstream) and user (downstream) industries. The benefits of a production process that is optimized on the basis of data would thus constitute the indirect effect of the data market on the economy as a whole. Secondary effects take account of consumption resulting from the additional wages of employees in the data market and its direct supply industry.

8 To estimate this percentage, reference was made to the Oxford Economics forecast of the EU's GDP in 2020 (in real terms, based on 2010 prices and exchange rates).

3
DIGITAL OBSTACLE COURSE:
How the planned ePrivacy Regulation will affect the economy

The planned ePrivacy Regulation is designed as a *lex specialis* to the GDPR. As such, it will particularize and complement the General Data Protection Regulation as it regards electronic communications data that qualify as personal data. Unlike the 2002 Directive on Privacy and Electronic Communications that has been valid until now, the plan is for the new ruling to take the form of a regulation that, when it takes effect, will immediately be valid across all EU member states. That is a rigorous and sensible step to take: A regulation (as opposed to a directive) would introduce consistent rules for all consumers and companies. Similarly, plans to introduce the law of the place of performance (*lex loci solutionis*) along the lines of the GDPR, whereby the regulation would be valid for all end-users in the EU – irrespective of where the controller operates or is headquartered – mark another important step toward creating fair competitive conditions for European and non-European companies. →B

Unlike its predecessor directive, the ePrivacy Regulation would also apply to what are known as over-the-top (OTT) communications services. These are Internet services such as WhatsApp, Facebook Messenger and Skype that provide electronic communications services as online applications. In the future, these OTT services will be bound by the same legal framework as conventional telecoms providers. The ePrivacy Regulation would thus accommodate both modern technological conditions and users' changed behaviors. The same is also true for the new possibilities for data-based value creation that telecoms providers can access subject to end-users' explicit consent.

Alongside these positive aspects, the draft ePrivacy Regulation also contains a number of elements that would have a negative impact on Europe's digital economy. For example, the ePrivacy Regulation is scheduled to take effect at the same time as the GDPR on May 25, 2018. Unlike the GDPR, however, the binding version of the ePrivacy Regulation is not even known yet. Indeed, due to the complexities of the legislative process, it will be ready only shortly before the regulation is due to become law. This fact burdens Europe's economy with virtually insoluble problems: How can companies prepare for a new set of rules whose content has not yet been finalized?

An added concern is that the planned ePrivacy Regulation will apply not only to electronic communications services, but to practically all digital services and a large number of Internet of Things (IoT) applications. That is a problem because the draft envisages even higher barriers to data processing than those anchored in the GDPR.

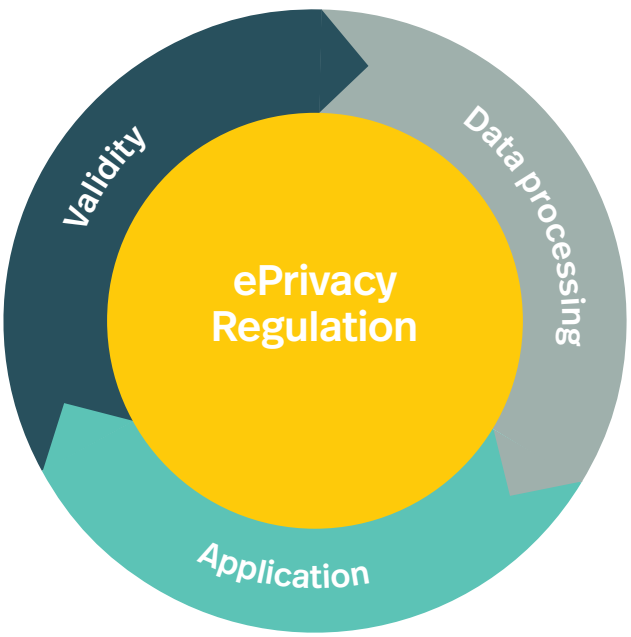
3.1 Broad scope of validity

Looking at all these areas of application, the Commission's proposal resembles a puzzle. At first glance, the planned regulation appears (and claims) to be a *lex specialis* that concerns itself with electronic communications services. Yet the more closely one examines the text, the more areas of application crop up in the regulation. And if you put these individual pieces of the puzzle together, a surprising picture emerges: The current

B New rules: The most important new provisions in the planned ePrivacy Regulation compared with the existing Directive on Privacy and Electronic Communications

Regulation instead of directive
Implementation in the form of a regulation rather than a directive is designed to introduce consistent rules across the whole of the EU.

Lex loci solutionis
The planned regulation would be valid for all end-users in the EU, irrespective of where the controller operates or is headquartered.



Consent to data processing
In almost all cases, the processing of communications data would in the future require the explicit consent of the end-user – even where user data is pseudonymized.

Central privacy settings
Users would be able to set their privacy settings (such as consent to data processing) centrally, e.g. in their browser.

OTT services
The privacy provisions would also apply to over-the-top (OTT) services such as WhatsApp, to put the latter on the same footing as conventional telecoms providers.

M2M communication
The planned regulation would also be valid for communication between machines.

Source: Roland Berger

draft of the ePrivacy Regulation has such a broad scope that it is scarcely possible to conceive of any digital business model that would not be affected by it.

The ePrivacy Regulation would, for example, apply not only to OTT service apps, but to all apps simply because of the way they work. All app developers who want to sell their products on the European market would therefore have to comply with the provisions of the ePrivacy Regulation. The rapid proliferation of innovative apps in recent years has been rooted in the possibility of drawing on personal usage data to analyze, improve, advertise and finance these products. →CASE 1 It follows that the ePrivacy Regulation would affect the whole of the European app economy – the most important growth segment in the digital economy. Beyond that, many digital offerings would be affected if the planned regulation were applied to communications services that only fulfil secondary functions of other services. Examples include chat functions that simplify specific transactions on digital platforms. →CASE 2

Nor is that all. Including machine-to-machine (M2M) communication in the remit of the planned ePrivacy Regulation would mean that any number of IoT applications would also be affected. Besides familiar applications such as connected driving and smart homes, the regulation would thus also apply to completely new IoT technologies that have not yet been developed. →CASE 3

Lastly, the planned ePrivacy Regulation would also affect numerous European companies that are currently developing digital business models. Given the pivotal importance of data in general and personal communications data in particular in the context of digital innovation and new business models, the planned ePrivacy Regulation threatens to put the brakes on digitalization all across Europe.

3.2 New barriers to data processing

Apart from the ePrivacy Regulation's very broad scope of validity, a critical look must also be taken at the barriers to the processing of personal data that the regulation calls for. One issue is that some provisions in the draft ePrivacy Regulation differ with those in the GDPR – which creates tremendous legal uncertainty for all businesses as well as public organizations that are currently investing to ensure compliance with the GDPR. On the other hand, the draft ePrivacy Regulation would raise higher barriers to the processing of personal data than those prescribed by the GDPR. At the same time, the draft produced by the parliamentary committee fuels fears that, in the course of the parliamentary process, even these barriers could be raised still further. →C

Unlike the GDPR,[9] the draft ePrivacy Regulation makes no provision for processing data on the grounds of the legitimate interests of controllers or third parties. This

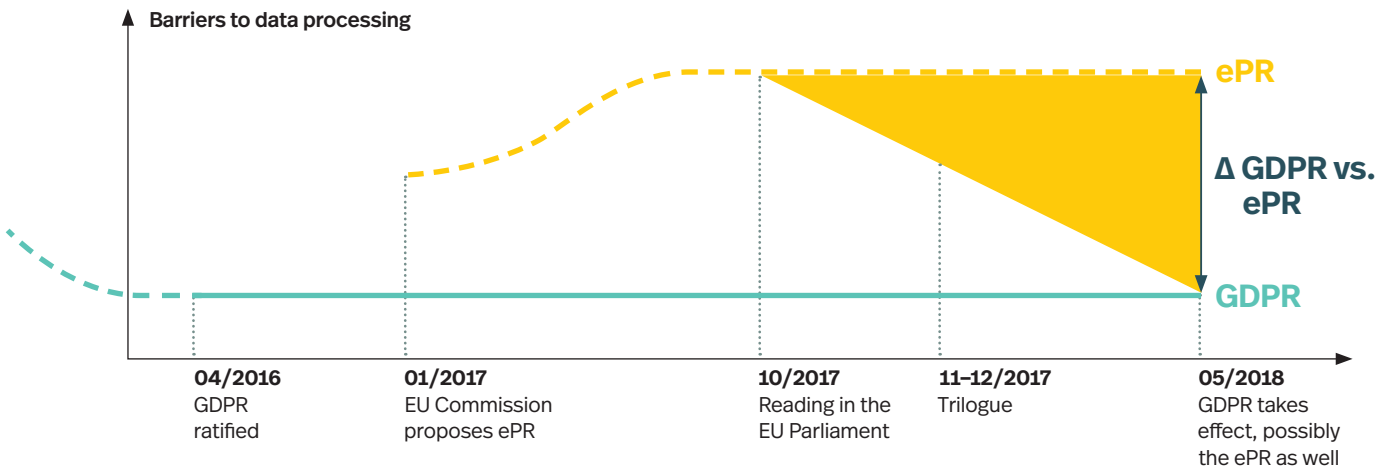
9 See Regulation (EU) 2016/679 Article 6 (1) f

means, for example, that communications data cannot be used to prevent the abuse of a service without the user's explicit consent to do so. Depending on how the planned ePrivacy Regulation is interpreted, it could even lead to situations in which the explicit consent of the sender is required before spam filters can be activated.

Unlike the GDPR,[10] the ePrivacy Regulation also makes no provision for technical data protection measures, especially those that involve the processing of pseudonymized data and/or encryption. Pseudonymization is a technique used to separate the identity of users from their data in order to guarantee a high level of privacy and also allow data to be processed. The GDPR acknowledges the fact that pseudonymized data require less protection than personal data and therefore allows such data to be processed without explicit consent under certain circumstances. By contrast, the ePrivacy

C Digital barriers: The planned ePrivacy Regulation would make barriers to the processing of personal data substantially higher than under the General Data Protection Regulation

Time line and barriers to data processing in the new ePrivacy Regulation



Source: Roland Berger

10 See Regulation (EU) 2016/679 Article 6 (4) e

CASE 1

How cookies improve digital offerings

Cookies are identification codes – usually in the form of text files – that websites and apps store on the user's terminal equipment. If the user returns to such a site again, the identification code is sent to its web server. This procedure lets the providers of digital services collect various kinds of information, including reports on disruptions to or problems with the use of the service, for example. Entries made in online forms can be stored in the same way and proposed as prompts if a user accesses the same form again. The technology is also used to personalize services. Users benefit, for example by being shown information such as the weather forecast or local news for their current location, as well as advertising that is tailored to their preferences. Cookies can also verify the effectiveness of an advertising campaign and make displayed advertisements more relevant. This in turn enables digital services to pay their way with a smaller number of advertisements. Broadly speaking, cookies are of central importance to both the functionality and financing of digital offerings.

Articles 8 through 10 of the planned ePrivacy Regulation seek to link the placement of cookies to the user's explicit consent in most cases (recitals 20-24 to the Commission's proposal). As things stand, other reasons for consent, such as due consideration for legitimate interests and technical measures such as pseudonymization, are completely ignored. Moreover, the draft affords paramount importance to central settings in the (browser) software with which users access the Internet. When first setting up this software, customers would have to make a generally valid decision about how cookies are to be handled. It is reasonable to assume that even users who appreciate the benefits of cookies in the case in point and therefore wish to use them might nevertheless decline to accept cookies as a general decision. The consequences of such a decision might not be clear to many users, as the specific benefits of cookies are quite varied and of a technical nature. It also remains unclear how individual providers might be able to obtain consent for the use of cookies despite the central browser setting, where this consent is necessary for a service which the customer wishes to use.

There is therefore a danger that numerous services will no longer be able to use cookies. That would detract from the quality of customer offerings, because cookies perform an important quality assurance function. At the same time, the planned ePrivacy Regulation would eliminate the basis for the funding of many free Internet services of which customers willingly take advantage. Among others, it would affect the providers of news websites that depend on cookies to fund their offerings. Small companies too can use cookies to place focused advertising on the Internet at low cost. Accordingly, the ePrivacy Regulation would hit these small firms hardest and undermine the diversity of digital offerings.

CASE 2

Why digital products depend on communications services as ancillary features

In the words of Article 4 (2) of the draft ePrivacy Regulation, services "which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service" are also to be classed as interpersonal communications services (see also recital 11 to the draft ePrivacy Regulation). The implication is that even interpersonal communications in the form of a chat function in a gaming app or on an e-commerce platform would fall within the scope of the planned regulation.

A lot of digital services use this kind of chat function to make their offerings more user-friendly. Customers visiting an e-commerce website can, for example, use such functions to contact the seller directly and clarify questions or submit complaints. The communications function thus facilitates straightforward and (normally) swift consultation between customer and seller without the need for the service provider to get involved. Most of the providers of platforms that offer or solicit shared rides also use this kind of chat function. In this way, drivers and passengers can establish contact ahead of a ride and discuss details such as the exact point of departure. In the case of online games, the communication function simplifies collaboration between multiple players in a team.

In all these cases, the service provider has a legitimate interest in filtering communication within its channels for inappropriate content such as verbal abuse or sexual harassment. Similarly, the service operator must be able to filter out any misuse of the service and/or illegal content to ensure that its customers can use its offerings in an atmosphere of trust and safety. If the ePrivacy Regulation comes into force in its present form, however, service providers would have to dispense with these filters. The ones who suffered would thus be the customers who were forced to do without these useful and protected communication channels.

CASE 3

How smart homes improve quality of life

Applying the ePrivacy Regulation to M2M communication would affect not only mobility applications but homes as well. Grouped together under the heading smart home, all kinds of household devices and appliances are being joined up to save energy, improve security, adapt functionality to individual members of the household and generally make life easier and more convenient.

The heating can be turned on if a resident's smartphone communicates the information that the person will soon be home. Sensors and cameras can be used to make one's own four walls more secure. A smart refrigerator can detect when the milk is running low and order a delivery from a grocery store.

All these applications have one thing in common: They are all based on personal communications data. However, they only serve their purpose if they operate without the involvement of the user: A connected refrigerator should order the milk without the user having to explicitly agree that this information can be transmitted to the supermarket. The same goes for heating: Users want to come back to a nice, warm home. But if they have to grant their explicit consent to transmitting their time of arrival each and every day, that erodes the benefit of the application.

Smart home applications need personal communications data to generate benefits for customers.

CASE 4

M2M communication – fundamental to the future of mobility

Recital 12 in the draft ePrivacy Regulation notes that communication between machines should also fall within the scope of the regulation. Known as machine-to-machine or M2M communication, it lays the foundation for IoT applications and is the single most important field of future activity for industrial value creation.

Connected driving is already widespread and exemplifies the importance of M2M communication. Millions of vehicles today send information about traffic flows, road conditions and the weather, allowing the drivers of connected vehicles to be notified in good time of a bank of fog, or of the tail of a traffic jam beginning after a bend in the road, for example. This system can only work, however, if as many drivers as possible consent to having their vehicle data transmitted and analyzed in an anonymized form. If individual vehicles do not transmit this information, that would detract from road safety but do nothing to enhance privacy.

M2M communication is even more important in the context of autonomous driving. Autonomous vehicles can only navigate safely if they receive regular updates containing current navigation and traffic information. This means that vendors must have the

option of storing data on the "terminal equipment" (in this case, the car) without the user's explicit consent. Safe and reliable autonomous driving can only be made possible if all autonomous vehicles have up-to-date information.

CASE 5

From point of access to gatekeeper

Alongside smartphone apps, web browsers are still the main interface via which Internet users access online e commerce, information and entertainment offerings. To create a user experience that is as attractive as possible (particularly by combining personalization with localization), the providers of these services usually depend on the use of cookies – unlike social media platforms with a far more extensive reach.

Following the logic of the proposed ePrivacy Regulation, web browsers would in the future play a weightier role in determining which Internet offerings can store information (e.g. cookies) on a user's terminal equipment and which ones cannot. The draft version foresees users making such decisions on a central basis in their browser settings. To use Internet offerings via browsers in the future, it would therefore no longer be enough to click one's consent to the provider's cookie policy on a given website. If central settings conflicted with this decision, the browser would still prevent cookies from being stored. Users would therefore have to trawl through the (usually complex) settings menu for their browser to confirm specific exceptions to the rule. And experience shows that very few users are prepared to go to so much trouble. Yet the proposed regulation makes no provision for a technical interface that could communicate individual exceptions directly to the central settings in a manner that is genuinely convenient for the user. As a result, providers would depend on the goodwill of browser vendors and the way they design their interface definitions – assuming that these exist at all.

Among Internet providers, the already strong position of those social media services that can do without cookie-based user identification would thus increase further, simply because their users tend to be always logged in. Another issue is this: Browser vendors operate in a small market with only a handful of powerful players that are themselves often part of vertically integrated ecosystems. If their "gatekeeper role" is now further strengthened, this could add to the danger of abuse and create new problems in the area of competition.

The ePrivacy Regulation would strengthen the role of browser vendors and thus create new digital gatekeepers.

Regulation does not draw the same distinction. The draft version instead restricts itself exclusively to explicit user consent as the basis for the processing of personal data. Its assessment is narrower and stricter than that of the GDPR.

It will be easier for the big Internet platforms than for small firms to overcome barriers to data processing that are higher than those in the GDPR. Above all, the Commission's proposal on the ePrivacy Regulation will put niche online services at a disadvantage compared to the major Internet platforms. Such platforms as Alphabet (Google), Apple, Facebook, Amazon and Microsoft[11] have built digital ecosystems in which customers can access all kinds of vertical services – such as browsers, email, messaging and cloud storage – from a single source. Coupled with a broad base of vertical integration, their dominant market position enables these digital platforms to combine extensive sets of customers' personal data to produce detailed user profiles. Strict requirements for consent to the processing of personal data have little influence on the business models of these huge Internet platforms, because they are in a position to offer their users a convenient universal opt-in for the whole spectrum of digital services they provide. In combination with the lock-in effects generated by their extensive verticalization, digital platforms will thus find it very easy to obtain consent to the processing of personal data. In effect, the draft ePrivacy Regulation would therefore facilitate the concentration of user data in the hands of just a few dominant Internet groups.

The new draft regulation's focus on explicit consent as the key condition for the processing of personal data is further sharpened by the creation of new "gatekeepers". In the future, a central setting in the software with which they access the Internet should allow users to decide whether they consent to the processing of their personal data. Exceptions can be made for individual services, letting users define specific services for which they consent to data processing. How digital services might obtain these exceptions and how any such exceptions are to be reconciled to conflicting central settings is not yet clear. All in all, however, browsers would become powerful gatekeepers for digital services. →CASE 5 That is especially worrying in light of the balance of power among browser providers: The browsers operated by the major Internet platforms currently enjoy a 78% share of the European market. →D

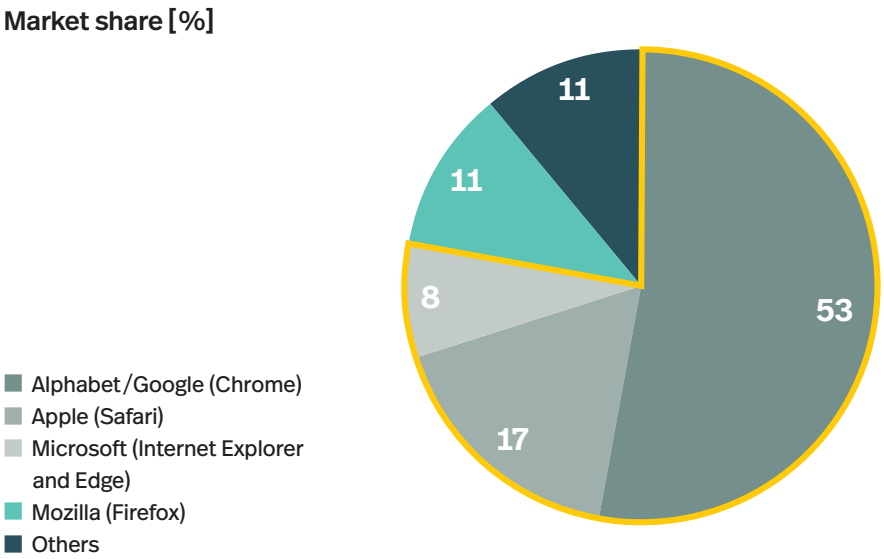
From two sides, the ePrivacy Regulation would hold the European digital economy in a vice-like grip. →E Given the regulation's very broad scope of validity, the whole app economy, numerous IoT applications and all businesses that depend on the ability to process communications data in the context of digitalization would be affected. The mere fact that the scope is so broad is not necessarily a problem. However, the draft ePrivacy Regulation also raises very high barriers to the processing of user data. In focusing on explicit consent, the provisions of the ePrivacy Regulation would deviate from those of the GDPR and adopt a stricter approach to assessment. If the additional obstacles to the processing

11 The Chinese companies Tencent and Alibaba also operate Internet platforms. Although they have hitherto played only a marginal active role in Europe, it is only a matter of time before they, too, penetrate the European market.

of user data foreseen by the draft ePrivacy Regulation are retained in their present form, the European data economy will be unable to realize its growth potential. While digitalization gains traction around the globe, Europe would keep itself from participating.

Especially the development of innovative, data-driven business models and the expansion of forward-looking aspects of IoT such as smart homes and autonomous driving would be slowed down by the regulation. In addition, the ePrivacy Regulation could prompt a shift in the balance of power on the Internet: If the big platform operators use their digital ecosystems to secure opt-ins, they will find it much easier in the future to collect and process personal data than smaller providers of individual online services. Overall, the excessive data minimal-

D Internet dominance: The browsers operated by the major Internet platforms have a 78% share of the European market



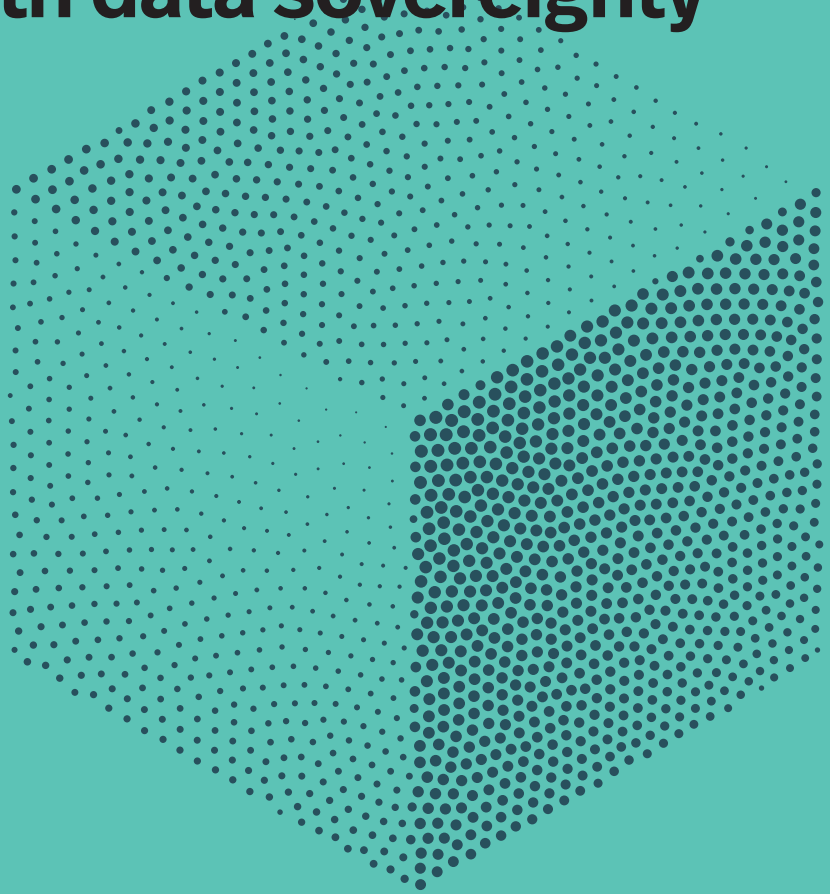
Sources: Statcounter (data from August 2017), Roland Berger

ism resulting from the planned ePrivacy Regulation would thus not only diminish growth opportunities in the European economy: By ceding the advantage to large platforms, it would also weaken privacy in Europe in the long run.

E The economy caught in a vice: The planned ePrivacy Regulation concerns all sectors of the economy and places high barriers to the processing of personal data in companies' paths

Source: Roland Berger

4
WHAT MUST BE DONE NOW:
Building effective privacy with data sovereignty



In economic terms, many European countries are today looking back on a lost decade. The continent's economy is now growing again, though, and brighter prospects are visible in the labor market. To inject further dynamism into Europe's upswing and make sure its economy can stand up to global competition, we now have to put the right conditions in place. Digitalization harbors the greatest potential for higher productivity, better jobs and a more equitable society. It is vital to prevent misguided regulation from blocking our ability to exploit this potential. Yet in its current form, that is precisely what the ePrivacy Regulation proposed by the European Commission could end up doing.

The fundamental problems inherent in the planned ePrivacy Regulation are the result of excessive "data minimalism" aimed at restricting the processing of communications data to the greatest extent possible. This policy deliberately limits opportunities for innovation and undermines citizens' data sovereignty. The scenario targeted by the ePrivacy Regulation should not be the rigid data minimalism reflected in the current draft, but should champion citizens' sovereignty over their own data. To strengthen individual data sovereignty, the planned regulation should therefore empower all citizens to handle their personal data in an informed and autonomous manner. That would reinforce people's digital maturity while at the same time laying a firm foundation for a sustainable Digital Single Market.

The combination of a very broad scope of validity and, in particular, even higher barriers to the processing of personal data than those enshrined in the GDPR means

The ePrivacy Regulation would weaken Europe's economic base.

that the current draft would weaken Europe's economic base. Above all, the proposed ePrivacy Regulation would also leave the European data economy at a disadvantage relative to the major digital ecosystems operated by US platforms. That in turn could lead to further market concentration and put more and more personal data in the hands of a very small number of companies. In this eventuality, the new regulation would actually weaken privacy rather than strengthen it.

To keep that from happening, three key points in the ePrivacy Regulation need to be amended:

1. The ePrivacy Regulation should allow electronic communications data to be processed under the same conditions as the GDPR. These include processing based on legitimate interests and the accommodation of privacy-friendly technologies such as pseudonymization.

2. The ePrivacy Regulation should not transform Internet access software into a new form of "gatekeeper". It must be ensured that no online providers are further obstructed by central privacy settings, as this would make them even more dependent on the dominant Internet platforms and the browsers they operate.

3. The EU Commission's ambitious time frame should be adjusted to provide for a transitional period, giving European firms sufficient time to properly implement the planned regulation.

A legal framework to protect personal data that is harmonized across Europe is an important step toward making the Digital Single Market a reality. That said, we cannot simply look away while digital innovation is hindered by an ill-conceived understanding of data minimalism. Users' interests must not be played off against those of businesses. Instead, it is important to see individual data sovereignty as the basis on which to reconcile the interests of consumers to those of companies that process data. Only then can Europe's Internet economy become more competitive, contribute to our prosperity and develop new offerings that add significant benefits for the customer.

Individual data sovereignty is the basis on which to reconcile the interests of consumers to those of companies that process data.

Imprint

Publishers

Internet Economy Foundation (IE.F)
Uhlandstraße 175
10719 Berlin
Germany
www.ie.foundation

Prof. Dr. Friedbert Pflüger
Chairman

Roland Berger GmbH
Sederanger 1
80538 Munich
www.rolandberger.com

Stefan Schaible
CEO Germany & Central Europe

Authors

Clark Parsons
c.parsons@ie.foundation

Felix Styma
f.styma@ie.foundation

Klaus Fuest
klaus.fuest@rolandberger.com

Dr. David Born
david.born@rolandberger.com

Contact

Clark Parsons
Managing Director
Internet Economy Foundation (IE.F)
c.parsons@ie.foundation
+49 30 8877 429-400

Claudia Russo
Press Officer
Roland Berger GmbH
claudia.russo@rolandberger.com
+49 89 9230-8190

Picture credits

page 1: chaluk/iStock **page 2:** sanchesnet1/iStock **page 6:** amgun/iStock **page 10 and 14:** RGAP/iStock
page 19–22: Olga Korshunova/iStock **page 26:** Samolevsky/iStock **page 31**: Ludmila_m/iStock