Sonderveröffentlichung zu ZD 2017, 251

MALTE ENGELER / WOLFRAM FELBER

Draft of the ePrivacy Regulation from the perspective of the regulatory practice

Is the regulation out of touch with technical reality?

offline-tracking
fingerprinting
over-the-top-services
audience measurement
electronic communication

■ With the draft of a regulation concerning the respect for private life and the protection of personal data in electronic communications, the European Commission has presented a follow-up to the ePrivacy Directive. This paper describes the difficulties encountered so far in implementing the Directive and will explain how the new regulation would affect these practical issues. The authors have come to the conclusion that the extension of the regulation's scope to over-the-top-services, the relation to the General Data Protection Regulation (GDPR), as well as many key principles pose a variety of challenges for enforcement. In particular, the provisions on the processing of communication data, as well as the data protection friendly settings in browsers and apps ignore the technical realities and cast doubt on the enforceability of the draft. This article thus propagates to not only approach the issues from a legal perspective but also to create the technical preconditions necessary to meet its legal demands.

■ Mit dem Entwurf für eine Verordnung über Privatsphäre und elektronische Kommunikation hat die EU-Kommission Nachfolgeregelungen für die ePrivacy-Richtlinie vorgestellt. Der Beitrag stellt die bisherigen Umsetzungsschwierigkeiten der Richtlinie dar und erklärt, wie sich die neue Verordnung auf diese Praxisprobleme auswirken würde. Die Autoren kommen dabei zu dem Ergebnis, dass die Erstreckung auf Over-The-Top-Dienste, das Verhältnis zur Datenschutzgrundverordnung (DS-GVO) sowie viele Kernbegriffe im behördlichen Vollzug vielfältige Herausforderungen mit sich bringen. Vor allem die Regelungen über die Verarbeitung von Kommunikationsdaten sowie für datenschutzfreundliche Einstellungen in Browsern und Apps gehen an den technischen Realitäten vorbei und lassen an der Vollziehbarkeit des Entwurfs zweifeln. Der Beitrag spricht sich daher dafür aus, die Probleme nicht nur rechtlich anzugehen, sondern auch die technischen Voraussetzungen für die datenschutzrechtlichen Forderungen zu schaffen.

I. Introduction

Following the announcement of the General Data Protection Regulation (GDPR) in the Official Journal on 05/04/2016, controllers are now more or less able to prepare themselves for the future legal situation.[1] While the data economy and the data protection authorities are tackling this major task, the next changeover has already been announced. The Directive on privacy and electronic communications (ePrivacy Directive),[2] last revised back in 2009, is also to be replaced by a regulation that, according to current planning, is to come into force simultaneously with the GDPR in May 2018[3]. The final draft[4] of the *European Commission* on a regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation) has been published in January 2017. The ePrivacy Regulation promises to bring challenges that will be equally large if not much larger than the GDPR's. This is partly due to the fact that the timetable with regard to the planned ePrivacy Regulation is much stricter, not to say ambitious. There are merely 17 months between the Commission's draft and the planned date of entry into force. In addition, the subject of the regulation is an area that is intrinsically linked to the processing of data: electronic communications. With its connecting to virtually any electronic communications data, even in the communications between machines, the draft aims at nothing less than dressing to Internet as such in a new guise of privacy.

It is therefore to be expected that the struggle over the not yet finalized content of the ePrivacy Regulation will turn out to be even more dramatic than it was the case with the GDPR. Instead of wide and in doubt flexible guidelines, the current draft addresses area-specific processing operations such as web analytics, offline tracking or cookies. Interest groups and the digital advertising industry have already voiced their fear of overly restrictive guidelines.[5]

Anyone who views the *Commission's* current draft of the ePrivacy Regulation only as a scourge for the digital economy and blessing for data subjects, underestimates the many and various

1 OJ EU L 119, p. 1,. 4.5.2016; some uncertainty is caused by a draft of the *Federal Government* for a data protection amendment and implementation law ("Gesetzentwurf der *Bundesregierung* für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU"), BT-Drs. 18/11325; s. also press release of the *independent data protection authorities of the federal states* (*Unabhängigen Datenschutzbehörden der Länder)*, 1.2.2017, available at: https://www.datenschutz.de/entwurf-zum-bundesdatenschutzgesetz-verspielt-chanceauf-besseren-datenschutz/; *Albrecht/Wybitul*, ZD 2017, 51; *Helfrich*, ZD 2017, 97; opinion of the *Federal Council* (*Bundesrats)*, BRDrs. 110/17.

2 Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications (Electronic Communications Data Protection Directive), last amended by the Directive 2009/136/EC.

3 Art. 27 of the ePrivacy Regulation (E).

4 Proposal for a regulation of the European Parliament and of the Council on respect for privacy and protection of personal data in the electronic communications and repealing Directive 2002/58/EC (Privacy and Electronic Communications Regulation), COM(2017) 10 final.

5 *Bitkom*, Initial assessment of the Commission's draft of the ePrivacy Regulation ("Erste Einschätzung zum Kommissionsentwurf der e-Privacy-VO"), available at: https://www.bitkom.org/noindex/Publikationen/2017/Positionspapiere/20171402-Erste-Einschaetzung-Bitkom-e-PrivacyFIN.pdf; *Schulz*, The end of the cookie-chaos? ("Ende des Cookie-Chaos?"), available at: https://www.bevh.org/blog/blog-post/2017/01/16/ende-descookie-chaos-drei-thesen-warum-der-entwurf-fuer-eine-eu-eprivacy-verordnung-aus-der-z/.

challenges that the implementation of the current draft would impose on the regulatory practice. With the help of a few examples, this article will describe the problems that the administrative implementation of the current draft would bring. It will also explore the relevant opinion of the *Article 29 Data Protection Working Party*[6], as well as the specific German situation with its existing regulatory landscape and federal supervisory structure.

II. Practical problems in the implementation of the previous ePrivacy Directive

The ePrivacy Directive already had a vivid past with regards to its implementation in Germany. The most prominent example is certainly the (non-)implementation of Art. 5 (3) of the ePrivacy Directive, which states that any cookie, aside from a few exceptions, may only be placed with the consent of the users. The *Federal Government* had always pointed out to the *EU Commission* that this provision did not require implementation in German law as the German Telemedia Act (Telemediengesetz, TMG) allegedly already complied with the requirements of the Directive.[7] However, both the literature[8] and the data protection authorities[9] criticized an implementation deficit as Art. 5 (3) of the ePrivacy Directive is applicable to any kind of cookies. However, Sec 15 (3) 1 of the TMG only covers the processing of personal data. Therefore, in many parts of Europe information and consent banners were indeed regularly required for the use of cookies, whereas only an opt-out solution, within the context of Sec. 15 (3) 81) of the TMG, was often used in Germany. Despite their criticism, the data protection authorities did not take action against website operators who exclusively complied with the guidelines of the TMG but not the stricter ePrivacy Directive. An immediate application of Art. 5 (3) of the ePrivacy Directive would have led to difficult questions regarding state driven intervention on the basis of non-implemented European law.[10]

For a long time, another 'classic' topic in the discussions regarding the eprivacy Directive was the question whether the ePrivacy Directive should also be applied to services that, since the end of the 1990s, have been developed into functional equivalents and alternatives which are increasingly replacing traditional telecommunications services such as the short messaging service (SMS) and number-based telephony. Although the ePrivacy Directive already clearly wanted to capture every form of electronic communications, for several reasons there was still a distinction between telecommunications and content services. This resulted in IP-based services such as messengers, chat applications, and communication apps not being subject to the regulatory regime of the telecommunications law but rather being treated as telemedia. In some cases and relatively early on, several data protection authorities of the German federal states classified the so-called over-the-top (OTT) services as telecommunications services within the meaning of the Telecommunications Act (Telekommunikationsgesetz, TKG) and referred the relevant cases to the *Federal Commissioner for Data Protection and Freedom of Information* (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI*) as the competent authority.[11] It is unknown, if there have been any supervisory procedures of the *BfDI* against OTT services such as *Skype* or *WhatsApp*. Moreover, the supervisory and control powers of the data protection authorities of the federal states and the federal government, which are not harmonized under the Data Protection Directive[12] make it difficult to ensure uniform enforcement of the provisions of the ePrivacy Directive.[13]

The discussion is additionally fuelled by the processing meta data in order to protect telemedia from technical errors or abusive use. Sec. 100 (1) of the TKG permits the use of such data[14] to the extend necessary in order to detect faults, errors and misuse or to prevent interference with availability. The TMG on the other hand is lacking such a provision to this day. Even though those responsible for telemedia are required to take technical measures to protect personal data or to prevent errors according to Sec. 13 (7) of the TMG. It is still unclear whether this obligation should be considered as legal basis for the processing of personal data at the same time.[15] Only now the *CJEU* has clarified with its judgement on Breyer that Art. 7 (f) of the Directive 95/46/EC (DPD) may constitute a legal basis for the processing of IP addresses to secure telemedia.[16]

III. The new provisions of the draft of the ePrivacy Regulation from a regulatory perspective

At first, the draft of the ePrivacy Regulation seems to provide a solution for some of the above-mentioned problems. As a directly applicable regulation, there is no need to argue about the possible lack of or differences in implementation, the legal bases hardly differ between telecommunications and telemedia anymore, and with the explicit inclusion of certain OTT services the allocation of responsibilities between the regulatory authorities in this regard also seems to be close to a solution.

However, the draft raises a large number of new issues. The subject matter of the regulation, the delimitation from the GDPR and the key terms used, as well as the regulatory objectives of many legal bases make the consistent application in administrative practice rather questionable.

1. Conflicting subject matter of the regulation

The draft[17] defines its objectives in Art. 1 as „protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services", respect for the „rights to respect for private life and the communications" and „protection of natural persons with regard to the processing of personal data". In that regard, the draft is in accordance with the ePrivacy Directive. Once again, however, the question arises as to how a regulation based on these objectives

6 *Article 29 Data Protection Working Party*, WP 247, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

7 *EU-Commission*, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive, COCOM11-20, with answers from the *Federal Government*, available at: https://www.telemedicus.info/uploads/Dokumente/COCOM11-20QuestionnaireonArt. 53e-PrivacyDir.pdf.

8 [1] *Rauer/Ettig*, ZD 2015, 255; *Schneider*, Telemedicus,. 11.2.2014, available at: https://www.telemedicus.info/article/2722-Die-Stellungnahme-der-Bundesregierung-zur-Cookie-Richtlinie.html; *Schleipfer*, RDV 2011, 170.

9 Decision of the *data protection conference of the federation and the federal states* regarding the tracking of user behaviour in the internet („Entschließung der *Datenschutzkonferenz des Bundes und der Länder* zur Verfolgung des Nutzerverhaltens im Internet)", available at: https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9759.de.

10 [1] *CJEU*, NJW 1994, 2473, 2474; for a possible regulations-compliant interpretation of the TMG s. *Moos*, K&R 2012, 635.

11 [1] 25. Activity report by the *Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI)* 2014/2015, p. 133 f., available at: https://www.datenschutz-hamburg.de/uploads/media/25_Taetigkeitsbericht_Datenschutz_2014-2015_HmbBfDI_01.pdf.

12 Directive 95/46/EC (DPD)on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

13 The *Federal Commissioner for Data Protection (BfDI)* has not yet been able to refer to Sec. 38 (5) BDSG.

14 The TKG adresses usage data under the term "traffic data".

15 *Schmitz*, in: Hoeren/Sieber/Holznagel (Hrsg.), Hdb. Multimedia-Recht, part 16.2, margin note 206 et seqq.; *Spindler/Nink*, in: idem/Schuster (Hrsg.), Recht der elektronischen Medien, 3. ed. 2015, TMG § 13 margin note 28.

16 *CJEU* ZD 2017, 24 s. note *Kühling/Klar* = MMR 2016, 842 s. note *Moos/Rothkegel; Weinhold*, ZD-Aktuell 2016, 05366.

17 All information without legal reference refers to the draft of the ePrivacy Regulation.

can distance itself so freely in the further process from issues of privacy and private life. While Art. 8 of the draft includes any form of access to data-related activity in the user's end device without exception, and the draft even addresses machine to machine (M2M) communications,[18] the scope of application is extended far beyond the protection of personal data. Thereby, the draft exceeds the limits of its own objectives losing its legitimacy under Art. 16 Treaty on the Functioning of the European Union (TFEU). However, if all draft provisions were measured against their relation to personal data, the extent of many rules would reduce dramatically. Finally, not every data processing affects the scope of protection of the right to free development of personality, neither within the meaning of Art. 7 of the EU Charter of Fundamental Rights nor within the meaning of the general right of personality under Art. 2 (1) in connection with Art. 1 (1) of the German Constitution (Grundgesetz, GG).[19]

Of course, a broad understanding of the term "identifiable" could again include many electronic and machine-to-machine communications data under the protection of personal rights.[20] However, the draft does not seem to have this objective in mind since it rarely alludes to personal data in the prerequisites of the individual legal bases. The provisions in the current draft therefore have a certain tendency to exceed their fundamental rights basis.[21]

In practice, this will lead to considerable uncertainties in the regulatory enforcement. The orders of data protection authorities typically interfere with freedom of action (Art. 2 (1) GG) or freedom to practice any occupation (Art. 12 (1) GG) of the addressees and must always be verified in each case with respect to their proportionality. For this, the administrative acts of the authorities must first and foremost always pursue legitimate objectives and take appropriate means to achieve them. However, the enforcement of rules that do not build on the processing of personal data is hardly a suitable means for the protection of the general right of personality.

To be applicable the current Proposal would require interpretation of the individual provisions in the light of Art. 1. Individual measures by authorities would have to be checked if they are related to personal data. This means that the current Proposal will keep up the discussion on the question when an information is related to an identified or identifiable person as this will be the key factor. All this is further complicated by the fact that European law considers the protection of the right to private life (Art. 7 of the EU Charter of Fundamental Rights) and the right to protection of personal data (Art. 8 of the EU Charter of Fundamental Rights) as different protective scopes.[22]

2. Unclear relation to the GDPR

Many practical problems will be caused by the relationship between the ePrivacy Regulation and the GDPR. The ePrivacy Regulation should be lex specialis for the GDPR and should „particularise and complement" it.[23]. It should not „lower the level of protection" in relation to the GDPR[24]. Following the rules for the elimination of conflicts between general and more specific provisions[25], the draft shall take precedence whenever it explicitly regulates the issues. The general rules of the GDPR on the other hand shall apply wherever the draft does not provide any regulations.

The principle of lex specialis[26] may seem familiar but it has already led to difficulties in the past regulatory practice. The *Higher Administrative Court of Schleswig-Holstein*[27] had, for example, affirmed a blocking effect of the state civil servant act compared to the data protection act of *Schleswig-Holstein*. By doing so, the court contradicted the *supervisory authority of Schleswig-Holstein*[28] represented in the proceedings which did not assume a blocking effect. Yet, the same regulatory authority did on another occasion assume such a blocking effect with regard to the competition of a regulation of the German Banking Act[29] (Kreditwesengesetz, KWG) and the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). Both cases show how prone to conflict the principle of lex specialis is. It will also lead to discussions with regard to the ePrivacy Regulation draft.

Data processing on behalf of another is, for example, not explicitly regulated in the current version of the draft. Following the principle of lex specialis, one would assume that the general rules of the GDPR apply. Art. 4 (1) Sup-para. 1 indeed does contain reference to general definitions, including definitions of the controller and the processor in Art. 4 Sub-para. 7 and 8 of the GDPR. This would mean that companies whose services fall within the scope of the ePrivacy Regulation would naturally also have to be assessed as processors, provided that they act on behalf of another controller.[30] The ePrivacy Regulation does not specify further whether a data processing agreement according to Art. 28 of the GDPR must also be concluded as a result of this classification. In the German discussion, it has become generally accepted that such a contractual or binding agreement is not required when it comes to the area of telecommunication. As a justification, it is generally pointed out that the obligation to follow instructions,[31] which is a constituent for data processing on behalf of another, is incompatible with the obligation to observe telecommunications secrecy.[32] In practice, this would be particularly relevant as a violation against the formal obligations of Art. 28 of the GDPR pursuant to Art. 83 (4) lit. a of the GDPR is subject to sanctions.

While the lex specialis principle would initially suggest that Art. 28 of the GDPR applies as a general provision in the absence of specific provisions in the ePrivacy Regulation, this can only apply if there is no evidence to suggest that the provisions of the ePrivacy Regulation for data processing on behalf of another are conclusive. Still, such a point could now be made because the ePrivacy Regulation on some occasions does not only declare the definitions of the GDPR applicable, but also explicitly refers to the additional requirements themselves. With regard to consent, for example, in addition to the definitions in Art. 9 (1) of the GDPR, the draft also expressly refers to the further require-

18 Recital 12 of the ePrivacy Regulation (E).
19 *Bock/Engeler*, DVBl 2016, 593, 595.
20 The controversial concept of personal data has gained even more ambiguity by virtue of the recent judgment of the *CJEU* (s. footnote 16 above).
21 The *Article 29 Data Protection Working Party* (s. footnote 6 above), para. 9, 40f, 40h, welcomes this expansion with a view on the relevance of machine communications for the privacy of persons concerned but calls for urgently needed clarification with regard to the overlap of privacy reference and linking to a particular person, on the one hand, and the individual provisions of the draft, on the other hand.
22 *Bock/Engeler*, DVBl 2016, 593, 595.
23 Recital 5 of the ePrivacy Regulation (E).
24 Recital 5 of the ePrivacy Regulation (E).
25 Inter alia *Vranes*, ZaöRV 2005, 391 incl. further evidence.
26 *Vranes* (s. footnote 25 above).
27 *Higher Administrative Court (OVG) of Schleswig-Holstein* ZD 2016, 545.
28 Schleswig-Holstein Parliamentary Printing Matter (SHLT-Drs.) 18/4198, p. 2.
29 35. Activity report of the *independent state center for data protection Schleswig Holstein (ULD)*, SHLT-Drs. 18/2730, section 5.7.1; in contrast with *Hilpert*, ZD 2015, 259.
30 To the realignment of data processing on behalf under the GDPR *Engeler*, Telemedicus v. 24.11.2016, available at:
https://www.telemedicus.info/article/3150-Die-Auftragsdatenverarbeitung-braucht-ein-Reboot-mit-der-DSGVO-in-derHauptrolle.html.
31 Other authors argue that the obligation to follow instructions is not a prerequisite of processing on behalf of another but merel a legal consequence of third-party involvement, *Engeler* (s. footnote 30 above).
32 *Local court (AG) Meldorf* ZD 2012, 144 (Ls.) = NJW-RR 2012, 186; *Spoerr*, in: Wolff/Brink (Hrsg.), BeckOK DatenSR, BDSG § 11 margin note 27; *Geuer*, ZD 2012, 515.

ments of Art. 7 of the GDPR. This clarification would be superfluous if Art. 7 of the GDPR was applicable as lex generalis anyways. This clarification would only make sense if, conversely, it were to be concluded that it should be read as an exception to an otherwise intended blocking effect. Wherever the rules of the GDPR are not explicitly referred to, it would then have to be deduced from the silence of the ePrivacy Regulation that additional legal consequences not explicitly referred to would be suppressed for lack of explicit reference. The obligation to observe the formal requirements of data processing on behalf of another according to Art. 28 of the GDPR would therefore be blocked by the current draft.

This conflict is also likely to be relevant in the absence of a reference to Art. 25 of the GDPR. Apart from a reference in Recital 25, the draft refrains from specifically referring to the provisions on privacy by design and privacy by default provided in Art. 25 of the GDPR. Once again, it should be clarified whether the provisions of Art. 25 of the GDPR should be regarded as lex generalis or the ePrivacy Regulation should be regarded as conclusive. This would result in Art. 25 of the GDPR not being applicable to the processing of data with regard to the provision and use of electronic communications services. The latter view would then have to withstand the justified objection that the level of protection afforded by the GDPR would be undermined, but it would have arguments regarding the legislative systematics and intention on its side.[33]

3. Lack of precision in core terms

The draft aims to include OTT services in its scope of application „in order to reflect the market reality", as it is stated in its explanatory statement. These are „conventional transmission services... functionally equivalent online services such as VoIP telephony, messaging and web-based email services", i.e. the OTT services that fall under the category of OTT1.[34] They will henceforth be covered by the definition of electronic communications services laid down in the Directive of the European Parliament and Council on the European Electronic Communications Code. It is questionable how it should be dealt with the services of category OTT2, i.e. all those services that can no longer be regarded as interpersonal communication but are based on classical data transmission of communication networks in the same way. In many respects, music streaming or on-demand video platforms use data processing similar to the OTT1 services, analyze customer usage patterns based on metadata and improve their own services by audience measuring. However, they are not covered by the draft directly but by a broad interpretation of the terminus „interpersonal communication services" in Art. 4 Para. 2 only by a broad interpretation of the concept of interpersonal communication services.[35] In practice, the interpretation of these terms of reference could inevitably lead to discussions.[36] The recent discussion about Xabber clients shows which pitfalls lie in the distinction between OTT categories 1 and 2.[37]

Art. 6 of the draft takes up more terms that are already controversial in the German discussion. Similar to Sec. 100 (1) TKG, Art. 6 (1) lit. b announces the processing of communications data to be admissible, insofar and as long as it is necessary or required „to maintain or restore the security of electronic communications networks and services or to detect technical faults and/or errors in the transmission". The critical issue of the duration that can be considered necessary is left open by the draft. This issue[38] that has been brought before German courts several times before will therefore stay unsolved.

The storage for the purpose of ensuring „continuity" should not be hindered either.[39] In German law, there is a similar requirement in Sec. 100 (1) 2 TKG, which is understood as the basis for fighting spam and bot traffic.[40] However, the draft does not explain to what extent unpleasant network traffic burdening the capacity of the communications systems, for example, in the form of spam emails, should be included. So, it remains unclear in which cases the operators should be allowed to identify, filter and block network traffic for the benefit of efficiency maximization. The draft leaves it to the data protection authorities once again to face this discussion with operators and service providers. Similarly, the *Article 29 Data Protection Working Party* calls for clarification in this respect and recommends the inclusion of the possibility to object to such filtering.[41]

Finally, the draft also remains unpleasantly vague on the issue of the misuse of services. According to Art. 6 (2) lit. b, electronic communications metadata may be processed if this is necessary for the detection of abusive uses. In this regard, cases have already been discussed in regulatory practice where in the interest of mobile phone operators third parties tried to identify customers who used flat-rate tariffs to an unusually high extent. Together with other characteristics, such behavior was considered by some as an indicator of abusive behavior and the operators had to be informed accordingly. However, conduct that is in compliance with a contract and simply exhausts contractually guaranteed positions to the maximum should not fall under the term of abuse. The draft does not provide any clarification, though.[42] It is to be expected that the competent authorities will once again have to determine by means of interpretation which usage behavior may ultimately be classified as abusive. The opinion of the *Article 29 Data Protection Working Party* is not very productive in this respect. It barely touches the issue. [43]

4. Legal bases without clearly recognizable legislative intention

In addition to the legal prerequisites of the respective provisions, on which the regulatory practice must build on, the ambiguous legislative intention of the individual provisions will also present a challenge. Art. 8 and 10 of the draft clearly show that the current draft is not able to communicate which regulatory objective is being pursued.

a) Art. (1) of the ePrivacy Regulation draft

Art. 8 (1) first of all chooses the broadest possible approach with regard to its regulatory scope. The legislator assumes that, in principle, any data, any hardware component, and any process

33 Recital 23 of the ePrivacy Regulation (E).

34 S. the different OTT categories of the *Article 29 Data Protection Working Party*, WP 240, Opinion 03/2016 on the evaluation andr eview of the ePrivacy Directive (2002/58/EC); *Scientific workgroup for regulation issues (Wissenschaftlicher Arbeitskreis für Regulierungsfragen, WAR) of the Federal Network Agency (BNetzA)*, Questions regarding the regulation of OTT-communication services ("Fragen der Regulierung von OTT-Kommunikationsdiensten"), available at: https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/WAR/Stellungnahmen/Stellungnahme_OTT.pdf.

35 Accordingly, services that "permit interpersonal and interactive communication only as [a] secondary function inseparably linked to another service" are also covered by the term.

36 The *Article 29 Data Protection Working Party* (s. footnote 6 above), para. 9, incl. further evidence, considers only some of the OTT2 services to be included and also points out that the distinction between the individual OTT categories is not a legal term.

37 S. *Telle*, Telemedicus v. 25.3.2017, available at: https://www.telemedicus.info/article/3182-Will-die-BNetzA-jetzt-Apps-regulieren.html.

38 Regarding the seven-day storage of dynamic IP addresses see German Federal Court of Justice, in: *BGH* ZD 2013, 614.

39 Recital 16 of the ePrivacy Regulation (E).

40 *Büttgen*, in: Hoeren/Sieber/Holznagel (s. footnote 15 above), part 16.3, margin note 116 et seqq.

41 *Article 29 Data Protection Working Party* (s. footnote 6 above), para. 18.

42 Cf. *Büttgen* (s. footnote 40 above), margin note 112 et seqq.; *Braun*, in: Beck'scher TKG-Komm., Sec. 100 margin note 24 et seqq. incl. further evidence

43 Opinion, para. 18.

in the end devices can be a potential infringement of the privacy of end users. The draft relies significantly on the assumption that modern tracking and profiling tools are no longer based solely on data such as cookie-IDs and IP addresses but that the most inconspicuous machine data can potentially also be part of an invasive procedure.[44] Accordingly, Art. 8 (1) of the draft places all „information from end users' terminal equipment" under a general ban on processing. Irrespective of the fact that it is problematic how much this approach moves away from a relatability to identifiable natural persons, the individual legal grounds will lead to disputes in practice.

Without exception and apart from consent, all individual legal grounds within Art. 8 (1) of the draft build on the concept of necessity. Whereas in the context of contractual obligations the required level of data processing follows the negotiated content of the contract,[45] the current technical communications standards already unilaterally determine which data has to be transmitted by end users. It is simply not possible to access a website or connect to a server of a messaging app without, for example, obtaining the IP address of the requesting end device. In addition, browsers, end devices, and clients send even more (meta)-data to the contacted servers, such as the browser version, the operating system used or installed plug-ins, based on the prevailing technical standards.[46]

Despite this, Art. 8 (1) of the draft demands that data may only be collected and processed if it is necessary „for carrying out the transmission of an electronic communication" (lit. a), „for providing an information society service requested by the end user" (lit. c), or for „ web audience measuring" (lit. d). This way, the draft tries to retroactively impose a (so far) foreign component of data minimization[47] on an infrastructure that is focused on maximum availability and integrity. In any case, these requirements of the draft cannot be implemented without adjustments to the technical foundations of the Internet itself.[48] For this reasons, Art. 8 (1) of the draft can only be interpreted in such a way that it prohibits further processing but not initial collection with regard to those data that are already prescribed by Internet and network protocols. Otherwise Art. 8 (1) of the draft would practically prohibit the participation in network traffic. This interpretation would also take into account the fact that although the collection of personal data constitutes an interference with fundamental rights in itself, the particular intensity often lies in the further processing (e.g., fingerprinting and profiling).

However, even considering such a narrow interpretation of Art. 8 (1) of the draft, it would remain problematic to reach a consensus on what is „necessary" to offer or use communications and other Internet services today. While some consider all available (additional) techniques to be necessary[49] in order to offer a modern, responsive and visually appealing service, others would be more than satisfied with a solution that is visually and technically reduced to the bare essentials. Without objective criteria, the concept of necessity thus remains too vague. Additionally, as indicated in the Recitals to Art. (1), the draft does not even consistently upholds this narrow scale itself. With regard to lit. c and d of the German language version, it reintroduces the elements of a proportionality assessment and declares that access to cookies for the purpose of audience measurement is a „legitimate and useful tool", while the English language version seems to apply an even more strict standard of „strictly necessary".[50] The confusion surrounding the future legality of the processing of data on the Internet is thus complete.

This uncertainty may ultimately lead to the providers of websites, apps and communications platforms not relying on the statutory permissions but – where possible – solely on obtaining the user's consent in accordance with Art. 9.[51] Thus, Art. 8 (1) of the draft could do a disservice to the aim of curbing the rampant flood of information and consent banners known as „banner fatigue".

b) Art. 8 (2) of the ePrivacy Regulation draft

A similar contradiction between technical reality and legal regulation is evident in the subject of offline tracking. In department stores, on the roads and in public areas in general, active radio connections of mobile devices belonging to pedestrians and road users are recorded in order to be able to make statements about visitor and traffic flows or personal interests of individuals. The subject of offline tracking has been a topic of concern for data protection authorities for years.[52] However, there is still no answer to the question of whether it is legally permissible and, if so, on what legal basis the data, that is actually being sent by the end devices only to establish a communications connection for the purposes of offline tracking, can be used. While a broad spectrum of approaches has been previously represented in the German discussion,[53] there is a lack of a clear positioning in Art. 8 (2) of the draft. Instead, all that is required of controllers is to „display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter ... and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection „.[54]

A confident judgment can hardly be made on the enforceability of this standard as it is often practically impossible to prevent the collection of MAC addresses of WLAN and Bluetooth components by surrounding receivers unless you turn off the function or even the device itself.[55] This shows that the regulations of the Commission's draft, with its obligation to notify of countermeasures, do not live up the technical reality. In addition, the fluctuating reach of WLAN networks makes it hardly possible to cover the respective areas with signs. Notices on entrance doors to turn off one's phone will also hardly meet the interests of department store operators and their customers. Ultimately, the real problem here, too, is that the technologies to be regulated have never been designed to provide the user with a particular degree of ability to intervene. Instead, the current WLAN and Bluetooth standards are primarily aimed at establishing a connection to the respective communications partners as effectively and reliably as

44 Recital 20 of the ePrivacy Regulation (E).
45 S. Art. 6 para. 1 lit. b GDPR.
46 The so-called "browser fingerprint"; when using Java script, even more metadata may be transferred (screen resolution, installed fonts etc.).
47 Alternative designs for a more privacy-friendly network are available, cf. e.g. *Kühne*, FIfF-Kommunikation 7/16, 46.
48 A standardization focused on data protection principles would be required in order to be able to work out what can actually be seen as necessary out of the large number of data in electronic communications.
49 Examples include graphically accelerated rendering of web pages or running certain scripts.
50 Recital 21 of the ePrivacy Regulation (E).
51 Those who, for example, assume that the clear characteristics of a graphic chip (cf. footnote 49) should already be prohibited pursuant to Art. 8 para. 1 of the draft as personally identifiable data would have to make the hardware-accelerated rendering of individual parts of the website subject to prior consent in the case of a narrow requirement scale.
52 Report of the *Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit)* dated 12/31/2015, Chapter 11.8.2, p. 182.
53 The processing of MAC addresses for offline tracking, as the use of publicly available data, could be, for example, subject to the permission under Sec. 28 para. 2 sentence 1 no. 3 BDSG to be justified by the general weighing of interests under Sec. 28 para. 1 sentence 1 no. 2 BDSG or always require consent.
54 Recital 25 of the ePrivacy Regulation (E).
55 Depending on the operating system and settings, the WLAN module of many smartphones sends out the so-called "probe requests" even when deactivated.

possible. This conflicts with the objective of data protection law to guarantee a sufficiently high degree of unlinkability.[56] Without the adjustment of the underlying technical standards, such as the implementation of a wireless standard used exclusively for offline tracking, which could be controlled separately, only the active consent of the end user remains a legal basis. However, even the *Article 29 Data Protection Working Party* itself was not ready to take this step.[57]

c) Art. 10 (1) of the ePrivacy Regulation draft

Finally, the draft addresses the present situation of end-users being „overloaded with requests to provide consent through so-called cookie banners"[58] due to the current legal situation[59]. Therefore Art. 10 (1) of the draft requires internet access software to provide settings that allows end users to prevent „third parties from storing information on the terminal equipment... or processing information already stored on that equipment". Even though such a feature (ban cookies[60]) is already provided by current web browsers for desktop computers, not all users are aware of it and the given default presets differ.

In the draft's previous version[61] from December 2016, Art. 10 was captioned with „privacy by default"[62] and provided that all components of terminal equipment and Internet access software should be configured by default in such a way that the storage and processing of information on the user's end devices by third parties is prevented. The current draft's version, on the other hand, shifts the decision about whether cookies should be stored and later be accessed by third parties back to the end users. This is a renunciation of the principle „data protection by default" which is provided for by Art. 25 (2) of the GDPR. This makes the practical application of Art. 10 (1) problematic not only due to the above-mentioned competition with the GDPR[63] but with regard to the drafts declared intention of not lowering the protection standard of the GDPR.[64]

It also is not clear what types of software should be included as required by Art. 10 of the draft. Neither the recitals nor the explanatory statement preceeding by the draft give a conclusive answer to this question. As part of the prior consultation with stakeholders[65], the citizens and public authorities surveyed expressed their support for obliging the „manufacturers of terminal equipment" to bring „products with standard settings for the protection of privacy" onto the market. The current draft, in contrast, obliges „software providers permitting electronic communication, including the retrieval and presentation of information on the internet".[66] This definition first of all is suited for classical web browsers, which the draft also explicitly mentions several times in the recitals.[67] Due to the fact, that they are in a „gatekeeper position", they should be build to help „end-users to prevent information from their terminal equipment ...from being accessed or stored „.[68] Smartphones and tablets are only mentioned as further examples for terminal devices in an additional comment in brackets.[69] However, in the case of mobile devices, the pre-installed or user-loaded, installed and executed application programs (apps) are becoming at least as important as the web browsers of the mobile operating systems that are also available there. However, most of the apps certainly do allow „the retrieval and presentation of information on the Internet" so that they can be considered as software in the sense of Art. 10 (1) of the draft.

Nevertheless it is questionable how the obligations as described before should be implemented in apps. In the preparation of the draft, the focus was obviously on classic „cookies" as they are used in web browsers on desktop computers. Still, „cookies" are not used in the same manner on mobile operating systems. Text files that can be used as unique identifiers for tracking purposes can also be stored in and read out from the applications designated storage area. However, settings for this are very often not available in apps. In addition, the data is far from being as easily accessible for end users as with desktop computers, and the actual data flows of the apps are also hidden from end users as far as possible. In addition, there are a number of unique identifiers[70] on the operating system level in the mobile area that the apps can access. The use of apps on mobile end devices as well as web browsers on desktop computers therefore presents a similar risk of tracking the online behavior of end users. Different and specific measures are required to mitigate this risk. Appropriate measures for desktop computers cannot simply be transferred to the mobile sector.

Art. 10 of the draft will therefore raise many questions regarding the implementation of the requirements by the providers of Internet access software. At the same time, the data protection authorities will find it far from easy to enforce the fines imposed by the requirements of Art. 10 of the draft.

IV. The question of enforcement competence

The enforcement of the ePrivacy Regulation must be delegated to the same authorities responsible for the enforcement of the GDPR.[71] What raises few questions in the mostly centralized data protection supervision of the other Member States[72] inevitably calls for clarification in the federal structure of data protection supervision in Germany.

The current distribution of responsibilities of data protection supervision is generally governed by Art. 83 et. seqq. GG. In the absence of other provisions in the sense of Art. 84 GG, the federal states have so far executed the BDSG as a matter of their own in accordance with Art. 84 (1) 1 GG and have decided on the specific structure of the data protection authorities in accordance with Sec. 38 (6) BDSG. For the same reasons, the enforcement competence of the data protection authorities of the federal states includes the area of telemedia (TMG). On the other hand, the German legislature has made use of its legislative power pursuant to Art. 86 GG with regard to the enforcement of the data protection provisions for telecommunication data

56 For an introduction to the protection objects of data protection see *Bock/Meissner*, DuD 2012, 425.

57 Instead, the opinion of the *Article 29 Data Protection Working Party* (s. footnote 6 above), para. 17, requires an effective possibility of objection as well as tight time and local limitations, without clarifying the resulting technical problems.

58 For the lack of the implementation of the so-called "cookie policy", s. inter alia *DSK*, Decision of the *data protection conference of the federation and the federal states* regarding the tracking of user behavior in the internet ("Entschließung der *Konferenz des Bundes und der Länder* zur Verfolgung des Nutzerverhaltens im Internet"), available at: https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9759.de.

59 Recital 22 of the ePrivacy Regulation (E).

60 The draft discusses tracking cookies.

61 Available under: http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf.

62 Now: "Information and privacy settings to be provided".

63 S. Section III.2 above.

64 Recital 5 of the ePrivacy Regulation (E).

65 Consultation with stakeholders, paragraph 3.2 of the justification of the ePrivacy Regulation (E), available at: https://ec.europa.eu/digital-single-market/news-redirect/37204.

66 Recital 8 of the ePrivacy Regulation (E).

67 Recitals 22 and 24 of the ePrivacy Regulation (E).

68 Recital 22 of the ePrivacy Regulation (E).

69 Recital 22 of the ePrivacy Regulation (E).

70 E.g. advertising ID, IMEI, UDID, etc.

71 Recital 38 of the ePrivacy Regulation (E).

72 The Opinion of the *Article 29 Data Protection Working Party* simply states that it is useful if the enforcement of the GDPR and the ePrivacy Regulation is exercised by the same authorities, Opinion, para. 5.

(TKG) and with the *BfDI* has created a federal authority[73] that acts as the data protection supervision for telecommunications companies pursuant to Sec. 115 Para. 4 TKG.

Both the data protection regulations of the TMG and the TKG will now be superseded by the primacy of application regarding the ePrivacy Regulation.[74] Initially, this has no direct influence on the question of enforcement responsibility because the draft primarily contains substantial regulations and does not provide for any procedural obligations for enforcement. In accordance with Art. 291 (1) of the TFEU, the decision as to which national authorities should enforce the EU law rests with the respective Member State. The only requirement is that the application must lead to effective enforcement of the European law. Therefore, it is not of any importance whether certain parts of the ePrivacy Regulation are more similar to sections in the TMG or the TKG. Art. 10 of the draft for example would not automatically be subject to the enforcement competence of the Länder because it happens to have similarities to the old Sec. 15 (3) TMG. Instead, according to the prevailing opinion, the provisions of Art. 83 et seqq. GG are applied analogously to the enforcement of the EU law.[75] Therefore, the decision that will be made by the German legislaor will be decisive for the question of enforcement. Without an accompanying German legislator, the enforcement of the ePrivacy Regulation would initially be left to the federal states, including with regard to the processing of personal data by companies that provide telecommunications services in the sense of Sec. 3 Sub-para. 6 TKG.

Without an activity of the legislator, the existing Sec 115 (4) TKG would not be applicable to the telecommunications-specific requirements of the ePrivacy Regulation as the guidelines for the processing of personal data regulated in the current draft must take precedence over the data protection regulations of the TKG. Sec. 115 (4) TKG would therefore have to include the enforcement of parts of the ePrivacy Regulation. A federal law would thus be necessary in any case. Such federal legislation would be possible by virtue of the exclusive legislative competence of the Federation pursuant to Art. 73 (1) Sub-para. 7 GG. The German legislator could attempt to include only those areas of the ePrivacy Regulation in a new Sec. 115 (4) TKG that would be normally assigned to the telecommunications sector, or transfer the entire enforcement of the Regulation to the competence of the *BfDI*. Regardless of what the distribution of responsibilities will look like in the future, an interaction between the *Federal Network Agency* (*Bundesnetzagentur*, *BNetzA*) and the data protection authorities will remain necessary in any case according to Art. 18 (2), which is also welcomed by the *Article 29 Data Protection Working Party.*[76]

V. Results and outlook

The authors of the ePrivacy Regulation are facing a difficult task. They must create a regulatory framework which, in view of the technical development of the regulatory subject matter, needs to offer the necessary flexibility to ensure that it is not outdated soon. This lack of clarity automatically is at the expense of the enforceability of the adopted regulations.[77] However, this conflict is particularly virulent in the current draft of the ePrivacy Regulation because it is evidently lacking a clear idea of the technical issues it aims to adress. Not only a struggle with the requirement of legal certainty is a recurring theme of the draft, but above all a „disconnect" between technical reality and legal regulation. At its core, the current draft regulates technical circumstances that are currently virtually non-existent.

Be it the reference to the principle of necessity, which seems to be blind to the technical conditions of electronic communications, or the expectation that people would turn off their smartphones in order to avoid offline tracking: The ePrivacy Regulation in its currenct state has not yet arrived in reality.

For the area of enforcement, the current draft would thus hardly represent an effective tool for preventing the infringement of fundamental rights emanating from the data processing operations of electronic communications. At this point, one needs to wish the legislator good advisers, an open ear for the practice and a great deal of courage. Fingerprinting, offline tracking, traffic analytics and the internet of things pose major challenges to the fundamental rights of private life and data protection. They can only be counteracted when accompanied with technical decisions. In any case, the problems will not be solved by making virtually unenforceable demands without, at the same time, entering into negotiations with the relevant Internet stakeholders on the part of the Commission. The ePrivacy Regulation would be an opportunity to influence the infrastructure of networking and the digitization of our communications and not just to try to legally capture the technical status quo retroactively. In doing this, the current draft has only moderately succeeded so far.

Dr. Malte Engeler
serves as judge at the administrative court of Schleswig-Holstein and is the former deputy head of the supervisory unit at the German data protection authority of Schleswig-Holstein.

Wolfram Felber
is the current deputy head of the supervisory unit at the German data protection authority of Schleswig-Holstein.

The article reflects only the personal opinion of the authors. The German version of this article is published in Zeitschrift für Datenschutz (ZD), ZD 2017, 251 ff.
Recommendation for citation: ZD 2017, 251 (E).
The translation has been drafted by Bitkom.

73 The *Federal Commissioner for Data Protection (BfDI)* is the supreme federal authority since 01/01/2016, cf. second amending law of the BDSG v. 25.2.2015, BGBl. I, p. 162.
74 However, pursuant to the recital 7 of the ePrivacy Regulation (E), the member states should be allowed to maintain or introduce national provisions within the framework laid down by the Regulation which clarify the application of the provisions of that Regulation.
75 *Stettner*, in: Dauses (Hrsg.), EU-Wirtschaftsrecht, B. III. Verwaltungsvollzug, margin note 48, incl. further evidence.
76 *Article 29 Data Protection Working Party* (s. footnote 6 above), para. 5.
77 Cf. to this ancient conflict *Simitis*, comments to BDSG, 8. ed. 2014, Introduction, margin note 20.