Specialist Group for Regulatory Issues (WAR)
at the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (Bundesnetzagentur)

Regulatory issues relating to OTT communication services

15 July 2016

To perform its tasks, the Bundesnetzagentur receives ongoing support from the Specialist Group for Regulatory Issues (WAR). WAR advises the Bundesnetzagentur with complete independence on all regulatory issues. In the following, WAR presents its opinion on the regulatory challenges associated with the increasing social and economic importance of OTT service providers.

I. Context

In the past year, WAR has focussed intensively on the evolution of regulation in the telecommunications and media sectors in view of the increasing relevance of over-the-top (OTT) providers, and on 18 November 2015 published a position paper on this issue. Prominent examples of OTT services include search engines such as Google, video platforms such as YouTube, social networking platforms such as Facebook and Twitter, messaging platforms such as WhatsApp, (video) telephony services such as Skype, and cloud services (web services). The position paper published in November 2015 addressed in relatively general terms both OTT communication and OTT content services. OTT communication services are often known as "OTT-1" or "OTT-I" services, while OTT content services are known as "OTT-2" or "OTT-II" services. The distinction between communication and content services – in the case of Facebook or Twitter, for example – is not always clear-cut, as the same platform often offers bundled, integrated services.

Around the time WAR's position paper was published in November 2015, Cologne Administrative Court (VG Köln) on 11 November 2015 (Az: 21 K 450/15) confirmed the Bundesnetzagentur's view that e-mail services, including webmail services, should be treated as communication services within the meaning of the Telecommunications Act (TKG). It is unclear whether the European Court of Justice (ECJ), the body ultimately responsible for the classification of these services, would agree with the assessment of Cologne Administrative Court. However, a wealth of regulatory issues have already been raised with regard to not only this OTT category, but also other services classified as telecommunication services. These questions are the subject of intense and fierce public

(and expert) debate and may ultimately have to be decided by the ECJ de lege lata or by the legislature de lege ferenda.

This position paper aims to support this discussion and decision-making process and therefore – in contrast to the WAR position paper published in November 2015 – focuses exclusively on OTT communication services (OTT-I services). It adopts positions on the question of whether the relevant provisions in national and European law are suitable for this service category and on the legal consequences of their application. At the same time – in view of the controversy in case law and literature –, proposals are to be developed for the adaptation of the regulatory framework as part of the forthcoming review of European Union law.

In general, OTT-I services such as messaging services or internet telephony services are in competition with traditional telecommunications services such as SMS or voice telephony. By contrast, OTT-II services such as search engines and social networking platforms, if anything, tend to complement traditional communications services. From the perspective of competition, the issue of how legal and regulatory frameworks should be applied de lege lata and designed de lege ferenda to enable a level playing field between traditional telecommunications services and OTT-I services is therefore of relevance.

In this context, it is important to note that traditional telecommunications services and OTT-I services are usually based on different business models. While a monetary fee is usually charged for traditional telecommunications services, either in variable or package form (eg a defined data volume) or as part of a monthly basic charge/flatrate, OTT-I services –at least basic services – are often provided at no cost for the customer. However, this does not imply that these can be used free of charge. Rather, users "pay" – at least from an economic perspective – with their data and/or attention for the third-party advertisements associated with the services, irrespective of how this exchange is viewed from a legal perspective. The data, in turn, is used by providers to, for example, place targeted advertisements and thus improve marketing. Because of these fundamentally different business models, the issue of a level playing field is an extremely complicated one. This is compounded by the fact that, from a user perspective, data – unlike money – can be used more than once as a means of payment. In contrast to financial resources, there is no rivalry or no shortage of data, making the question of possible customer exploitation and thus the need for regulation more difficult to answer. With this in mind, this position paper evaluates the possible need for regulation.

It is therefore necessary to first establish what exactly is included in the category of OTT communication services or OTT-I services and how these can be differentiated from OTT content services or OTT-II services (see II.). The analysis which follows is based on the regulatory structure of the TKG and therefore begins by considering market regulation issues (III.) before examining customer protection issues (IV.), followed by data protection issues (IV.) and finally public security issues (VI.). Conclusions are then derived on the basis of these analyses (VII.). In the context of the OTT business models examined in this paper, the significance of data from the perspective of competition economics and consumer protection is addressed in the sections on market regulation and customer protection issues.

II. Distinguishing between OTT communication and OTT content services

The OTT paper from November 2015 showed how OTT communication services or OTT-I services can be differentiated from OTT content services or OTT-II services. This distinction is of vital importance if OTT-I services are to be classified as telecommunications services. Distinguishing between traditional telecommunication services and OTT-I services which also offer traditional telecommunications functions – for instance, calling a conventional landline via Skype (what BEREC refers to as "OTT-0" services) – is then less important because all these services (traditional telecommunications services, OTT-0 and OTT-I services) are subject to the telecommunications regime; the flexibility options outlined below must be observed, particularly with regard to legal consequence. However, if the opposite opinion were to prevail, ie that OTT-I services de lege lata are not telecommunications services, the distinction between traditional telecommunications services and OTT-0 services on the one hand and OTT-I services on the other would be critical. This shows that, either way, a regulatory distinction is clearly required: either between OTT-I and OTT-II services in agreement with Cologne Administrative Court or between traditional telecommunications services and OTT-0 services on the one hand and OTT-I and OTT-II services on the other in agreement with the opposite side. It would be advisable for the future regulatory regime to provide further guidance on the classification of different services. It should be acknowledged in this context that the potential field of OTT-I services is extremely broad (should, for example, communication via PlayStation also be included?); the inclusion OTT-I services therefore heightens the need to discuss the possibility of reducing or enhancing the flexibility of the legal framework for telecommunications.

There is much to be said in this context for moving away from the necessity of signal transmission as the sole criterion for applying telecommunications regulations to OTT-I services and focusing instead on the telecommunications function of a service, thereby distinguishing it from a content service. Given the dynamic development of these services, the need for a further conceptual distinction is questionable since the categories of telecommunications services reflect a coherent, real-world service portfolio which can be reliably differentiated from content services.

For example, as demonstrated in the OTT paper from November 2015, OTT-I services can be broken down further into (web) e-mail services (such as GMX, Web.de, Gmail), OTT instant messaging services (such as WhatsApp, Skype, iMessage) and OTT internet telephony services (VoIP) or video telephony services (such as Skype, Skype for Business, Viber, WhatsApp, FaceTime calls). However, there are no indications that further differentiation of the regulatory framework is required for these sub-categories.

A common feature of OTT-I services is that they do not provide content services and instead enable individual and group communication in the form of voice, images, videos and other data using internet protocol (IP). By contrast, OTT-II services have a content element, even if it is extremely heterogeneous, and can range from search engine services such as Google, Bing and Yahoo, and streaming and video-on-demand services or platforms (YouTube, iTunes, Netflix, maxdome, Watchever, Amazon Instant Video, etc), to information portals such as Wikipedia, (daily) newspaper websites, and the media centres of TV stations. The homogeneity of these services is much less pronounced, such that no uniform regulatory framework for OTT-II services currently exists and is ques-

tionable. Since it can be assumed that OTT-I and OTT-II services will be increasingly coupled in future – by providers such as Facebook –, the future legal framework should provide guidance on this. A general issue to be clarified is the extent to which services can be functionally separated and subjected to different regulatory treatment. An alternative approach would be to classify services according to their predominant character. Currently and in the medium term, it can be assumed that the distinction between OTT-I and OTT-II services can be maintained and, with it, the different regulatory frameworks.

In the following, the focus is solely on OTT-I services. Even if, in agreement with Cologne Administrative Court, it is assumed that OTT-I services constitute telecommunications or electronic communications services (which must ultimately be decided by the ECJ), it does not necessarily follow that the existing regulations would have to be applied to OTT-I services or that they may be applied in unmodified form. Instead, the issue of regulation would have to be addressed in a very differentiated manner. German law requires the providers of these services to be notified under section 6(1) TKG, and all substantive and procedural standards would then potentially apply, including the regulations on data collection in the Bundesnetzagentur's Activity and Annual Report under sections 121 and 122 TKG. However, it should be noted on the one hand that a level playing field can also be created through deregulation and on the other that the protective purpose and the associated requirements for application of the regulatory instruments often cannot be readily applied to all OTT-I services owing to the different underlying technologies and business models. From a detailed perspective, a variety of sensible reclassifications are also possible or necessary based, inter alia, on whether services are publicly available or whether service providers have a dominant market position, etc. This is explained in greater detail in the sections below.

III. Market regulation issues

As a result of technological progress, the market is witnessing the emergence of many new providers which, with the help of new digital technologies, are competing with existing telecommunications services (plain old telephone services or POTS). The primary effect of the market entry of new OTT communications services such as Skype and WhatsApp is therefore more intense competition, with corresponding consequences for demand for traditional telecommunications services. While OTT communication services such as internet telephony (eg Skype) and messaging services are not complete substitutes for "traditional" voice telephony and SMS, they nonetheless compete with them, albeit not in every respect. They therefore also exert indirect competitive pressure on the wholesale markets for traditional telecommunications services. The effects of this increased competition may lead to price reductions; at the same time, they tend to reduce the need for regulation of these communication services.

To determine the possible need for regulation based on the market power of a service or provider in the field of electronic communication using the three-criteria test (section 10(2) first sentence of the TKG), the relevant market must first be defined. It is then necessary to determine whether one or several providers have significant market power, not only temporarily but permanently, such that the imposition of appropriate remedies is necessary. Defining the relevant market serves to identify the relevant competitive forces on a market. The crucial question when identifying relevant competitive forc-

es is whether two or more products or services are considered to be relevant alternatives for a sufficiently large user group, ie whether they are interchangeable from a user perspective. To establish whether two services are interchangeable from a user perspective, it is neither necessary for the underlying technologies (eg the transmission technology) to be identical nor for the services to be based on the same business model. For market definition, the only determining factor is whether a sufficient number of users consider two services to be sufficiently interchangeable.

While the definition of terms is important with regard to the regulatory treatment of a service, from the economic perspective the definition of the relevant market is crucial with regard to market regulation on the basis of significant market power. In this context, the distinctions between terms – for example, between OTT-I and OTT-II services or between OTT services and traditional electronic communication services – need not necessarily correlate with the defined markets. In many cases, traditional communications services and OTT-I services will be attributable to the same relevant market. OTT-I and OTT-II services can also, at least in part, be assigned to the same relevant market since precise classification of individual services either as OTT-I or as OTT-II services is not always straightforward due to the bundling of products – for example, many OTT-II services also have a messaging function. However, it is not the definition of terms or the classification of certain services in certain terminological categories that is important when determining the possible need for regulation based on significant market power, but rather the definition of the market and assignment to a relevant product market. From an economic perspective, possible market regulation should therefore be triggered by the significant market power of a provider, the assessment of which is based on market definition rather than the definition of terms under telecommunications law.

Transmission technologies and business models can play a role in market definition insofar as they influence the substitution behaviour of users, and different transmission technologies and different business models can, in individual cases, be indicative of limited substitutability. However, neither the type of signal transmission nor the specific business model alone should serve as a trigger for differentiated market regulation. The former goes against the concept of technology neutrality, and the latter fails to recognise the fact that business models also compete with each other. Instead, market definition from a user perspective and identified market power are crucial with regard to differentiated market regulation.

OTT-I services are frequently offered at no cost. However, this does not run contrary to the assumption of a competitive market, as determined by the Ministry draft of the Ninth Act Amending the Competition Act (GWB) in the new sub-paragraph 2a to section 18 GWB. The success of OTT-I services can be attributed to the ability to collect, link and analyse large quantities of structured and unstructured data in order to improve own online services on the basis of data acquired in this way and offer additional (primarily target group-specific) services. Even if data collection is less important for OTT-I services than for OTT-II services, it can be a relevant input resource. It is therefore important to examine whether possession of data can contribute to an undertaking's market power. Data possession leading to value creation by just one undertaking could result in market entry barriers for other competitors. These considerations are also reflected in the new sub-paragraph 3a to section 18 of the Ministry draft of the Ninth Act

Amending the Competition Act, according to which access to data should be taken into account when evaluating the market position of an undertaking in multilateral markets.

To comprehensively analyse the competitive significance of data, the basic economic characteristics of data must be considered. Unlike other input factors, data can in principle be copied and used any number of times. Data therefore possesses the economic characteristic of non-rivalry in consumption; several undertakings can, in principle, use the same data at the same time without negatively affecting use by others or even excluding others from use. However, users can be effectively excluded from the use of data; the exclusive use of collected data by just one undertaking is possible in practical terms. The data collected by OTT-I providers is not usually available to other users, at least not directly.

To establish a significant correlation between market power and the use of data or the value-generating information it contains, the importance of this data usage and the use of information to generate value must be determined in relation to the undertaking's market position. It must therefore be proved, for example, that it is not possible for other undertakings to successfully enter the market due to the non-availability of this data-based information pool. It must also be proved in this context that the quality of the OTT communication service is so outstanding due to the high level of data availability that other providers are unable to offer a comparable product. Closer analysis reveals that the attractiveness and quality of the service is not determined primarily by continuous access to the extensive database, but rather by the combination of product idea and design, algorithm and computer capacities. It therefore does not seem possible to attribute market power to the availability of mass-generated data alone. The importance of data is always relative to the respective business model. For this reason, a competitive assessment of OTT communication service providers with business models which also comprehend data-based value generation should include a comprehensive analysis of the importance of data usage for the competitive position of this provider, together with other "traditional" market analysis parameters such as market access barriers, consideration of economies of scale and network effects, etc. Fortunately, therefore, section 18 of the Ministry draft of the Ninth Act Amending the Competition Act has been supplemented by a subsection (3a), which provides sample criteria for determining the market position of an undertaking on multilateral markets:

"(3a) Where multilateral markets and network effects exist, the evaluation of an undertaking's market position should give special consideration to the following:

1. direct and indirect network effects,

2. the parallel use of several services and switching costs for users,

3. its economies of scale in connection with network effects,

4. its access to data,

5. innovation-driven competitive pressure."

It should also be noted that traditional communication services, which are in competition with new OTT-I services, are not currently subject to regulation based on market power, at least not in Germany. This applies to both voice telephony services and SMS

services. Instead, regulation based on market power focuses mainly on access and termination products. For termination, in particular, there may even be potential for deregulation, provided competitive access to the internet and therefore to OTT-I services is ensured. However, rather than being judged on a sweeping basis, this should be assessed on a case-by-case basis , taking primarily account of the actual substitution behaviour of users. Whether or not, as is the case with traditional services, any-to-any communication is desirable should also be examined in this context as most users of OTT-I services use multihoming solutions. As mentioned above, the parallel use of several services should, in accordance with the Ministry draft of the Ninth Act Amending the Competition Act, also be taken into consideration when evaluating the market position of undertakings in these areas.

The 2015 WAR paper also notes that the *asymmetric regulation of dominant market positions* in the case of OTT-I services is generally not advisable as such markets are not mentioned in the European Commission's 2014 Relevant Markets Recommendation. In other words, a relevant market would have to be defined before any market regulation could be triggered.

A more difficult question to answer is whether or not OTT-I service providers could potentially be subject to symmetric *access regulation under section 18 TKG, which is not based on market power*. While the wording of the German legislation seems to preclude this by limiting the scope of regulation to "public telecommunications network operators," the scope of Article 5(1) para 2 lit (a) of the Access Directive potentially is broader ("undertakings that control access to end-users"). This means that, in accordance with the Directive, it might be possible to impose interconnection and interoperability obligations on providers of OTT-I services to thus ensure end-to-end connectivity for end-users. In detail, however, this is contentious de lege lata. Even if it is conceivable in principle, it is questionable whether it is advisable. While it is possible for users to use several OTT platforms (eg WhatsApp and Viber) at the same time without a problem ("multihoming"), this is not – or at least not currently – the case for traditional telecommunications services. However, such instant messaging services, unlike e-mail services, are not interoperable. This is relevant from a consumer and data protection perspective, but the need for an interoperability obligation cannot be derived from this on the basis of market regulation considerations. From a customer perspective, the lack of interoperability means that a user of an instant messaging service can only be reached via this communication channel if you yourself are using that same service at the same time and thus accept the terms and conditions of use. This also has implications for data protection (see V.4. below). Nonetheless, the user can be reached via other communication channels as multihoming is the rule rather than the exception for users. For example, if user A of instant messaging service X also uses instant messaging services Y and Z and SMS, user B, who does not use instant messaging service X, can still reach user A via instant messaging services Y and Z and by SMS. The need to also use instant messaging service X is therefore significantly reduced. Another issue from a user perspective is whether and in what circumstances users want to be contacted in these networks from outside closed networks. Clarification is also required with regard to whether, if users use or can easily use multihoming solutions, OTT-I providers can be classified as "undertakings that control access to end-users" under Article 5(1) para 2 lit (a) of the Access Directive.

It is important to consider in this context that, in many cases, OTT-I services are new products with strong product differentiation. While traditional telecommunications services such as voice telephony and SMS are characterised by a high degree of product homogeneity, OTT-I services are often highly differentiated. This product differentiation is really what drives competition. The interconnection of OTT-I services – possibly resulting from a regulatory requirement – could have a negative effect on competition. Because the business models of many OTT-I services are based on advertising income, it is crucial for these models that users use the corresponding applications (eg by installing them on their terminal equipment). If users evade advertising, the business models are rendered unviable. In the same way that content providers sometimes prevent users with ad blockers from using their content free of charge or require them to pay a fee, OTT-I providers are likely to have little interest in providing free services for outside parties who do not wish to use the corresponding applications. However, this is exactly what would happen if interoperability requirements were imposed. There would be the danger that free services would ultimately be forced out of the market. It is doubtful whether this would be in the interest of the majority of users. A cautious approach to the imposition of interoperability obligations is therefore advisable. There is currently no need to impose regulatory obligations in respect of the interconnection and interoperability of OTT-I services.

IV. Customer protection problems

The second major area of regulation, namely *customer protection* under sections 43a ff TKG (Articles 10ff Universal Service Directive 2002/22 in the version of Directive 2009/136), is usually less relevant for OTT-I providers than for traditional telecommunications services. OTT services were not the main focus for legislators when the legislation was drafted. The customer protection regulations of the TKG are clearly intended to apply to traditional telecommunications services based on the provision of a network connection. In terms of customer protection, OTT-I services within the meaning of VoIP or video telephony (eg Skype), messaging services (eg WhatsApp) and e-mail services (eg Gmail) can be distinguished from these traditional telecommunications services in three key respects:

Firstly, OTT services are provided via the internet, not via independent physical connections. If the customer is connected to the internet through a contract with a DSL, cable or mobile provider, there is generally no need for special hardware connections or additional terminal equipment. Customer protection regulations relating to *connection to public telecommunications networks* (eg section 45d(2) TKG/Article 10(2) of the Universal Service Directive) therefore clearly do not apply to OTT-I services.

Secondly, OTT-I services are usually non-exclusive. As explained above, multihoming is unproblematic, whereas the parallel operation of two landlines or DSL connections from rival providers is not possible for technological reasons. Customer protection provisions which are intended to facilitate the process of *switching providers* (namely section 46(1 and 2) TKG/Article 30(4) para 2 and 3 of the Universal Service Directive) therefore also do not apply to OTT-I services. OTT-I service contracts usually do not specify a fixed contract term. And even if they did, this would not be a problem due to the fact that such services are usually provided at no cost and because of the option of multihoming (con-

trary to traditional telecommunications services, see section 43b TKG/Article 30(5) of the Universal Service Directive).

The situation is not quite so clear-cut with regard to *number portability*, as provided for by section 46(3 and 4) TKG/Article 30(1 to 4) of the Universal Service Directive. Portability is assured by these provisions "to guarantee provider switching". Irrespective of whether users are identified directly or indirectly on the basis of a telephone number or a potential equivalent (such as an e mail address), this raises the general question of whether portability is necessary at all since "switching" to a new provider, unlike with traditional telecommunications services, does not require the termination of the business arrangement with the existing provider. The user can continue to use the existing service in parallel and can therefore still be reached via the existing number. Nonetheless, a differentiated analysis which focuses on the relevant OTT-I service appears to be appropriate.

- The portability of e-mail addresses (eg "JoeBloggs@gmail.com") does not appear to be necessary, particularly as this could, from the perspective of domain names, encroach on the rights of providers and lead to confusion about the service used for third parties. To facilitate the change to another provider, it is worth considering a rule which would require the provider of such a service to automatically forward e-mails to the new address for a certain period. This is particularly relevant for e-mail addresses which are provided as part of a bundle with other telecommunications services (eg "JoeBloggs@t-online.de" or "Joe.Bloggs@netcologne.de"), while pure OTT services such as Gmail and Web.de already seamlessly provide such a forwarding service free of charge.
- A regulation regarding the portability of other data (eg the content of e-mails and address books), as provided for, for example, in Article L 121-120 ff of the French Consumer Code in the version of the draft legislation on a digital Republic, appears to be superfluous – quite apart from the fact that, as a content-related regulation, it would be dealt with in the Telemedia Act rather than the Telecommunications Act – as all users can easily generate a local copy of this data themselves using any e-mail program (eg Outlook). The situation is different with some messaging services such as WhatsApp. However, given that Article 20 of the EU General Data Protection Regulation (2016/679), which is set to come into effect in 2018, provides for a comprehensive European portability regulation, no additional national regulation is required.
- User name porting (eg "JoeBloggs" for Skype) can already be ruled out since such names (unlike telephone numbers) are not exclusive across all providers. On the one hand, the user can therefore choose to use the same user name with another provider, provided this name is still available there. On the other hand, it may not be possible to use the existing user name if it has already been allocated to another user by the new provider. In both cases, there would be no point in a statutory regulation on user name porting.
- If users are identified by an OTT-I service by means of a traditional telephone number – as is necessary with, for example, WhatsApp and optional with Threema or Apple Facetime –, further differentiation is required: If the number is used only indirectly for identification (as with WhatsApp), number porting is not nec-

essary. The user is free to use the same number for identification with another OTT-I service (instead of, or at the same time as, the old service). Moreover, WhatsApp has no power of disposition over these numbers.

Thirdly, a key difference between OTT-I services and traditional telecommunications services is the fact that OTT-I services are, for the most part, not subject to monetary charge. Therefore, traditional misuse or customer protection problems related to billing do not arise, such that *charge-related protection provisions* also could not be applied or could only be applied in modified form.

The logging of call data, which is contentious from the perspective of data protection law in any case, is superfluous here. In general, the customer requires neither itemised billing to check the appropriateness of billing (section 45e TKG/Article 10(2) and Annex I Part A (a) of the Universal Service Directive), nor a regulation for prepaid services (section 45f TKG/Article 10(2) and Annex I Part A(c) of the Universal Service Directive); likewise, the other billing provisions of the TKG concerning monetary compensation (sections 45g ff TKG) are not applicable for OTT-I services.

Exceptions apply only if – for example, in the case of Skype calls to the public telephone network – call charges are billed which require users to have control options in accordance with the existing regulations for traditional telephone services.

However, OTT-I services give rise to *new problems* due to the fact that, as mentioned earlier, although it is common for no monetary fee to be charged for these services, they are not necessarily provided "free of charge" because users have to provide data as consideration. This raises the question of whether *data-related regulations* are required in parallel with the customer protection regulations relating to monetary payments in sections 45e ff TKG.

In this context, it is necessary to distinguish between the issue at hand and data protection legislation. While the focus there is on finding the constitutionally required balance between the business interests of OTT-I providers and protecting personal data from illegal collection and use, the existing customer protection regulations focus on preventing the financial exploitation of customers.

Regulations to *improve transparency* seem to be generally expedient since, despite the intense debate of recent years, there are still customers who are unaware that, in return for (seemingly) free OTT-I services, they are actually disclosing their personal data. However, it is doubtful whether such a regulation should be anchored in sector-specific customer protection provisions. The commercial collection and use of data within the meaning of "big data" is usually discussed in the context of OTT-I services, but it is also playing an increasingly important role in many other sectors (particularly in the banking and insurance sector, but also in retail through customer cards). Special provisions should therefore only be made in cases where there are no, or only inadequate, corresponding protection provisions in general data or consumer protection law. Of interest in this context is the extent to which instruments used in traditional customer protection law to improve transparency (sections 45g ff TKG/Article 10ff of the Universal Service Directive) already exist in equivalent form, or are to be provided for in future, in the

applicable telecommunications data protection law. This is examined in greater detail in the following section.

In this connection, we must also consider the complex issue of the right systematic placement for regulations designed to *prevent customer exploitation* through the excessive collection or use of data. This is a classic customer protection issue. Establishing a further-reaching regulation to protect customers from economic exploitation would require a market failure to have been identified which cannot be corrected through the application of data protection legislation or any other general legislation (including antitrust legislation). While it is sometimes argued in public and political debate that such a market failure has occurred, there is no evidence of this. The legislature would therefore have to call upon its by no means unlimited prerogative of assessment in uncertain decision-making situations. In this respect, there is currently a lack of basic economic and legal research. Such research would have to clarify the following aspects:

- On closer inspection, the very concept of data is extremely complex and unclear. It includes, for example, customer, traffic and user data, personal and non-personal data, individualised, pseudonymised or anonymised data, more or less valuable data, young and old data, data supplied voluntarily by users, eg when registering for a particular service or creating a profile, and data – such as movement profiles – which is usually generated by the service providers themselves, eg based on internet logs, cookies, etc (see Monopolies Commission, Special Report 68, 2015, para 74 ff). Exploitative abuses almost always relate to personal data.
- However, the issue of who this data "belongs" to (and which proportion of the data is attributable to whom) remains largely unclear. The customer about whom the data provides information and who is therefore the subject of the data protection rights is not the only possibility. Moreover, the person who stored the data or on behalf of whom the data was stored, for instance, is also authorised to dispose of data within the meaning of section 202a of the Penal Code (StGB) (Illegal acquisition of data). From an economic perspective, there are ultimately some arguments in favour of attributing at least some of the value of data to the party who gains commercially valuable findings from the raw data by linking it with other data and processing it.
- There is also a lack of clarity with regard to how the value of individual data can be measured, what the value-generating factors are, and how to account for the value generated by customers through the disclosure of their data without subjecting them to "total surveillance", which is prohibited under data protection law. This applies all the more since data is non-exclusive and non-expendable and therefore – unlike money – can be used more than once as payment.
- Finally, there is a lack of clarity as regards how the value of OTT-I services can be measured and whether the customer is therefore receiving too little consideration. There is often no chargeable alternative to OTT-I services and, where such alternatives do exist, customers usually opt for the advertising and therefore data-based variations. This is also reflected, for example, in the crowding-out of SMS by WhatsApp, in Germany in any case. Determining the value of OTT-I services based on their value-generating potential (eg on the basis of advertising in-

come) would at first glance seem conceivable, but ultimately does not answer the crucial question of which proportion of this value-generating potential is attributable to the customer. If customers were aware of the intrinsic value of their data, the provision of this data for the use of a service could be seen as market pricing, which prevents exploitation without necessitating regulatory interference (or even an exact determination of service value and consideration).

It is therefore advisable with regard to customer protection to first and foremost improve transparency. Where the TKG is applicable, this could be achieved by including an obligation for OTT-I undertakings to inform customers on the use of the data. A regulation on the temporary forwarding of e-mails also seems expedient. Further-reaching regulations which go beyond the scope of (telecommunications) data protection law are not appropriate at the present time. In cases where the data protection law does not provide for indirect remedial action, misuses can already be challenged on the basis of general terms and conditions of business law (sections 307 ff of the Civil Code (BGB)) and, where appropriate, on the basis of antitrust legislation (abuse of conditions within the meaning of section 19 of the Competition Act or Article 102 TFEU) and, in this way (eg through the proceedings initiated by the Federal Cartel Office against Facebook on 2 March 2016), findings can be gathered.

V. Data protection issues

1. Relevance of data protection provisions

As indicated in the 2015 OTT paper, OTT-I providers also earn money by evaluating user data. The extent to which such providers are subject to the data protection provisions under telecommunications law, or should be subject to these in future, has therefore been identified as a key regulatory issue. Further problem analysis confirms the importance of this issue. It is therefore interesting to note that jurisprudential literature refers to ambiguities in precisely this area and that, even on the basis of a more narrow understanding of the concept of a telecommunications service within the meaning of the TKG, the application of the TKG is nonetheless considered appropriate in some cases, at least for issues relating to data protection. This is entirely logical since neither the Federal Data Protection Act (BDSG) nor the Telemedia Act (TMG) is geared to the protection of telecommunications processes.

2. Minimum legal requirements for traditional telecommunications services and OTT-I services

From the perspective of European Union law, which is decisive for the review of the regulatory framework for electronic communications, contrasting findings can be found in two similar directives: “Directive 2002/58/EC on Privacy and Electronic Communications” (hereinafter E Privacy Directive) sets out specific, more stringent provisions on the characteristics of electronic communications, while the currently applicable general Data Protection Directive 95/46/EC (hereinafter Data Protection Directive) does not. This is not set to change with the application of the new General Data Protection Regulation (hereinafter GDPR), which has been postponed until 2018. The GDPR will replace the Data Protection Directive from 2018, but will not contain specific provisions on electronic communications, despite this having been proposed during the legislative pro-

cess. Therefore, the focus will continue to be on the special provisions of the E-Privacy Directive. However, the Commission has also initiated a review process for this special regulation following the adoption of the GDPR.

The point of departure for any (non-constitutional) legal reform at the EU or member state level must be the applicable fundamental legal provisions or minimum requirements. Given that general and telecommunications-specific data protection law is shaped by EU law, the relevant framework is formed by the Charter of Fundamental Rights of the European Union (CFREU) and the judicial decisions of the European Court of Human Rights (ECHR) based on the European Convention on Human Rights, which play a key role in the fundamental judicial decisions of the European Court of Justice (ECJ) in matters relating to data protection legislation. In its decision on data retention, the Federal Constitutional Court also clearly indicated that the right to informational self-determination and the secrecy of communications can be important elements in controlling the actions of EU institutions with regard to the conflict of law between the German national legal system and European Union law, which is why the national constitutional framework should also apply.

The key point of reference is the fundamental right to the protection of personal data enshrined in Article 8 of the European Convention on Human Rights and Article 16 TFEU. This fundamental right applies to all forms of data processing, irrespective of whether this happens in the context of traditional telecommunications services or OTT-I services. Distinctions by the legislature are not prohibited outright, but must be consistent with the principle of equality set out in Article 20 of the European Convention on Human Rights. As the ECJ has made very clear in its recent rulings (C-131/12, Google Spain, judgement of 13 May 2014; C-362/14, Schrems (Facebook), judgement of 6 October 2015), fundamental rights also apply – where there is sufficient connection to the EU – to the regulation of private data processing by transnational internet groups based outside the EU. In dogmatic terms, the fundamental right therefore has an indirect third-party effect and gives rise to duties of protection for EU legislators with regard to the design of private legal arrangements – where appropriate, also with third-country nationals. These duties of protection are deemed to have been violated if, in the case of private data processing, there is no effective monitoring of data protection by, in particular, independent European entities or the equivalent supervisory authorities in third countries, or if adequate legal protection against private data processing is not ensured for those affected.

In addition to fundamental data protection rights, the right to respect for communications, as ensured by Article 7 of the European Convention on Human Rights – which in Germany is referred to as the right to privacy of correspondence, posts and telecommunications – as a specific element of the right to respect for private and family life, is of particular relevance for a legal framework for OTT-I services which complies with fundamental rights. The ECJ classifies, for example, the retention of traffic data by private undertakings as interference with Article 7 of the European Convention on Human Rights, albeit interference which can be justified. It classifies the perusal of the content of electronic communications as particularly serious interference (ie interference which can only be justified by meeting qualified requirements) with the fundamental rights set out in Article 7 of the European Convention on Human Rights, and the general monitor-

ing of content as interference with its very substance, without excluding from the outset that these strict standards apply not only to the monitoring of content by the state, but potentially also to private monitoring and evaluation activities (judgement C-293/12 inter alia, Digital Rights Ireland inter alia, judgement of 8 April 2014). It is particularly noteworthy in this context that, in terms of traffic data, the ECJ makes no qualitative distinction between data concerning fixed telephony and mobile telephony on the one hand and data concerning internet access, internet e-mail and internet telephony on the other, but instead observes that the general retention of such data "applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives" (para 56).

From the perspective of fundamental rights, regulatory classifications and different business models are therefore irrelevant when the communication services in question are considered functional equivalents from a user perspective and, above all, are associated with equivalent threats to fundamental rights. This analysis therefore appears to support the uniform protection of electronic communications, rendering the need to distinguish between traditional telecommunications services and OTT-I communications services irrelevant. Moreover, this would not be affected by the (targeted) combining of OTT-I services with OTT-II services in bundled products. Individual problems concerning fundamental rights would simply be judged on a differentiated basis. The ECHR's ruling on the parallel fundamental right to respect for private life under Article 8 of the European Convention on Human Rights has, for some time, recognised a duty of protection on the part of state actors with regard to the regulation of private legal arrangements (ECHR, 19 February 2015, application no 53649-09 – Ernst August von Hannover v Germany, NJW 2016, 781 ff). Although the ECJ has not explicitly acknowledged this to date, it implicitly recognises similar approaches in its rulings (see most recently C-362/14, Schrems (Facebook), judgement of 6 October 2015, para 94 read in conjunction with para 91-95, 38, 42, 58).

The Federal Constitutional Court takes a parallel approach in its rulings on Article 10 of the German Basic Law (GG). It merely aims to establish whether electronic communication takes place, such that from the perspective of constitutional law a distinction between, for example, whether an internet-based e-mail service is used or whether an e-mail is sent via a "traditional" telecommunications service provider, is of very little relevance. In its decision of 16 June 2009 (2 BvR 902/06), the Federal Constitutional Court investigated the seizure and confiscation of e-mails on an e-mail provider's mail server from the perspective of the right to secrecy of telecommunications provided for by Article 10(1) GG and indicated that protection is particularly required where this type of electronic communications service is used. For the Federal Constitutional Court, the decisive factor for the applicability of the secrecy of telecommunications was the fact that the e-mails were still stored on the e-mail provider's server. The protection afforded by the right to secrecy of telecommunications relates primarily to protection against the access interests of the state, but, as part of the sovereign duty of protection, the state must also ensure that private undertakings observe the right to secrecy of telecommunications.

From the perspective of interpreting the E-Privacy Directive and the TKG in compliance with fundamental rights, there is therefore much to be said for not focusing on too nar-

row or too technical a definition of the concept of the telecommunications service, but instead on functionally establishing whether or not electronic communication takes place. However, it should be noted that, as outlined earlier (see II.), this type of differentiation is much more difficult than differentiation on the basis of technology.

At any rate, a uniform protection standard for traditional telecommunications services and OTT-I communications services is necessary from the perspective of fundamental rights. Furthermore, this standard cannot be lowered arbitrarily since it is a question not only of protection *from* the state (for example, with regard to "public security"), but also of protection *by* the state from private providers of electronic communications services.

3. Different requirements de lege lata: TKG/E-Privacy Directive vs TMG/Data Protection Directive

a. Scope of application of TKG/ E-Privacy Directive and TMG/Data Protection Directive

Under the TKG, the application of telecommunications regulations in the area of data protection depends of whether "telecommunications services [are provided] on a commercial basis in telecommunications networks," as set out in section 91(1) sentence 1 TKG. The TKG even specifies: "including telecommunications networks supporting data collection and identification devices, provide or are involved in the provision of." In some cases, however, the scope of application is subsequently limited to *publicly available* telephone services within the meaning of section 3 para 17a TKG (see, for example, section 99(1) sentence 8 and (2) sentence 7, section 101(1) sentence 4, and section 102(3) TKG), such that no corresponding obligations apply with regard to non-publicly available services (for example, in closed user groups or e-mail services offered by a university to its students). This limitation is consistent with Article 3 of the E-Privacy Directive, which states that the Directive shall apply to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices." The majority, but not all, special obligations correspond with the relevant provisions in the E-Privacy Directive. This Directive is also generally applied "with respect to the processing of personal data in the electronic communication sector" and is to ensure not only an equivalent level of protection of fundamental rights, but also the free movement of such data in the Community (Article 1(1)). According to Article 1(2) E-Privacy Directive, the provisions of this special regulation serve to "particularise and complement" the general directive (Data Protection Directive). Thus, where there is no publicly available electronic communications service within the meaning of the E-Privacy Directive or no telecommunications service within the meaning of the TKG, the general Data Protection Directive applies (and the GDPR as of 25 May 2018), which in Germany has been considerably expanded upon on a sector-specific basis by the TMG. In light of the applicability of the GDPR, it will be necessary to determine whether the specific provisions of the TMG can be upheld in addition to the GDPR. It remains to be seen whether this is permissible (or politically desirable).

b. Overview of different requirement profiles

The following distinctions should be made:

In principle, the general obligations regarding the provision of information in section 93 TKG (which stems from, inter alia, Article 4(2-5) and Article 6(4) E-Privacy Directive) and section 13 TMG (see Article 10 Data Protection Directive) are very similar, even though the obligations of the TKG are clearly more strict. According to section 93(1) TKG, they begin upon conclusion of the contract and not just upon use of the service, as with the TMG. Another point worth noting is the permitted range of choices and options. Furthermore, section 93(2) TKG sets out information obligations which are not provided for in the same way in the TMG. However, the German provisions in the TKG go much further than the provisions of the E-Privacy Directive. This is particularly true of section 93(1) TKG and Article 6(4) E-Privacy Directive with regard to, for example, the duty to provide information regarding choices and options.

Fewer problems arise with regard to *customer data*, ie data which may be processed within the scope of organising contractual arrangements. Section 14 TMG even contains a provision which is fundamentally similar to section 95 TKG which, for its part, stems from Article 13 E-Privacy Directive, although it is more differentiated. Section 14 TMG has no specific equivalent in the general Data Protection Directive. It therefore provides greater specificity for the sector.

Traffic data enjoys special protection under telecommunications law in section 96 TKG (largely consistent with Article 6 E-Privacy Directive), and is also protected in similar form as usage data in section 15 TMG, even if the intensity of protection differs and, for the most part, is lower. Under section 15(3) TMG, for example, the service provider may, where pseudonyms are used, use user profiles for the purposes of, inter alia, advertising if the user does not specifically object to this. In other words, an "opt-out" solution applies. By contrast, section 96(3) TKG is much stricter; it requires the consent of the party concerned and therefore constitutes an "opt-in" solution. Moreover, the called party must be made anonymous rather than just pseudonymised. Much stricter boundaries therefore apply to marketing in the area of telecommunications. Section 15 TMG also has no equivalent in the general Data Protection Directive and therefore provides greater specificity for the sector. Whether or not the "opt-out" solution will continue to exist in future in view of the GDPR is extremely doubtful as the regulation of consent in Article 7 and its definition in Article 4 para 8 raise questions as to the continued use of "opt-out" approaches in light of the need for clear and unambiguous consent. In this regard, a partial levelling-out of differences could therefore potentially be expected in future.

In the case of *location data*, differences are evident with regard to categorisation; these are particularly relevant to mobile communication and regulated in detail in the TKG, but not considered separately in the TMG due to the tailoring of the act. Here, jurisprudential literature argues that section 98 TKG, as a lex specialis, also applies to services which do not consist primarily of signal transmission or are not qualified as such. However, this is by no means guaranteed; thus, the data protection standard for telemedia services is unclear in this respect. In any case, no comparatively strict additional requirements apply under the TMG; if section 98 TKG is not applied, traffic data could therefore be treated in the same way as other usage data. Considerable facilities would

then apply to the compilation of user profiles for advertising purposes, for example. In other words, if an OTT-I communication provider is working with location data – for instance, as part of a "friend finding" app –, there would be much greater commercial scope for the financial exploitation of the data, whereas stricter restrictions apply under the TKG (for example, with regard to consent). Section 98 TKG is otherwise consistent with Article 9 E-Privacy Directive.

Finally, the TKG sets out a range of provisions which, in terms of regulatory purpose, are not suitable for OTT-I services based on the business models typically used to date. This applies, for example, to itemised billing under section 99 TKG, which requires a monetary charge to be paid for the service (for individual calls), which is currently not the case for OTT-I services.

4. Preliminary conclusions

At this juncture, it is therefore fair to conclude that the differentiated regulation of traditional telecommunications services by the data protection provisions of the TKG on the one hand and of OTT-I services by the corresponding provisions of the TMG on the other, but particularly the differentiated application of the EU regulations of the E-Privacy Directive and the general Data Protection Directive or the future GDPR, do not ensure a level playing field. An overly lax data protection standard for OTT-I communication services is also extremely problematic from the perspective of fundamental rights as, according to the rulings of both the Federal Constitutional Court and the ECJ, a relatively high minimum standard must be upheld. Distinctions in this context are generally made on the basis of the need for protection rather than the business model of the service or technical processing. In terms of fundamental rights, there is therefore much to be said for a uniform data protection standard for traditional telecommunications services and internet-based communications services (OTT-I services).

This indicates that future legislation should provide for uniform regulations in this respect. In principle, the regulations relating to data protection in the telecommunications sector can also be applied to OTT-I services. Based on the recognition of these services for the purposes of data protection legislation in the telecommunications sector, it may be possible to critically examine whether or not a partial reduction in these provisions is appropriate, while maintaining the minimum standards for fundamental rights. However, analysis of the aspects of data protection law, in particular, indicates that there are good reasons to interpret the applicable law – or design the future legal framework – in such a way that uniform provisions apply since the TMG (and also the general Data Protection Directive) barely ensures the necessary data protection standard for electronic communication.

With regard to a possible differentiation of data protection requirements, it should be discussed whether and to what extent, on the basis of transparent and clear information of the users, it can be assumed in future that a user gives his/her consent for the service provider to exploit data relating to their communication processes as a permissible form of consideration which is typical for such contracts. Elements worthy and necessary of discussion in connection with better transparency could be the appropriate periodical provision of information about actual data usage by the service provider or substantive certification by independent third parties. Comparable facilities and obligations should,

however, then also be laid down for traditional telecommunications services. This explicitly opens up to them – albeit at the price of increased transparency – the business model of numerous OTT-I service providers, whereby the service provider's communication service is provided in exchange for consent to comprehensively process the service recipient's data.

However, this raises complex questions with regard to the voluntary nature of consent for services where no reasonable alternatives are available or where services are not interoperable. For example, WhatsApp messaging and communication with WhatsApp users is only possible when users themselves accept the terms and conditions of use of WhatsApp. By contrast, a Gmail customer can also be reached by customers of other webmail service providers. Consequently, consideration should be given to whether the voluntary nature of consent can only be assumed if an OTT-I undertaking's portfolio also includes a data-efficient, charge-based service. However, this would require the appropriateness of the charge to be ensured.

Moreover, there is no question that the data protection standard can and must be enforced for every service provider, regardless of whether it is based in an EU or a non-EU country. This is consistent with the state's duty to protect fundamental rights and does not pose any unreasonable requirements. After all, this would only have to be imposed on services which are used in sufficient measure by users. As soon as an undertaking has large customer groups in an EU country or in the EU as a whole, however, enforcement of European data protection standards would also be possible. This is consistent with the ECJ's above-mentioned recent rulings, particularly in the case of Google Spain, and – with the codification of the lex loci solutionis in the GDPR – is set to become an explicit standard in general European data protection legislation in future.

VI. Security issues

The individual and group communication enabled by OTT-I services has increased rapidly in recent years. Security authorities, in particular, have a vested interest in assessing these processes in order to avoid risks and investigate crime. The existing regulations are based on the model for traditional telecommunications. The question, therefore, is whether these new services should be measured against the public security standards of the TKG. The following section examines the circumstances under which uniform regulations are appropriate and the circumstances under which different treatment seems justified based on the individual public security provisions of the TKG. It also aims to establish at what stage the legislature must intervene de lege ferenda to close gaps in protection. This is always done under the premise of creating a level playing field. After all, measures to protect the secrecy of communications or to enable telecommunications interception for law enforcement agencies give rise to costs for the relevant telecommunications undertakings. Unequal treatment can therefore quickly lead to distortions of competition.

1. Service and network security

a. Technical and organisational safeguards

Section 109 TKG contains provisions on technical safeguards which must be observed by telecommunications service providers. This regulation stems from Article 4 E-Privacy

Directive, which is supplemented by Article 13a of the Framework Directive. The provisions of section 109 TKG concern measures to protect the privacy of telecommunications and to protect against personal data breaches. However, telecommunications providers must also, under section 109(2) TKG, initiate measures to protect against faults which would result in considerable harm to telecommunications networks or telecommunications services, and to control risks to the security of telecommunications networks and services. To implement these measures, they must draw up a security concept and nominate a security commissioner (section 109(4) TKG).

These provisions are sector-specific regulations of the TKG. Section 13(7) TMG contains a similar regulation for telemedia service providers, which was added to the TMG through the IT Security Act. However, unlike the TKG, the underlying aim of the data protection provisions of the TMG is not to protect the privacy of telecommunications, but rather to prevent an attack on critical infrastructures and on data protection.

When using traditional telecommunications services and OTT-I services such as WhatsApp and comparable voice and video telephony services which enable real-time communication, risk situations similar to those which apply to traditional voice communication can be identified with regard to the privacy of telecommunications. This supports the case for treating these OTT-I services de lege ferenda as telecommunications services and applying the statutory regulations of the TKG accordingly. However, it must be noted that the technical systems of OTT-I services can currently differ greatly from the architecture of traditional telecommunications services. Therefore, existing security requirements must be adapted de lege ferenda to the public security challenges presented by OTT-I services, including from a technical and organisational perspective. If, as discussed above, an OTT-I service were to be classified de lege lata as a publicly available telecommunications service, it would be possible to demand the relevant safeguards now.

b. Reporting data breaches

Section 109a TKG sets out an obligation to notify the Bundesnetzagentur of any data breaches. In the event of a serious personal data breach, the telecommunications service provider must also immediately inform those affected. Section 3 para 30a TKG defines what is meant by “personal data breach”. It states that it means a “breach of data security leading to the loss, unlawful deletion, alteration, storage, disclosure or other unlawful use of personal data transmitted, stored or otherwise processed in connection with the provision of publicly available telecommunications services, and unlawful access to such data.” This aims to enable users to respond adequately to existing dangers. The provision implements Article 4(3), (4) E-Privacy Directive, which was amended by Article 2 of Directive 2009/136/EC. Here, too, it seems appropriate to harmonise protection standards to create a level playing field. Article 31f GDPR already sets out an inter-service obligation to notify those affected as well as the supervisory authority; however, this is not consistent with the current strict provisions of the TKG.

c. Emergency calls

Specific problems arise in connection with the obligation to provide access to emergency services under section 108 TKG, which stems from Article 26 of the Universal Service Di-

rective. Because the obligation to enable emergency calls has cost implications, it is also relevant to the creation of fair competitive conditions. The provision is directed at those who provide publicly available telecommunications services for outgoing national calls to one or several numbers within the national telephone numbering plan. The wording of the provision ties in with "traditional" call numbers and therefore applies to traditional telephone services and, for example, Skype-out. Conversely, telephone services provided exclusively via the internet with which users communicate with each other via computers or tablets and would therefore have to use these devices to make an emergency call are not included in the scope of the provision. This applies all the more to new services which, for example, contain both a messaging function and a telephone function, whereby this only stretches to subscribers on the same platform. It should be clarified de lege ferenda whether and, if so, how emergency calls should be extended to these services; in doing so, the question of functions and support for those with speech and hearing impairments must also be taken into consideration. Technological solutions are currently available which allow VoIP providers to determine the location of a person making an emergency call via the ISP/IAP from the network access provider. The problem of location information being requested unnecessarily can be counteracted by only informing the VoIP provider, at its request, of the locally responsible public safety answering point and providing a reference which is only valid for a short time. Using the reference, the answering point can request the exact location from the network access provider. The introduction of emergency calling functions for OTT-I services depends, however, on the willingness of public safety answering staff to support non-voice communication forms. Text communication takes longer than voice communication and also cannot reliably transmit background noises or the state of agitation of the person calling. Finally, there are questions as to the reliability, availability and real-time capability of the service as well as liability on the part of the recipient of an emergency message.

2. State intercepts and information requests from security authorities

Provisions concerning public security, eg the prosecution of crime, are largely excluded from European harmonisation (see Article 15 E-Privacy Directive). In the Federal Republic of Germany, the Federal Constitutional Court's double-door model applies, whereby the fundamental legal provisions for transmitting customer data are regulated by the TKG and those for requesting data are regulated in the relevant specialist laws, eg the Code of Criminal Procedure. In other countries, both processes are often regulated by the same security laws.

a. Provisions on the technical implementation of intercepts

Under section 110 TKG, an operator of a telecommunications system by means of which publicly available telecommunications services are provided shall, at his own expense, provide technical facilities with which to implement telecommunications interception measures. It is possible, for example, to provide corresponding hardware and software. The specific underlying technical requirements for this stem from the Telecommunications Interception Ordinance. They are tailored to traditional telecommunications services. Section 110 TKG serves to enable security authorities to access the content of real-time communication, eg telephone conversations or video conferences. Under section

100a of the Code of Criminal Procedure (StPO), intercepts of this kind may only be authorised in the case of serious crimes and by a judge.

Intense discussions are currently taking place in Germany and abroad as to whether these provisions should be extended to OTT-I service providers which also enable real-time communication, eg voice and video telephony or messaging services. It is true that security authorities could receive access to the relevant data packages via the respective access provider, as an operator of telecommunications systems. However, this is often of little use since online communication via, for example, Skype or WhatsApp, is encrypted. The option of accessing the desired communication content by installing software on terminal equipment (known as source telecommunication surveillance) is extremely costly and often not even possible. The seizure of servers and terminal equipment, on the other hand, can only be applied to retrograde processes. In many cases, this is also impossible if servers are located abroad. Other obstacles include cases where security authorities have to go to great lengths to decipher the private PIN of a mobile phone, as was the case with the iPhone of the alleged perpetrator of the San Bernardino attack. Thus, on a purely factual basis, it is possible to identify gaps in protection which lead to the unequal treatment of telecommunications services and OTT services. If section 110 TKG is to be applied de lege ferenda to OTT-I services such as messaging services, the relevant technical directives of the Bundesnetzagentur, which are based on the Telecommunications Interception Ordinance (TKÜV), will have to be adapted accordingly.

Security circles are also calling for effective decryption mechanisms to be made available to authorities at the service level by the providers of WhatsApp, Skype and similar services, as set out in section 8(3) TKÜV. On the other hand, the German Government has declared its intent not to limit the free availability of encryption products in order to promote the development of German IT security technology and help prevent hacker attacks, which have risen sharply in recent years. A series of proposals have also been made to require the storage and processing of OTT-I services in data centres located in Europe. This would considerably facilitate the enforcement of national and European law. However, there is currently no political consensus on the introduction of these and similar measures.

b. Information procedures with regard to customer data

Under section 111(1) sentence 1 TKG, any person commercially providing telecommunications services and in so doing allocating telephone numbers or other forms of line identification must collect and store customer data and, where necessary, make this available to the security authorities. Under the requirements of section 111(1) sentence 3 TKG, the obligation to store (not to collect) data gathered for operational purposes also applies to e-mail providers. According to Cologne Administrative Court's ruling from 11 November 2015, the Gmail service constitutes a telecommunications service and therefore an e-mail service within the meaning of the TKG. For other OTT-I services, it is decisive that a provider issues a subscriber (customer) with a fixed identification code. The term "line identification" has no legal definition. The committee recommendation and report of the Committee on Legal Affairs (6th committee, Bundestag printed paper 16/6979, 46.) from 7 November 2007 indicates, however, that dynamic IP addresses are not to be included in this category. For the sake of clarity in this respect, a legal definition should be provided de lege ferenda.

c. Data retention

With sections 113a to 113g TKG, the Federal Republic of Germany is once again pushing for the introduction of data retention provisions. The primary legislative objective in doing so is to enable effective criminal prosecution. Under European law, there is currently no obligation to introduce a statutory duty to retain data.

Under section 113a(1) sentence 1 TKG, parties subject to the obligation are all providers of publicly available telecommunications services for end-users. The retention obligation covers not only traditional call numbers and the beginning and end of calls, but also in the case of internet telephone services the internet protocol address of the calling and called connection. The same applies to the transmission of SMS text messages as well as multimedia and similar messages. Call data must be retained for ten weeks and location data for four weeks.

De lege lata, OTT-I services are usually not subject to the strict provisions of the TKG regarding the retention and, in particular, deletion of traffic data under sections 113a ff TKG. In practice, OTT-I services in many cases voluntarily retain the data they accrue (based on user consent, for example) for a period longer than that required under the retention obligations for traffic data of section 113b TKG. If the scope of application of data retention were to be extended de lege ferenda to OTT-I service providers, a uniform retention period would apply to the traffic data specified in section 113b TKG. On the one hand, this would have the advantage that supervisory authorities could rely on this traffic data being available for this period at the service provider. On the other hand, however, this would also mean that, at the end of the retention period, this data would have to be deleted from the data retention systems of service providers. Insofar as there is no other legal basis for permitting the retention and use of traffic data under the TKG, the data would have to be deleted from all of the service provider's systems.

3. Preliminary conclusions

To close existing gaps in the protection of public security and creation of a level playing field, a variety of clarifications are required de lege ferenda. The term "line identification" within the meaning of section 111 TKG must be defined. The security requirements under section 109 TKG must be adapted to reflect the risks to public security arising from OTT-I services. Decisions must be made on fundamental issues regarding telecommunications intercepts, including the use of encryption mechanisms or possibilities for accessing foreign servers which process OTT-I services.

VII. Recommendations for the further development of the legal framework and regulatory practice

Telecommunications legislation must be adapted to the new challenges presented by the internet. A key objective in this regard is to ensure fair competitive conditions for OTT-I and telecommunications services. The following fundamental considerations should be taken into account when revising the existing legal framework:

- Firstly, the definition of telecommunications services needs to be updated; in particular, the definition should no longer be based solely on the criterion of signal transmission, but should place greater emphasis on the corresponding functions. Where appropriate and possible, we therefore recommend the homogeneous regulation of specific service categories (such as telephone, webmail services, etc), irrespective of technical characteristics.
- However, every extension of the scope of regulation must be accompanied by a review of whether the legal consequences of classifying OTT-I services are appropriate. Such a review must be conducted separately for each individual regulatory instrument.
- Before the scope of regulation is extended to OTT-I services, it is first necessary to examine whether, conversely, the increased competition resulting from OTT-I services does not enable, or in fact require, the deregulation of traditional communications services. If the answer to this question is no in respect of a concrete provision and the need for continued regulation is identified, this would suggest that there is, in principle, a need for the regulatory consideration of OTT-I services. Depending on the interpretation of the applicable law and its scope of application, this must take the form of either a clarification or an extension. Given the pace of development, the creation de lege ferenda of an independent regulatory category for OTT-I services is not recommended as this would, in turn, create new problems with regard to definition, and the differences between "traditional" telecommunications services and OTT-I services are not sufficiently pronounced. The necessary distinction between traditional telecommunications services and OTT-I services can instead be made through the application of these regulatory instruments. Clarification of the respective concrete requirements of services may therefore be necessary.
- Overall, we recommended that legal consequences are made more flexible. This should be factored into the investigation of whether the current regulatory requirements for traditional telecommunications services are still appropriate – especially in light of the rise of OTT-I services. This must also be answered separately for each individual instrument – as with the obligation to provide an emergency calling function. At the same time, it will be necessary to check whether additions are required. It will also be necessary to establish whether symmetric or asymmetric regulation based on specific market power is required.

Specifically, WAR sees the following need for reform, which in order to create a level playing field in the EU should be taken into account, in particular, in the forthcoming review of the regulatory framework for electronic communications:

- The increased competition resulting from new OTT-I communication services may lead to lower prices and reduce the need for regulation of traditional telecommunications services.
- Neither the type of signal transmission nor the specific business model alone should serve as a trigger for differentiated market regulation. Instead, this should be based on market definition from a user perspective and identified market power.

- Traditional communication services, which are in competition with new OTT-I communication services, are also not currently subject to regulation based on market power, at least not in Germany.
- Regulation based on market power applies mainly to wholesale and termination products. For termination, in particular, there may be potential for deregulation, provided competitive access to the internet and therefore to OTT-I services is ensured. However, rather than being judged on a sweeping basis, this should be assessed on a case-by-case basis based primarily on the actual substitution behaviour of users.
- A cautious approach is also advisable with regard to the imposition of interoperability obligations. There is currently no need to impose obligations for the interconnection, or interoperability, of OTT-I services.
- Irrespective of this, it makes sense to create or further clarify the legal basis for the authorised collection of market data with regard to OTT-I services.
- The customer protection provisions of sections 43a ff TKG are less relevant for OTT-I providers than for traditional telecommunications services. These regulations are clearly intended to apply to traditional telecommunications services based on the provision of a network connection. Unlike traditional telecommunications services, OTT-I services are provided via the internet, not via independent physical connections. They are usually non-exclusive (multihoming is normally possible with little outlay and is very common) and the portability of identifiers which are functionally similar to telephone numbers (eg e-mail addresses or user names) is usually not possible or necessary. However, a regulation on the temporary forwarding of e-mails to the new address seems appropriate if the old address is lost when switching providers. Where the customer protection regulations of the TKG refer to charges, these regulations cannot be applied directly to OTT-I services because these services are usually not provided in return for money, but rather data/attention. This raises the question of whether data-related regulations similar in function to sections 45e ff TKG are required (eg to prevent customer exploitation). However, issues relating to the “data economy” are primarily issues for general or specific telecommunications data protection law. Thus, it is worth considering extending transparency regulations de lege ferenda to ensure that users have to be informed about the use of their data.
- The data protection standard of the TMG and, in particular, the general Data Protection Directive is much lower than the standard of the TKG and the E-Privacy Directive. The application of both regimes to electronic communications services (OTT-I communications services on the one hand and traditional telecommunications services on the other) would not result in a level playing field. In terms of fundamental rights, there is much to be said for a uniform data protection standard for traditional telecommunications services and internet-based communications services (OTT-I services). After all, according to the rulings of both the Federal Constitutional Court and the ECJ, a relatively high minimum standard applies to communication services, and this standard is generally differentiated on the basis of the need for protection rather than the business model of the service or technical processing. The TMG and the general Data Protection Directive barely ensure the data protection standard for electronic communications which is nec-

essary to comply with fundamental rights. With regard to a possible differentiation of data protection requirements, it should be discussed whether and to what extent, on the basis of transparent and clear information, it can be assumed in future that a user has given his/her consent for the service provider to exploit data relating to their communication processes. Data protection standards can and must be enforced for every service provider, regardless of whether it is based in an EU or a non-EU country.

- The provisions regarding the protection of public security in sections 108 ff TKG are geared to the conditions of traditional telecommunications. In contrast to regulations in other parts of the TKG, however, they are shaped only minimally by European law. National legislators therefore have a comparatively broad scope of action. Legal action is required with regard to detailed issues. The definition of "line identification" within the meaning of section 111 TKG should be clarified. The security requirements under section 109 TKG should be adapted to the special characteristics of OTT-I services. Provisions on the communications intercepts are traditionally fiercely controversial. The use of encryption technologies results in gaps with regard to intercepts of real-time communication. Another obstacle to access by security authorities is the fact that the desired informed is often stored on OTT-I providers' foreign servers. A fundamental legal policy decision is required to determine whether this problem is to be solved. This decision will be based primarily on security requirements and constitutional principles, which is why WAR, which focuses on regulatory issues, is refraining from adopting a position on this matter. From a regulatory perspective, however, discussion is required as to whether OTT-I providers should contribute to the cost of monitoring OTT-I services which is incurred by traditional telecommunications providers. Further action is also required with regard to the obligation to provide access to emergency services under section 108 TKG. Here, clarification is needed as to whether the authorities empowered to provide emergency services see a need de lege ferenda to extend the regulation, and which possible technical solution is preferred at what cost.

Bernd Holznagel (chairman), Frank Brettschneider, Torsten J. Gerpott, Justus Haucap, Iris Henseler-Unger, Torsten Körber, Jürgen Kühling, Claudia Loebbecke, Albert Moser, Klaus Möller, Franz Jürgen Säcker, Jens-Peter Schneider