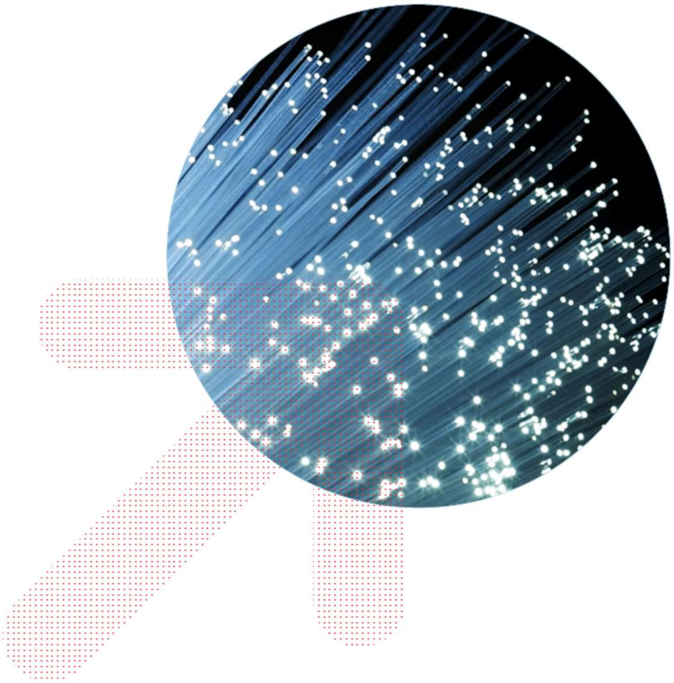
WIK-Consult • Report

Study for the Federal Network Agency



# Interoperability regulations for digital services

## Impact on competition, innovation and digital sovereignty especially for platform and communication services

Authors:

*WIK-Consult:* Dr. Lukas Wiewiorra; Dr. Nico Steffen; Philipp Thoste; Dr. Niklas Fourberg; Serpil Taş; Ing. Peter Kroon

*Univ. Osnabrück:* Prof. Dr. Christoph Busch

*Univ. Passau:* Prof. Dr. Jan Krämer

Bad Honnef, August 2022

WIK CONSULT

## Acknowledgments

The authors would like to thank Prof. Dr. Jörg Schwenk (Ruhr University Bochum), Prof. Dr. Rainer Böhme (University of Innsbruck) and Prof. Dr. Joachim Posegga (University of Passau) for their comments and assessments on end-to-end encryption.

## Imprint

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik-consult.com
www.wik-consult.com

**Authorised representatives and signatories**

| | |
|---|---|
| Managing Director | Dr Cara Schwarz-Schilling |
| Director | Alex Kalevi Dieke |
| Director<br>Head of Networks and Costs | Dr Thomas Plückebaum |
| Director<br>Head of Department<br>Regulation and Competition | Dr Bernd Sörries |
| Head of Administration | Karl-Hubert Strüver |
| Chairperson of the Supervisory Board | Dr Thomas Solbach |
| Commercial Register | Local Court Siegburg, HRB 7043 |
| Tax no. | 222/5751/0926 |
| Value added tax identification no. | DE 329 763 261 |

## Table of contents

## List of figures

## List of tables

## Executive Summary

In this study a lack of ***interoperability (IOP)*** as a potential cause or driver of concentration tendencies, but also as a possible remedy in already concentrated digital markets is investigated. Based on the findings, the need for and the potential impact of IOP regulations for digital services in areas of the platform economy and online communications services, and in particular for number-independent interpersonal communications services (NI-ICS), are examined.

### Background

The ***DMA (Digital Markets Act) regulation***, which is currently being implemented, provides for an IOP obligation for basic features of providers of NI-ICS in addition to regulations in the area of hardware and software features. However, an obligation in the area of social media has been waived for the time being. Similar efforts are underway in the United States (ACCESS Act), the United Kingdom and Australia, among others.

IOP is understood to mean the exchange of information and, in particular, its mutual utilisation for the establishment of features. In general, the understanding of the term and the various concepts of IOP from a technical, legal and economic perspective give rise to a broad, sometimes inconsistent picture. In particular, IOP goes beyond one-off, usually unilateral, data portability and is distinguished from it by continuous, usually reciprocal, data exchange. This form is also referred to as data IOP, while protocol IOP focuses on a more fundamental interconnection and exchange of features. In addition to this two-way IOP, however, there are also one-way forms of IOP, such as the sharing of external media content on social media platforms or so-called adversarial IOP through reverse engineering.

In the platform economy, in addition to competition between homogenous services, there are many upstream and downstream links between different stages of the value chain, whereas online communications services are primarily represented by horizontal competition between the different providers. Horizontal IOP thus concerns firms or services in direct competition and aims at the sharing of direct network effects. Vertical IOP, on the other hand, aims to ensure the sharing of indirect network effects and thus affects companies or services in upstream and downstream markets, which can gain access to another stage of the value chain through IOP.

### Interoperability obligations

The basic argument for ***horizontal IOP obligations*** is to enable users to use alternative providers without losing access to interaction partners who exclusively or mainly use the service of one (dominant) provider. A pro-competitive effect exists through the dissolution of firm-specific network effects or of network-related lock-in effects as well as a reduction of the risk for market tipping. However, horizontal IOP can also have an anti-competitive effect, since homogenization restricts differentiation and innovation opportunities and may reduce existing incentives for multi-homing. It is unclear ex ante which of these effects will ultimately dominate.

Caution is therefore advised with regard to IOP obligations in horizontal competition between relatively homogeneous services and goods. Depending on the market structure and environment, the possibility and exercise of customer-side multi-homing in particular can create competitive pressure even without IOP or IOP obligations. If multi-homing is possible without significant costs, the potential welfare gains from IOP are limited. On the other hand, horizontal IOP entails risks for innovation incentives of the companies involved, since competition *for* the market is replaced by competition *within* the market and the current state of technical development is cemented. Further developments are less dynamic, especially in the case of fixed technical standards, and less attractive due to network effects being shared across the whole market. In addition, possible IOP obligations at the horizontal level can weaken emerging competitive advantages and thus reduce important innovation rents. IOP leads to less product variety between horizontally competing products, implying a poorer match between product characteristics and consumer preferences. The resulting negative welfare effect is particularly significant when consumer preferences are strong.

***Vertical IOP obligations*** can facilitate modular combinations of services across upstream and downstream stages of the value chain and create corresponding innovation incentives. This is particularly the case for established vertically integrated firms. However, "too open" access may inhibit incentives for (radical) innovation among third-party suppliers and platforms themselves.

However, IOP obligations in vertical structures are often favourable overall. Vertical IOP creates planning security via available APIs (application programming interfaces) and promotes innovations by complementary providers. Likewise, mandatory vertical IOP standards ensure access to an entire user base of a market and thus increase the potential demand in upstream and downstream markets.

In addition to the implementation costs of IOP, which can represent a market entry barrier for smaller providers, there are also general pitfalls in standardisation processes due to potential collusion and the influence of dominant players, e.g., through the strategic placement of patents. In terms of digital sovereignty, IOP can enable freedom of choice and self-determination for consumers by reducing lock-in effects on the one hand, but on the other hand make it more difficult to control data processing if, through an interoperable network, providers with which the user has no direct business relationship also have access to their (meta-)data. The effects on the sovereignty dimensions of cybersecurity and strategic aspects are also ambivalent.

## Interoperability of NI-ICS

The ***classification and definition of NI-ICS***, which among other things serves as the basis for the IOP obligation of messaging services under the DMA, still has legal ambiguities in the context of modern online communication services. An assessment of whether, for example, the private messaging feature of Instagram has to be regarded as a *minor ancillary feature of* Instagram as a social network cannot always be determined based on technical criteria and may depend on the dynamic usage habits of users. The distinction is also complicated by the proliferation of services that belong to vertically integrated ecosystems and by a wide range of features. For example, Telegram offers features that, comparable to social media, make information available to an indefinite number of people in open channels, but it is also used analogously to WhatsApp or Signal for bilateral or private communication in groups.

WhatsApp and the services Facebook Messenger and Instagram Messages, which also belong to the Meta group, represent the most popular online communication services, particularly in Europe. A custom analysis of an annual WIK survey on the use of online communication services as part of this study shows that 80% of users in Germany use at least one of these three services. Services from other companies are used by only up to 30% of respondents in each case (Microsoft services) or fewer (other services).

The high proportion of ***multi-homing*** at the service level (75% of users use at least two services, with an average of 3.7 services used) is partially offset by aggregation to the providing companies. Still, 61% of users use services from different companies, and on average 2.8 services are used by different companies. An international empirical study shows that despite the increased number of installations for alternative services, only about 0.5% of users actually uninstalled WhatsApp. Nevertheless, a high proportion of multi-homing can contribute to disciplining the market power of a dominant provider, as it enables faster and less complicated switching between communication channels.

All regulations of the DMA are imposed asymmetrically on dominant so-called "gatekeepers", such that alternative providers are still free to choose whether they want to seek for IOP with gatekeepers or with each other. Market participants and observers were particularly critical of an industry-wide, symmetrical regulation in the run-up, as they feared a lack of opportunities for differentiation and a lack of innovation potential due to excessive homogenisation. In terms of features, the obligation is also limited to the basic feature of exchanging messages and files between individual users, which will be expanded over time to include group chats and calls. Staggered development entails the risk that planning will be outpaced by dynamic market developments, making adjustments at a later date ever more costly. Although providers still have the opportunity to differentiate themselves with independent offerings or additional features, this also impairs the original goal of horizontal IOP, the dissolution of firm-specific network effects.

In addition to the voluntary decision for alternative providers, the preservation of freedom of choice is also emphasised for users, which, however, may further limit the practical benefit of IOP. End users of both the gatekeeper and an IOP requesting provider are to remain free in their decision to use the interoperable features or not. Users can thus decide, for example, whether they actually want to be reachable (and discoverable) by users of each other provider. From a data protection perspective, this will presumably require a granular opt-in model, the design of which, however, poses major challenges in terms of complexity and usability in practical implementation.

Overall, the legal text places a high value on maintaining data security and data protection, whereas there were warnings in advance of a drop to a "lowest common denominator". This includes a data minimisation requirement in which the collection and exchange of data is to be limited exclusively to the level necessary to ensure effective IOP. The same level of protection offered to own users must also apply to IOP with external providers. This explicitly includes the preservation of existing end-to-end encryption, if applicable. This regulation can be understood to mean that maintaining the security level is a hard prerequisite for opening up a gatekeeper's service to other providers. However, the extent to which this resolution can be maintained in practical implementation is highly questionable due to the technical complexity of reconciling IOP and end-to-end encryption.

Existing developers of open messaging standards of their own and aggregation services using so-called bridges ("translators" between different protocols) such as Matrix and Beeper have already expressed their interest in making use of the IOP obligation, while alternative messengers such as Signal and Threema have taken a critical stance and continue to reject cooperation with other services, citing privacy and security risks.

As the example of the Meta group shows, which has not yet been able to fully implement the end-to-end encrypted IOP between its own services announced in 2019, even encryption between services within a firm is already a challenge. Also according to experts for encryption technologies interviewed as part of this study, there can ultimately be no true end-to-end encryption under IOP without complete standardisation or use of a common standard.

In general, the effort required to reach agreement on full standardisation is considered to be extremely high and can be equated to that of the development of a completely new interoperable messenger platform. The implementation of IOP for end-to-end encrypted services and features could therefore still be several years away. Some of the experts surveyed put the time required for complete standardization at several years (up to 5). The implementation and standardisation effort increases significantly from bilateral text messages to group chats and audio and video chats.

In addition, there is the problem, not least for the legal text of the DMA, that the terms of a "security level" and also of "end-to-end encryption" are not subject to a uniform or objective definition. Depending on the application and its value proposition, user (base) and infrastructure, sometimes very different "ends", attack and attacker models can be relevant, which also imply different trade-offs at the technical level. Uniform technical solutions are conceivable in principle at an abstract level, but they reach their limits in detail and in practical implementation. Corresponding compromises and an expansion of the parties and actors involved therefore ultimately also imply an expansion of possible points of attack and thus, in case of doubt, cause a drop in security levels.

The final version of the DMA provides for compliance with the IOP obligations via interfaces for now, but a more comprehensive standardisation requirement is reserved for the future. Given the complexity, a coordinated full development approach could lead to better and less costly results in the long term than the envisaged partial and staggered implementation. However, the arguments against standardisation itself also include similarly high costs, the possible prevention of innovations and risks resulting from the standardisation process, such as strategic influence by dominant players.

Consequently, in particular if IOP were to be implemented with the aid of only interfaces, the existing security level would have to be ultimately softened, or agreement would have to be reached on a (possibly already existing proprietary) encryption standard. The latter option, however, would entail high switching costs for the companies concerned, which would drastically reduce the attractiveness of IOP for alternative providers. It should also be borne in mind that if alternative providers reject IOP, their users will not be able to benefit from the potential advantages of such a solution. Therefore, an attractive solution with broad acceptance is to be considered more desirable. If, on the other hand, an easier-to-implement solution is chosen, with a softening of the existing security level, it is equally questionable whether companies with a currently high security level would implement such a solution and whether users (if implemented) would make use of this option at all.

In the overall assessment, it therefore remains questionable how the approach pursued in the DMA and generally an IOP obligation for messaging services can be implemented in a targeted manner. In view of the possible risks, close regulatory support seems necessary to keep undesirable side effects for consumers, competition and innovation as low as possible. Ultimately, the focus of all IOP regulations is a potential market failure that could be overcome by establishing IOP. If, as in the case of messaging services, the level of multi-homing is comparatively high and the costs of multi-homing are low, a rather low welfare loss for consumers can generally be assumed if an interoperable exchange across providers is not possible. In contrast, there are a number of costs and risks associated with implementing IOP obligations, both through interfaces or standards, such as a reduction in multi-homing, incentives for innovation, security levels including end-to-end encryption and usability. There is thus a risk that such projects will result in interoperable systems that have to be developed at great expense in terms of time and money, but are ultimately not accepted in the market. In addition, (regulatory) costs arise for the continuous monitoring and compliance with the IOP obligations and the maintenance and care of the corresponding interfaces with high quality and availability.

Against the background of the final adoption of the DMA, care should in any case be taken to ensure that the risks described are minimised regulatorily in the best possible way in the practical implementation of the obligation that is now pending and, not least, that the announced focus on consumer aspects such as the preservation of encryption and data minimisation is maintained.

# 1 Introduction

Digital services such as trading platforms, social networks, search engines, messaging services, operating systems or app stores have found their way into various areas of daily life in recent years, bringing about numerous positive changes by facilitating access to information, products and services or offering new ways to get in touch with family and friends. However, with the development of large internet corporations, the internet is becoming increasingly centralised, forming more and more interlocking, closing ecosystems and concentration tendencies (cf. Lancieri & Sakowski, 2021).

In this context, providers of closed and proprietary services can exploit lock-in effects through network effects and after reaching critical mass, thereby further increasing their market power. Also across vertical value chains, lack of access can prevent the emergence of complementary services and competition in upstream and downstream markets. This can affect both the immediate features of services such as NI-ICS (Number-independent Interpersonal Communications Service) and the integration of these services into the wider digital ecosystem of platform operators (e.g. smart home, streaming services, social networks, etc.). This could in turn lead to negative welfare effects, as customers do not use alternative offers, accept worsened conditions of use, or providers have fewer incentives to invest and innovate.

This study will therefore examine a lack of interoperability (IOP) as a potential cause or driver of concentration tendencies and associated negative welfare effects, but also IOP as a potential remedy for already concentrated digital markets. Based on the findings, this study will then examine the potential need for and impact of IOP regulations for digital services in the areas of the platform economy and online communication services, NI-ICS in particular. A particular focus lies on the effects of IOP regulations on competition, innovation and the realisation of aspects of digital sovereignty in the form of self-determined action by market participants.

The study is structured as follows. Chapter 2 provides a basic overview of IOP. It classifies and distinguishes the term in relation to related concepts and defines its understanding in the context of this study. Subsequently, different types, characteristics and forms of implementation of IOP are presented. In addition, the Chapter discusses basic interrelations and effects of IOP on competitive processes, innovation incentives and consumer aspects.

Chapter 3 looks at IOP in the general context of digital platforms and services, analysing the potential role of IOP in the platform economy. It discusses the status quo of IOP in the platform economy, a potential lack of IOP, and possible IOP obligations as a remedy. The desired positive effects of IOP are contrasted with the identified risks and various market constellations are discussed that can influence a corresponding trade-off. Based on this, a test scheme for the assesment of possible IOP regulations in the context of digital services is established. Furthermore, technical and procedural aspects and hurdles for (the introduction of) IOP are outlined.

Chapter 4 focuses on online communications services and in particular NI-ICS, for which a partial IOP obligation is envisaged under the Digital Markets Act (DMA). First, online communication services and NI-ICS are distinguished from each other and the current market situation is described. Referring to the test scheme from Chapter 3, specific market characteristics and economic features are elaborated. In particular, technical aspects are discussed that would be necessary for different implementation approaches of IOP in this market segment. The focus is on the question of whether and how these approaches to IOP are compatible with end-to-end encryption. For the different approaches to implementing IOP, an assessment is made based on economic, technical and legal aspects and the current approach of the DMA is assessed.

Chapter 5 summarises the conclusions of the study and offers an outlook on future developments.

# 2 Effects of different interoperability concepts

## 2.1 Interoperability concepts

### 2.1.1 Compatibility and interoperability

In technical contexts, *compatibility* generally refers to the functioning of parts together. Accordingly, in an early overview article on compatibility and standardisation, Farrell & Saloner (1986a) define compatibility as the result of coordinated product design. The authors distinguish between three classes of compatibility:

- *Physical compatibility* (e.g. cameras and lenses, cars and petrol pumps, TVs and broadcasting systems, etc.)
- *Communications compatibility* (e.g. telephone systems, street signs, national languages, etc.)
- *Compatibility by convention* (e.g. currencies, time zones, bank cards, etc.)

However, the authors note that these categories are neither exhaustive nor distinct. For example, telephone systems and street signs are also based on compatibility by convention. Furthermore, according to the authors, compatibility also depends on whether products from the same manufacturer are considered or products from different manufacturers. Particularly when using products from different manufacturers, there may also be only partial compatibility. The authors have thus already touched on many aspects of this topic, which were further specified and sharpened in later research work.

In the context of digital products and services, IOP can be broadly defined as the ability of two or more software components to work together despite differences in language, interface and execution platform (Wegner, 1996, p. 1). The concepts of compatibility and IOP are often used synonymously or at least not distinctly. In the following, different definitions of IOP will be presented in order to work out a working definition for this study.

The ISO/IEC/IEEE Directory of Technical Terms in the Field of Systems and Software Engineering (ISO, 2017, p. 79) defines ***compatibility*** as, among other things, the "degree to which a product, system, or component can exchange information with other products, systems, or components, or perform its required features, while sharing the *same hardware or software environment*" and "the ability of *two or more systems* or components to *exchange* information*"*. Other definitions explicitly refer to the aspect that technical components are compatible with each other as long as both are in the same environment (e.g. operating system) *without affecting the behaviour of the other component* (TestingStandards.co.uk). This implies, for example, that mutually compatible software can function on the same end device without conflicts, but that functionality between the two software components or across different end devices does not necessarily have to be ensured. However, compatibility can also include overlapping functionality between, for example, different software and operating system versions or even end devices. For example, the database provider Oracle refers to compatibility as the ability of systems with different versions (or releases) to interoperate (forward and backward compatibility) (Oracle, 2010).

***IOP*** is defined in the ISO/IEC/IEEE Directory of Technical Terms for Systems and Software Engineering (ISO, 2017, p. 237) as the "the degree to which two or more systems, products or components *can exchange* information and *use the information* that has been *exchanged"* and "capability of objects to *collaborate*, that is, the capability mutually to communicate information in order to exchange events, proposals, requests, results, commitments and flows." According to this definition, IOP does not focus specifically on functionality within a hardware or software environment and also explicitly takes up the aspect of the usability of information exchanged between systems, products or components and thus the *cooperation of systems.* The database provider Oracle describes IOP as the ability of systems of the same version (or releases) to work together (Oracle, 2010).

In this technical context, compatibility therefore often refers only to the interchangeability of different dependent components (e.g. newer/older, variant A/B) in an environment to achieve functioning of a specific feature, as well as the trouble-free coexistence of components within the same technical environment, which can also be functionally independent of each other. In the case of forward or backward compatibility, additional technologies are often necessary, so-called adapters or converters (see Chapter 2.1.2), which mediate between the diverging versions or designs of technologies.

Although IOP is often used synonymously with compatibility, this concept focuses more specifically on the cooperation of systems in different environments and the usability of the transmitted information across system boundaries. Depending on the definition, the concept of IOP is therefore already based on the prerequisite of a common standard.

In a general analysis of IOP in the context of data-centred research activities to achieve IOP between two entities[1], Thanos (2014) identifies different concepts that can determine IOP:

- Exchangeability: The two entities must be able to exchange *meaningful information*.
- Compatibility: The two entities must be able to exchange *logically consistent information* (if the information exchanged is a description of functionality, policy or behaviour).
- Usability: the user instance must be able to *use the information exchanged* to perform a range of tasks that depend on the use of that information (Thanos, 2014, p. 89).

[1] An entity is an information object in data modelling. This means a uniquely identifiable object about which information is to be stored or processed. Such an object can be, for example, a user account, a state or even a physical object.

To ensure a meaningful exchange of information between two entities in terms of interchangeability, three types of heterogeneity must be overcome. First, heterogeneity between data formats and the languages used to query the data (syntactic interchangeability); second, heterogeneity between data models (structural interchangeability); third, heterogeneity in semantics describing, for example, dimensions such as granularity, scope, time, synonyms, homonyms, etc. (semantic interchangeability). If the interchangeability alone is sufficient to enable the user entity to perform a set of tasks based on the exchanged information, this is called "basic IOP".

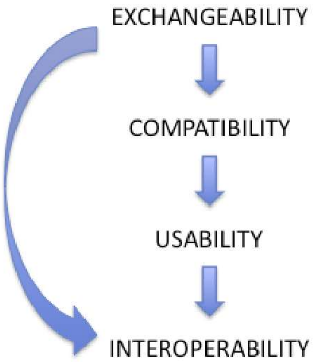
Compatibility additionally ensures that no discrepancies occur, e.g. at the functional level, in behaviour and business logic. Compatibility therefore means that the first condition (interchangeability) is met, as well as logical consistency in all dimensions relevant to the collaboration. A compatibility check therefore first requires a description of the static characteristics of a service. However, this only describes the abstract capabilities of a service, but not under which conditions and circumstances the service can actually be provided. Therefore, a description of the dynamic characteristics of a service must also be available. These describe which information or specific conditions are required for the provision of a service. However, compatibility does not necessarily imply that two compatible services (components) can be combined with each other, e.g. to provide a new service, as is regularly the case in the platform economy (service composition). Compatibility is therefore no guarantee for IOP (Thanos, 2014, p. 91).

"Usability is accomplished when perceived usefulness and perceived ease of use of data/tool/service are tightly linked" (Thanos, 2014, p. 92). This means that the data provided by a provider's service must also be provided with additional information in order to be usable by other users. This condition refers to the availability and consistency of metadata information in addition to the accuracy, completeness, consistency and timeliness of the data provided itself. If, for example, a service is to be used by different user groups or for different application scenarios, different (or richer) metadata information must be made available in order to be able to establish IOP in all these cases.

Overall, the conditions presented build upon each other. This means that interchangeability is a necessary but not sufficient condition for compatibility. If exchangeability alone is already sufficient to enable an entity to perform a number of tasks based on the exchanged information, we can speak of *basic IOP.*[2] Furthermore, both interchangeability and compatibility are necessary but not sufficient conditions for usability. Only when interchangeability, compatibility and usability are guaranteed, *full IOP* is achieved. *Thus, compatibility is a weaker concept than IOP* (Thanos, 2014, p. 93).

[2] The direct arrow in Figure 2-1 indicates "basic interoperability" if interchangeability is sufficient as the sole condition.

Figure 2-1: Hierarchy of conditions for IOP



Source: Thanos (2014, p. 93)

While other authors also explicitly use the terms interchangeably from an economic/legal perspective (Lemley & Samuelson, 2021), Kerber & Schweitzer (2017) transfer the technical view of IOP to digital markets and define IOP in terms of the *functionality and cooperation of products from different companies,* while compatibility from their perspective typically refers to the ability of products from one and the same company to function together. This definition can thus not be seen as fully consistent with the definition of Thanos (2014), but it does aptly underline that usability, as a prerequisite for IOP (after compatibility alone), is more of a challenge across company boundaries than within a company, where there is already relevant metadata and knowledge about how to interpret it correctly. Riley (2020, p. 101) concludes that effective IOP in the context of digital markets thus requires not only common standards, but also compatibility. Standards therefore also relate in particular to the creation of usability across the boundaries of individual environments such as the ecosystem of individual companies.

**Working definitions of compatibility and interoperability**

In the context of this study, **compatibility** is understood as the *unimpeded operation and consistent interchangeability of* components, applications and systems, especially *within an environment.*

**Interoperability (IOP)** refers to the *cooperation and combinability of* components, applications and systems that may be located *in different environments.*

In the context of digital markets, an environment can be understood as the technical sphere of influence or ecosystem of a company.

In the following, the concept of IOP will be further explored. To this end, various dimensions and aspects of IOP will be further elaborated.

### 2.1.1.1 Interoperability as a continuum

IOP between different applications may vary depending on the scope of the features mapped. For example, a subset of all features provided by a specific application may be interoperable with other applications, while the remaining features are only available to the users of the corresponding application itself. Between the extremes of "full IOP" and "no IOP", analyses of ***partial*** IOP can also be found in the literature, which suggest this spectrum (Chou & Shy, 1993).

Furthermore, IOP can also be located in a temporal continuum. While ***data portability*** refers to a selective export of data from an application or a service, which is available for import when switching to another service, full IOP can be seen as the automated two-way exchange (export and import) of data between services in real time. Data portability is therefore also possible for services that are not interoperable in operation, but requires at least an exchange capability.

Crémer et al. (2019) distinguish between different types of IOP in these two dimensions. **"Protocol IOP"** ensures that two systems are fundamentally interconnected and can function together. This enables the establishment and provision of complementary services. Standards may thus be necessary to establish protocol IOP. Under full protocol IOP, substitutes of services can also be made interoperable with each other. This can, for example, concern the IOP of messaging services or Internet-of-Things products. This definition of protocol IOP thus corresponds to the classic view from competition law and includes, for example, operating systems, as well as telephones and chargers.

**"Data IOP"** refers to real-time data exchange according to Crémer et al. (2019) and can thus be seen as the continuous form of data portability for which so-called APIs (application programming interfaces) are usually required. This can, for example, enable the development and integration of third-party add-ons for prominent applications and services. In such a situation, users can switch to a new provider without losing access to network effects emanating from users who remain with the old provider. This can be illustrated by the example of a social network. Even if a user were able to take their data to a new social network, they would still not be able to interact with the users who remain with the old network. In this context, it has been argued that "identity portability" (Gans, 2018) or "social graph portability" (Zingales & Rolnik, 2017) - both actually a form of protocol IOP - would be desirable to overcome user-side network effects. Identity portability in this case even means that a person can move to a new network and take their identity with them, so that all messages relating to that person are forwarded to the new network, and vice versa. The idea of identity portability is thus comparable to the interconnection associated with number portability in telecommunication networks.

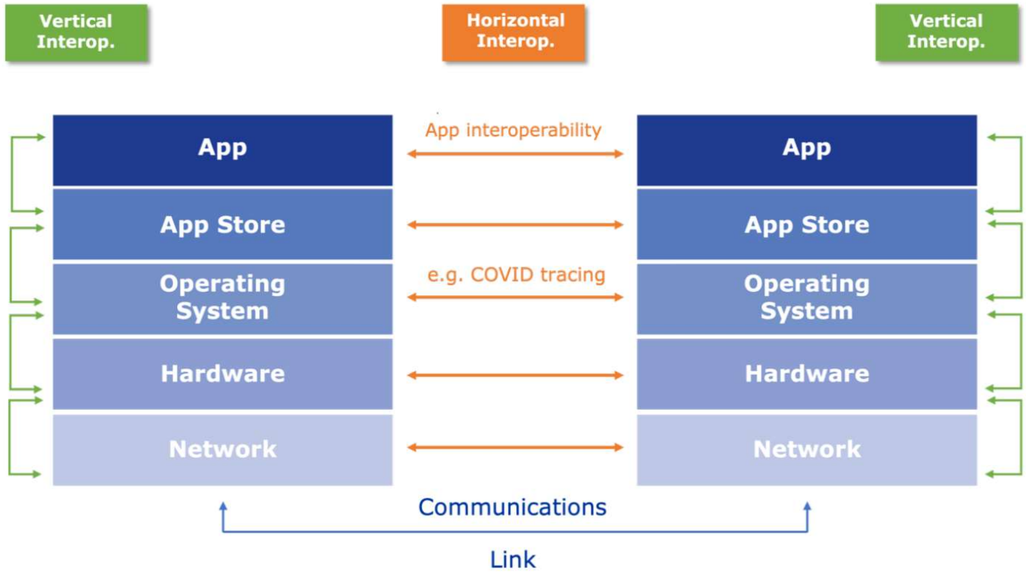
### 2.1.1.2 Horizontal and vertical interoperability

A further distinction can be made between **horizontal IOP (similar services)** and **vertical IOP (upstream and downstream stages of the value chain)** (Riley, 2020). In this context, it is crucial whether these services are in direct competition with each other or whether one service in particular influences the competition of services at upstream or downstream stages of the value chain.

The case of horizontal IOP describes, for example, the situation of messaging services that can be perceived by consumers as substitutes and are thus in direct competition with each other at the same value creation level. In this case, IOP concerns in particular the access or sharing of direct network effects between services. For a number of products and services, the benefit gained by a consumer through consumption is not always the same, but depends strongly on how many other consumers also demand and use the product or service. This characteristic is typical, for example, for communication services of all kinds or for hardware and software systems. A messenger thus becomes more attractive the larger its user base is to communicate with. These positive demand externalities are also commonly referred to as network effects, which can be distinguished in terms of a direct as well as indirect channel of impact (Farrell & Klemperer, 2007; Katz & Shapiro, 1994). Direct network effects exist when the benefit for consumers depends positively on the number of other consumers of the same service or service system (see messengers). Indirect network effects, on the other hand, work through the number of actors on another side of the market or at another level of the value chain. For example, a large user base of a hardware system promotes the supply of corresponding suitable software, which in turn creates a positive benefit for the users of the hardware system.

The case of vertical IOP is particularly relevant in the context of digital platforms and ecosystems, where services can be vertically combined and orchestrated across the value chain (Jacobides & Lianos, 2021b). According to Evans (2003), a platform is understood as providing the possibility of interaction and coordination between at least two market sides in the function of an intermediary. As conditions for the establishment of a platform, Evans names at least two distinguishable market sides, (potentially) realisable externalities from coordination and the intermediary as an internalising instance of these externalities. If the network effects are not limited to a specific user group, but also influence one or more other user group(s), we are speaking of cross-group network effects. If cross-group network effects can be observed between two user groups (e.g. A and B) *in both directions,* we speak of indirect network effects, since in this case the benefit for a participant in group A depends on the number of participants in group B, whose benefit in turn depends on the number of participants in group A. Thus, the utility of a participant in group A depends indirectly on the number of participants in group A. These cross-group network externalities are internalised in platform markets through intermediaries such as matching platforms. Parker et al. (2020) therefore define a platform as a digital resource for realising efficient interactions of market sides such that value creation can be enabled. For this purpose, they distinguish between platforms that aggregate, such as search engines, or digital marketplaces that enable matching between two market sides. In this case, IOP concerns in particular the access to a value creation stage by upstream and downstream providers and thus the access or sharing of indirect network effects. This distinction between horizontal and vertical IOP was subsequently taken up by various authors (Bourreau, Krämer, & Buiten, 2022; Mancini, 2021; Steffen, Wiewiorra, & Kroon, 2021).

Figure 2-2: Horizontal and vertical IOP in mobile ecosystems.



Source: Bourreau et al. (2022, p. 15)

Figure 2-2 illustrates the relationship of these two concepts in the context of mobile ecosystems. Building upon the physical communication layer (radio waves), the network layer is situated. At this level, standardisation (e.g. 5G, LTE, GSM) already results in IOP, since any terminal device that has implemented the corresponding standards can be used in all mobile networks and can communicate with each other. However, the interconnection and thus IOP of these networks is mandated by regulation. The value creation stages based on this, however, have not been subject to mandatory IOP regulations so far. At the hardware level, there are also standardised interfaces (e.g. Bluetooth, NFC) that enable IOP on this level (e.g. the use of any Bluetooth headset or headphones with any terminal device). There are also examples of IOP at the operating system level, which builds on this. The operating system feature of COVID-19 tracking rolled out during the pandemic, which forms the basis for the Corona warning app, is also interoperable between the two dominant mobile operating systems (iOS, Android). The next value creation level is represented by software marketplaces, which are currently not interoperable between providers of different mobile operating systems on a voluntary basis. However, examples of voluntary IOP can be found at the mobile application level. Service providers such as Dropbox enable data sharing across the boundaries of different mobile ecosystems. Similarly, different mobile video game providers allow "cross-play" features that allow players to play together across platforms between different operating systems.

Vertical IOP in this context refers to the combination of features beyond the boundaries of individual value creation stages. In this context, for example, the Corona warning app requires access to the COVID tracking functionality of the operating system in order to issue corresponding warnings to individual users. The operators of the two large ecosystems (Apple, Google) currently only grant access to this interface to one state-verified provider per country, thus specifically restricting IOP. In addition, the providers unilaterally specify the interface to the app operators. Similarly, a banking app that wants to process payments for its customers via a mobile device needs access to the respective NFC interface. This access to the NFC interface and thus vertical IOP is handled differently by Apple and Google. While Google grants app developers relatively free access, Apple handles access to the NFC interface of its end devices very restrictively.

The distinction between horizontal and vertical IOP therefore appears to be a particularly useful distinction in the context of this study, as it can clearly contribute to a differentiation between relevant services of the platform economy and online communication services. While in the platform economy, in addition to the offer of similar services, there are many upstream and downstream links between different value creation levels, online communication services primarily exhibit a horizontal relationship between the different providers.

#### 2.1.1.3 One-way (asymmetric) and two-way (symmetric) interoperability

With **one-way (asymmetric) IOP** it is possible to transfer information directionally to or from an application, without a two-way exchange between two applications. In contrast, with **two-way (symmetric) IOP,** exchange between users of different applications and services is possible in both directions (Manenti & Somma, 2008).

In the case of asymmetric IOP, service providers may, for example, offer features that increase migration to their platform or its reach, while restricting features that could increase migration to or reach from competing services. A concrete example can be found in import and export features for smartphones. Apple and Google each offer apps for OS switchers on competing operating systems to facilitate switching to their own platform, but do not actively support migration to other operating systems through a dedicated export feature. This example is discussed in Chapter 2.1.2 in the context of adapters and converters. The Competition and Markets Authority of the United Kingdom (CMA, 2020) also found that social media platforms rarely offer APIs reciprocally. Facebook, in this context, allows competing platforms to easily share content on its platform through interfaces. In contrast, Facebook users have very limited access to comparable features to share Facebook content on other social media.

If IOP is established against the will of a company, this is called **adversarial IOP**. Examples of this are printer cartridges from third-party manufacturers that circumvent the authentication of the printer's recognition as an original accessory, or modified versions of the WhatsApp messenger that are widely used in Africa, for example. This can be achieved, for example, through so-called "reverse engineering", i.e. replicating what is actually a proprietary implementation of an interface or software component. In this case, the company in question can, for example, defend itself against the unwanted IOP by making rapid and frequent technology changes, which results in frequent interruptions of the IOP for consumers. In addition, the companies concerned are also open to pursue legal action if they hold patents on the technology necessary for the IOP, which are used by competitors (or manufacturers of complements) without consent.

These examples illustrate that horizontal IOP can be symmetric or asymmetric. In contrast, vertical IOP is always asymmetric, since a platform only grants unilateral access to a value creation stage for third-party providers, but not vice versa (Bourreau et al., 2022).

In principle, a company can therefore confront IOP in a cooperative ("invitation" of complements, accessories, add-ons, etc.), adversarial (e.g. reverse engineering) or indifferent (not positively or negatively influenced economically by IOP) manner.

### 2.1.2 Bypassing incompatibility: adapters/converters and multi-homing

In the economic literature, however, there are also discussions and analyses on the use of so-called **adapters or converters** for establishing IOP (Farrell & Saloner, 1992). In this case, there is no need for a uniform standard and in some cases also no need for cooperative behaviour, but a (technical) link provides the translation between two systems that are actually not compatible. Adapters or converters can thus be seen as translators between non-standardised systems or two systems that follow different standards. Via these technologies, IOP can partly be established without the direct consent of one of the two sides and only asymmetrically. A two-way converter corresponds to the possibility offered by many programmes to read and save in the format of a rival (Farrell & Saloner, 1992; Manenti & Somma, 2008).

Ultimately, the goal of IOP is the exchange of information between users across the boundaries of specific services or operators for the provision and use of a service. Even in the case where there is no single standard for a specific service category and no adapters or converters are available, consumers can overcome incompatibilities through **multi-homing** by themselves (De Palma et al., 1999; Doganoglu & Wright, 2006). Multi-homing, i.e. simultaneous use of different services, is thus another way for consumers to benefit from the network effects of different services simultaneously. Of course, multi-homing can involve additional costs for consumers (e.g. effort, time, monetary costs) and is thus only an attractive option for overcoming incompatibility if these costs are comparatively low or negligible (Belleflamme & Peitz, 2019). From the company's point of view, the relationship between compatibility and profits depends on two opposing effects. On the one hand, low compatibility under multi-homing increases demand and thus profits; on the other hand, low compatibility leads to stronger competition at the output level and thus lowers profits. Under multi-homing, therefore, asymmetric equilibria can occur in which large firms would prefer the lowest possible degree of compatibility, while smaller firms would prefer full compatibility (De Palma et al., 1999).

### 2.1.3 Compatibility by convention: standards

A **standard** is a set of technical specifications that are adhered to by a manufacturer either tacitly or by formal agreement (David & Greenstein, 1990, p. 4). Most often, IOP requires the definition of a standard, i.e. a convention (e.g. data formats, interfaces and features) of how data can be exchanged and interpreted between different services to provide specified features on a regular operational basis. Establishing IOP in this case requires the availability of or agreement on a common standard. Standards can arise both **de facto** (ex post in the market) and **de jure** (established ex ante). Well-known de jure standards are, for example, the ISO or DIN standards shaped by public standardisation organisations. But private standardisation organisations can also produce de jure standards, such as the Bluetooth short-range radio standard (headsets, headphones, peripherals, etc.), which is shaped by the "Bluetooth Special Interest Group"[3] staffed by well-known technology companies.

In the economic literature, standardisation is analysed from different perspectives, which are briefly presented below.

#### 2.1.3.1 Standards wars

Standards wars describe the market dynamics in a situation where the parties involved have not agreed on a standard ex ante. Therefore, there are different (technical) approaches or formats for a specific purpose that customers can choose from. Through consumer choices, proprietary technologies can establish themselves as a generally used standard (de facto) through market penetration, if customers prefer one of the available alternatives over time. In this process, direct and indirect network effects, for example through the availability of complementary products, usually play a crucial role. The economic literature on market-based ex post standardisation and the relevant dynamics is very extensive (Besen & Farrell, 1994; Clements, 2004; Economides, 1996; Farrell & Saloner, 1985a, 1985b, 1986b; Katz & Shapiro, 1985, 1994; Regibeau & Rockett, 1996). From the recent past, there are many examples of standards wars and de facto standardisation. These include the popular Microsoft Office formats, Adobe's Portable Document Format (PDF) or the BluRay format, which has prevailed in the market for physical video data carriers against the HD DVD as the successor to the classic DVD.

[3] Bluetooth (2022)

#### 2.1.3.2 Coordination and coalition games

Farrell & Saloner (1988) were the first to investigate the efficiency of a hybrid standardisation mechanism. In addition to the market-based solution, this also takes into account coordination via a committee in which the parties involved can meet and coordinate. The authors find that hybrid standardisation can be superior to the two pure forms of standardisation, as it gives firms more opportunities to coordinate before entering the market, thus avoiding the negative effects of standard wars or incompatibility.

Comparable analyses exist in the context of standard setting coalitions. Often a market cannot be persuaded to adopt a standard by a single actor and its product. Therefore, the formation of coalitions (e.g. computer manufacturers, software providers, peripheral equipment providers) can be productive. In practice, there are often alliances behind many of the formats discussed in Chapter 2.1.3.1, that want to jointly establish a standard on the market. Alliances are more stable if the size of the alliance increases and more unstable if there are (close) rivals in the alliance (Axelrod et al., 1995). From a theoretical economic perspective, firms first decide to join a standard alliance and then find themselves in an oligopoly game in the market. By joining an alliance, a firm benefits from the network effects generated by all members, but subsequently faces increased competition in the product market. Therefore, the extent of network effects can have a significant impact on the alliances formed. When network effects are very strong, all firms join together in an alliance and there is complete compatibility. If network effects are weaker, one company may already deviate and offer a standard on its own, while all remaining companies remain in a common alliance. At the other extreme, with very weak network effects, there is complete incompatibility, as none of the companies want to join forces (Economides & Skrzypacz, 2003).

##### 2.1.3.2.1 Waiting games (wars of attrition)

In formal ex ante standardisation processes, the aim is to reach consensus within the framework of committees and boards. It must usually be assumed that costs are incurred in this process, which increase for all participants the longer it takes to reach a consensus. This situation can be described as a war of attrition, as the participants have to incur costs in each round of the coordination game in order to continue participating in the process. The goal in a war of attrition is to be the last participant in the process to have the upper hand and thus to be able to significantly influence standardisation. Players who are already unwilling to continue to bear the costs of reaching consensus earlier drop out of the process, leaving the remaining player(s) with decision-making power. The value of being able to significantly influence the setting of a standard is determined by the business success influenced by it and a possible reduction of one's own costs if one's own technical solutions can continue to be used and thus, for example, economies of scale or scope can be achieved. These processes therefore bear the risk that the aggregated costs invested by all participants to emerge successfully from standardisation exceed the value of the standard. Therefore, in some cases, direct random selection may outperform the outcome of a war of attrition. Moreover, the outcome of such a situation is determined by the composition of the players. Participants without strong vested interests, or a reduction in the vested interests of all players, can thus reduce delays in standardisation and increase the ex ante incentive to improve the proposals introduced into the standardisation process (Bishop & Cannings, 1978; Farrell & Simcoe, 2012a).

#### 2.1.3.2.2 Signalling games

Standardisation can also be understood as a signalling game. In this case, consumers view a standard as comparable to a seal of approval or certification. Standardisation organisations are called upon by the owners of technologies and decide on the proposals submitted with varying requirements on the quality of the proposals. Sophisticated standardisation organisations are more difficult to convince of a proposal than less sophisticated standardisation organisations, as they put more weight on the interests of consumers rather than companies. Consumers perceive these differences in standardisation and appreciate a more demanding and consumer-friendly standardisation. Therefore, a DIN standard, for example, is perceived by consumers as more binding and far-reaching than a purely industrial standard such as Bluetooth. Thus, a company's decision on the appropriate standardisation organisation for a technical proposal becomes a crucial strategic variable. With regard to the consumer's optimisation problem, standardisation thereby influences the conditional expected value of the true (for them unobservable) quality of a technology and thus creates (depending on the quality claim of the standardisation organisation) more or less certainty in the purchase decision (Chiao et al., 2007; Lerner & Tirole, 2006).

## 2.2 Effects on competitive processes

IOP according to the working definition used in this study (cf. Chapter 2.1) is mainly examined in the economic literature under the umbrella term of compatibility. Accordingly, interoperable services share common features and corresponding competitive effects affect the user base of interoperable services equally. Of main competitive interest in this context are in particular the different effects of IOP between horizontally competing services and IOP to upstream and downstream market stages (Farrell & Saloner, 1985b; Katz & Shapiro, 1985).

The main motivation for introducing IOP from an economic perspective is to dissolve firm-specific network effects so that resulting utility gains from the size of the network benefit consumers of all interoperable services. This basic mode of operation of IOP implies a number of competitive as well as innovation economic effects, which are explained in general terms in this Chapter.

### 2.2.1 Interoperability and competition

#### 2.2.1.1 The role of network effects

In a horizontal competitive environment, where there is no IOP between services, the benefit of any network effects for consumers of a service arises only on the basis of the user base of the respective provider. A (symmetric and complete) horizontal IOP resolves this situation and the relevant network size on the basis of which network effects arise in such a scenario includes the consumers of all interoperable services. By combining the market shares of the horizontally interoperable providers, the resulting network effects are maximised and thus, ceteris paribus, welfare gains are realised in static competition (Katz & Shapiro, 1985). However, resulting second-order effects, such as changes in prices and the ultimate distribution of these additional network rents between producers and consumers, depend on other market conditions such as market structure or demand elasticity. Implications for the dynamic competition perspective are the subject of Chapter 2.2.2.

#### 2.2.1.2 Interoperability as a corporate strategy

In addition to an externally postulated IOP of products, there are also inherent incentives for companies to establish IOP of their products and services themselves. If the technical implementation of this is generally possible, either unilaterally through converters or multilaterally through market-driven standards (see Chapter 2.1.2), IOP becomes a strategic decision variable in economic terms, similar to market prices or quantities offered. As a result, the private and societal (welfare-maximising) incentives to produce IOP can vary significantly.

This is especially true for firms that already have a large user base or market share and whose users would benefit comparatively little from horizontal IOP to other products and resulting additional network effects. Katz & Shapiro (1985) indicate that large firms have significantly stronger incentives to maintain "non-interoperability" even if IOP is desirable and efficient from a welfare perspective. Conversely, smaller firms with a small user base benefit particularly strongly from an IOP between products. Consequently, they prefer to introduce IOP even if it is inefficient from a welfare perspective.

Different incentives for the introduction of vertical IOP in particular can also exist with regard to the temporal sequence of opening. In a so-called "open early - close late" strategy, a platform benefits in the early product cycle from innovative complementary products and can thus increase its attractiveness (Eisenmann et al., 2009). The more established such a platform service becomes, the stronger the incentives to integrate successful complements and features into the platform and provide them themselves (so-called "sherlocking"). Reducing vertical IOP at this advanced stage then becomes more attractive from the platform's point of view.

#### 2.2.1.3 Dissolving market concentration and market tipping

Possible asymmetries in market shares ("installed bases") are particularly relevant in markets of the platform economy and for communication services, as there are especially strong positive network externalities here. In such markets, it is essential for providers to gain a "critical mass" of customers for their own product as quickly as possible in order to be able to optimally use company-specific network effects and realise a competitive advantage. In such a "competition for the market" environment in the sense of Rochet & Tirole (2003) it can therefore lead to a complete "market tipping" and ultimately a strong market concentration on one or a few suppliers. In such a market situation, dominant firms have no incentive to engage in horizontal IOP, while firms that want to release a new product or newly enter the market would benefit from this.

Chen et al. (2009) show that IOP of products and breaking the exclusivity of network effects at the dominant supplier can help to counteract market concentrations. In an already concentrated market, however, this ex post introduction of horizontal IOP is not incentive-compatible for the dominant firm and will therefore not occur in a symmetric form driven by the market. In markets with a comparatively small difference in market shares, i.e. which are not yet "tipped", there may be incentives to introduce horizontal IOP for all competing firms. In such a symmetrical scenario, benefits from realised network effects accrue to all market participants to a comparable extent and IOP acts like an increase in market size. A market-driven introduction of IOP is thus strategically advantageous for the companies. Chapter 3.2.1 specifies the possibilities of counteracting market concentrations in digital platform markets with a horizontal IOP regulation.

#### 2.2.1.4 The role of multi-homing

In principle, horizontal IOP between products is not the only way to fully exploit firm-specific network effects in a market. If it is possible for consumers to use several competing products and services side by side, then so-called multi-homing is present and corresponding network effects can occur to the full extent. For example, consumers can use several messaging services at the same time in order to reach the user base of one provider as well as the other. If multi-homing is possible without significant additional costs, i.e. non-monetary transaction costs as well as monetary product prices are low, then the potential gain from horizontal IOP is limited. If multi-homing is only possible to a limited extent and is associated with significant additional costs, multi-homing is only an imperfect substitute for actual IOP as Doganoglu & Wright (2006) show. Costs incurred through multi-homing are not internalised by firms and could be avoided in a welfare-enhancing way through a horizontal IOP scheme. The model of Doganoglu & Wright (2006) assumes, however, that the network benefit is not very pronounced, so that markets do not collapse and several (horizontally differentiated) suppliers can establish themselves in the market even without IOP. The model therefore has only limited explanatory power in markets with very strong network effects that can tip. Since in “tipped” markets there is only one dominant supplier, multi-homing is initially not relevant. The comparison of the effects of multi-homing and IOP with regard to the question of which instrument is more likely to favour the market entry of an innovative newcomer cannot be clearly answered ex ante in this scenario and is not investigated in Doganoglu & Wright (2006). Chapter 3.3.1 therefore specifies the substitutive interaction of multi-homing and IOP in the context of the platform economy in more detail and focuses in particular on the dynamic competition perspective of both concepts.

#### 2.2.1.5 Homogeneity of products

An IOP of horizontally competing services makes them significantly more similar from the consumer's point of view. Digital platforms offer a core of comparable or even identical features, different networks and communication services allow communication to the identical and common user base or meet the same security and privacy requirements due to technical standards. Through horizontal IOP, products and services become more homogeneous and the possibilities for providers to differentiate themselves rivals shrink (Farrell & Saloner, 1985b). If one abstracts from other accompanying factors such as network effects, less horizontal differentiation of products in static competition implies more intense price competition.

On the one hand, more intensive competition, in monetary prices or still differentiable product dimensions, is good for consumers, but entails rent losses on the supply side. Depending on the cost structures of currently operating suppliers, an ex post IOP obligation could thus limit the pricing leeway, reduce profits and ultimately result in the market exit of individual companies. For a more detailed discussion of product differentiation options in the context of platform services, we refer to Chapter 3.3.4.

**Competitive effects of interoperability**

- IOP of services allows all users of interoperable providers to benefit from provider-specific network effects.
- **Incentives** for the subsequent introduction of **horizontal IOP vary greatly in terms of market share** and the user base already gained. Large providers may lose a competitive advantage through IOP, whereas smaller providers' services become more attractive.
- IOP can **mitigate market concentrations** or **prevent markets from tipping,** as network effects no longer occur on a provider-specific basis and a change of provider can take place without a loss of network effects.
- If **multi-homing is** possible without significant costs, the welfare **gains from IOP are limited.**
- IOP **increases the homogeneity of products** and limits the possibility of product differentiation. This implies a **stronger competitive focus in** other product dimensions, such as **prices or quality characteristics,** which are not affected by IOP regulation.

#### 2.2.1.6 Cost effects of interoperability

While the focus so far has been on possible benefits from IOP of products, this section looks at various cost dimensions associated with the introduction or maintenance of IOP. In this respect, a distinction between company-specific and welfare cost components makes sense.

##### 2.2.1.6.1 Company-specific fixed costs due to interoperability

Certain cost components are expected to be incurred only once by firms when introducing or implementing IOP obligations. Such expenses can be, for example, expenses for research and development in order to adapt existing products, negotiation costs for the design of a necessary technical standard or the costs of introducing a completely new, interoperable product.

Such one-off costs represent economically sunk costs and Katz & Shapiro (1985) find that in such a case the marginal costs of both interoperable and non-operable products and services are identical. Thus, sunk fixed costs due to IOP are not relevant for downstream strategic decisions, such as the choice of prices, quantities or product qualities, and cost-induced competitive effects are not to be expected.

Likewise, in such a scenario, the private-sector incentives to produce IOP are often lower than from a welfare perpsective. This is because high fixed costs can be a barrier for companies to make products and services interoperable. This is especially the case when potential gains from IOP are highly asymmetric and not all market participants benefit from IOP, so that fixed costs of deployment cannot be amortised. In this respect, high fixed costs due to IOP, e.g. complex technical requirements due to introduced standards, can also hamper market entry of young companies and thus weaken future competition. The danger that high costs due to IOP standards can act as a barrier to entry to platform markets is concretised in Chapter 3.3.6. There are also incentives for incumbents to degrade the quality of established IOP interfaces ex post in order to cause continuous costs for access-seeking companies to maintain the IOP. Through such sabotage incentives (see also Chapter 3.3.3), it is therefore likely that there will be ongoing costs to maintain and "service" the IOP interfaces.

#### 2.2.1.6.2 Company-specific variable costs of interoperability

In contrast to fixed costs, there are also situations where IOP costs are variable and depend on product demand or the user base. In non-digital markets these are often input costs per unit produced, but examples can also be found in the digital context. The implementation of IOP can potentially involve royalty payments under a standard, which are incurred depending on the subsequently realised demand and user base. The amount of the total costs incurred for this can thus be influenced by the companies afterwards and plays a strategic role in the choice of prices and notified sales volumes.

Katz & Shapiro (1985) point out that such variable cost components have a contractionary effect on the quantity offered due to the compatibility of services, ceteris paribus. This incentive for companies to strategically reduce quantity works against the actual motivation for introducing IOP, namely the benefit of network effects through a larger connected user base. If variable cost components are inherent to an IOP, it should be taken into account that the above contractive quantity effect mitigates possible positive effects. If variable cost components are not created by IOP, care should nevertheless be taken that they are not artificially created, e.g. in negotiations on standards in the form of volume-based licence fees. In addition to being a channel for welfare-reducing quantity reduction, these also harbour collusion risks (see Chapter 3.3.2). In the context of vertical IOP and variable costs, this contractionary quantity effect is reinforced by the marginal principle in the profit maximisation calculation of the companies on an upstream or downstream market. Classical inefficiencies along the value chain, such as double marginalisation, are thereby reinforced (Bourreau et al., 2022).

#### 2.2.1.6.3 Consumer and welfare costs of interoperability

In addition to cost components that are directly incurred by firms, IOP can also cause indirect costs that consumers bear directly or that materialise in society as a whole with a possible time lag. Chapter 2.2.1.5 has already shown that horizontal IOP leads to a homogenisation of horizontally competing products. A reduced possibility for product differentiation is synonymous with reduced product variety from the consumer's point of view. Consumers can only choose from a more limited range of products and find products that are on average a poorer match to their inherent needs and preferences. Due to the poorer match between product characteristics and preferences, reduced product variety has a detrimental effect on the benefits derived from consumption and ultimately on overall welfare (Brynjolfsson et al., 2003; Scherer, 1979). This channel between product variety and a welfare effect is particularly important when consumer preferences are particularly strong, i.e. likes or dislikes of certain product characteristics are of great importance for consumer utility (Norman & Thisse, 1996).

Particularly in the context of the platform economy or messaging services, the products offered can be assumed to be increasingly complex and have a large number of properties for which corresponding preferences prevail on the consumer side. In particular, preferences about privacy and data protection settings or the range of features of the services are significantly heterogeneous between consumers, so that a restriction of the product variety can lead to significant utility losses.

**Cost effects of interoperability**

- Company-specific **fixed costs** due to the introduction of IOP represent sunk costs and **are not competitively relevant** once paid. Nonetheless, such cost components can **make IOP adoption difficult** and act as a **barrier to entry for** small firms. There are also likely to be ongoing cost expenditures to maintain and **service** IOP interfaces.
- Volume-dependent **(variable) costs** through IOP are **relevant to competition** and have a **contractive effect on the quantity offered** or set incentives to reduce one's own user base. This is **contrary to the actual motivation of IOP**, the use of network effects through the largest possible connected user base.
- IOP leads to **less product variety** between horizontally competing products **and** implies a **poorer match between product characteristics and consumer preferences**. The resulting negative welfare effect is particularly significant when consumer preferences are strong.

### 2.2.2 Interoperability and incentives for innovation

Decisions to innovate and invest in R&D are always made in a current competitive environment and take into account future and still uncertain market situations. Mechanisms designed to promote the will of companies to innovate therefore take strategic influence on either the current or future market situation following an innovation. The assessment of innovation effects by IOP as a naturally occurring aspect as well as an exogenous instrument follows this logic. Applying the static competitive effects of 2.2.1 to a longer-term time horizon, dynamic effects can be estimated. Similar to the previous Chapter, implications for innovation in general are explained at this point. For a concrete reference, especially to innovation effects on markets of the platform economy or on messaging services, we refer to Chapters 3.2.2 and 3.3.5 and separately on messengers to Chapter 4.

When assessing innovation incentives in the context of IOP, it makes sense to distinguish between effects of IOP at the horizontal level on the one hand and at the vertical level, i.e. to upstream or downstream markets, on the other. The advantageousness of IOP and expected innovation effects differ in this respect, sometimes significantly.

#### 2.2.2.1 Innovation effects through vertical interoperability

Investments in innovative ventures are fundamentally decisions under uncertainty. This is particularly true in platform economy markets, which are characterised by a complex mix of competitive dynamics, technological progress and potential regulatory intervention. In this market context, an exogenously specified IOP of services, possibly via a standard, creates planning certainty about product features offered in the future or technically available interfaces. This security not only promotes the plannability of innovation projects at the horizontal level, but also in particular the development of new complementary vertical products and services (Baldwin et al., 2000; Farrell & Simcoe, 2012b). In particular, the guaranteed availability of technical interfaces is a critical (un)certainty factor in the development of complementary services on digital markets.

In the case of vertical IOP, which must be symmetrically maintained by all services at an upstream market stage, another positive innovation aspect arises. With a larger relevant user base of all now interoperable services, the potential market for complementary service providers increases. Without vertical IOP regulation, only individual providers may make corresponding API interfaces available, whereas a corresponding symmetrical IOP standard makes users of all providers technically accessible. The addressable market for complementary providers is thus enlarged and it becomes more attractive to develop new complementary products and services for the enlarged user base in upstream and downstream markets (Katz & Shapiro, 1985).

In extreme cases, IOP may even open up the emergence of entirely new complementary business models and enable consumers to mix and match and create their own innovative service compositions. Matutes & Regibeau (1988) show that the possibility of combining different modular services on the one hand generates benefits through increased product diversity and that companies are able to participate in this through higher prices. Private and welfare incentives for vertical IOP can thus be aligned and corresponding IOP interfaces may be market-driven.

#### 2.2.2.2 Innovation effects through horizontal interoperability

While the expected innovation effects of vertical IOP are predominantly positive, IOP at the horizontal level does, however, harbour some obstacles to innovation. First of all, while setting an IOP standard guarantees certain product characteristics and technical interfaces, standards can also fortify a certain state of technology or an implementation process. The technical implementation of such IOP specifications may be more efficient in the future rather than with today’s means. Innovations in this respect can therefore be hampered if standards are not formulated in a sufficiently flexible and future-proof manner. The danger of an overly rigid technical standard is particularly present if it is set exogenously and does not result as a de facto standard in a market-driven manner (Arthur, 1989).

Another innovation problem may be associated with the magnification of network effects through horizontal IOP and the associated competing products. While the extension of supplier-specific network effects to the entire market has the effect of preventing markets from "tipping" towards a single supplier, it also implies that the current state of technology may be manifested through a standard. Product innovations that would mean a deviation from this standard may no longer be interoperable with already existing competing products and their consumers no longer benefit from market-wide network effects. The reduced attractiveness from a consumer perspective of innovative but non-interoperable products inhibits corresponding shifts in demand, reduces potential innovation rents for suppliers and dilutes the unilateral incentives to innovate in the first place. Although innovation is desirable from a welfare perspective, it does not occur because unilateral private incentives are too low due to the loss of market-wide network effects and early innovators bear disproportionately high costs from the then lack of IOP (Farrell & Saloner, 1985a; Farrell & Saloner, 1986b). In economic literature, this phenomenon is described as "excess inertia", i.e. an inefficient persistence in the status quo. The market-driven escape from such an innovation trap is expected to be very difficult or even impossible (Arthur, 1989; David, 1985). This danger is particularly prevalent when the expected network effects are particularly strong and losses due to a lack of IOP are correspondingly high for the first mover of the innovation.

While horizontal IOP can be helpful in a static perspective to create competition within a market and to dissolve market concentrations tipped by network effects (see Chapter 3.2.1), it poses additional innovation risks from a long-term, dynamic perspective. Digital platform markets are generally dynamic and have high incentives for innovation. Competitive advantages through innovative products are quickly multiplied by existing network effects and can thus lead to substantial gains in demand (see Chapter 3.3.1 on competition for the market). These positive demand elasticities for the market-superior product of a supplier are economically efficient and secure necessary innovation rents and justify investment expenditures similar to the way patents work (Gallini, 2002; Kamien, 1992). Market intervention to establish horizontal IOP may therefore reduce the rents of innovations that have already taken place or signal the possibility of further IOP intervention in the future. The latter in particular is a potential risk factor for future innovation projects. In an environment of strong firm-specific network effects, firms could thus become victims of their own success in that natural market dynamics disproportionately reward innovative products, but these rents are also made available to competitors through ex post IOP intervention. Against this background, Geradin & Rato (2007) emphasise, among other things, the importance of fair reasonable and non-discriminatory (FRAND) royalty payments to maintain incentives for innovation when introducing possible IOP standards.

**Interoperability and innovation**

- **Vertical IOP** creates **planning security** via available technical interfaces (APIs) and **promotes innovations of complementary providers.** Likewise, mandatory vertical IOP standards ensure the **accessibility of the entire user base of** a market and thus increase the **demand potential in upstream and downstream markets**.
- **Horizontal IOP poses innovation risks by** cementing the current state of technical innovation. **Further technical developments** are either not **possible** due to compliance with a standard that is not future-proof or are **foregone** because **market-wide network effects** for an **innovative but non-interoperable product do not** initially **arise** ("excess inertia"). In addition, possible IOP obligations at the horizontal level can **weaken** emerging **competitive advantages and** thus **reduce important innovation rents**.

### 2.2.3 Interoperability and consumer protection

In the digital society, IOP and compatibility of goods and services also play an increasingly important role from the perspective of consumer protection. German and European consumer law takes this into account through a number of recent regulations. As an example, the pre-contractual duty to inform from Section 312d para. 1 BGB (German Civil Code - Bürgerliches Gesetzbuch) in conjunction with Art. 246a Section 1 para. 1 sentence 1 no. 18 EGBGB (Introductory Act to the Civil Code – Einführungsgesetz zum BGB) can be mentioned as an example.[4] According to this provision, in the case of contracts concluded away from business premises and distance contracts, traders are obliged to provide the consumer with information on the compatibility and IOP of goods with digital elements (Section 327a (3) sentence 1 BGB) or digital products (Section 327 (1) sentence 1 BGB) before the conclusion of the contract.[5] According to the explanatory memorandum, the term IOP refers, for example, to hardware and software with which digital content can be used (BT-Drs. 17/12637, 74). However, the wording of the law limits the scope of the duty to inform in two ways. On the one hand, the information on compatibility and IOP is only required insofar as it is "essential". Secondly, the duty to inform only exists "[insofar as this information is known or must be known by the trader]" (“*soweit diese Informationen dem Unternehmer bekannt sind oder bekannt sein müssen*“). The trader therefore only has to inform about the IOP and compatibility with reasonably marketable and up-to-date hardware and software; a reference to the lack of usability with completely outdated and hardly used systems is not required (BT-Drs. 17/12637, 74).

The Act Implementing the Directive on Certain Aspects of the Law of Contracts Concerning the Provision of Digital Content and Digital Services of 25.6.2021 (BGBl. 2021 I 2123) anchored the terms "compatibility" and "interoperability" in an even more prominent place in German consumer contract law. According to Section 327e para. 2 p. 1 no. 1 lit. a) BGB n.F., a digital product complies with the subjective requirements of product quality if it has "[the agreed quality, including the requirements as to its quantity, its functionality, its compatibility and its interoperability]" (“*die vereinbarte Beschaffenheit hat, einschließlich der Anforderungen an seine Menge, seine Funktionalität, seine Kompatibilität und seine Interoperabilität*“).[6] According to the legal definition in Section 327e (2) p. 3 BGB n.F. and the underlying definition in Art. 2 No. 11 Digital Content Directive (EU) 2019/770, the term compatibility means "the ability of the digital content or digital service to function with hardware or software with which digital content or digital services of the same type

[4] In its original form, the provision goes back to Art. 5(1)(h) of the Consumer Rights Directive 2011/83/EU (cf. also recital 19 of the Consumer Rights Directive: "The notion of relevant interoperability is meant to describe the information regarding the standard hardware and software environment with which the digital content is compatible, for instance the operating system, the necessary version and certain hardware feature"). The current version of the provision, which is applicable from 28.5.2022, goes back to Art. 4(3)(b) of the Modernisation Directive (EU) 2019/2161.

[5] In the case of other consumer contracts, a corresponding duty to inform arises from Section 312a (2) BGB in conjunction with Art. 246 (1) No. 8 EGBGB. Art. 246 para. 1 no. 8 EGBGB.

[6] A corresponding provision for contracts of sale was inserted by the Act on the Regulation of the Sale of Goods with Digital Elements and Other Aspects of the Contract of Sale of 25.6.2021 (BGBl. 2021 I 2133) in section 434 para. 2 sentence 2 BGB n.F..

are normally used, without the need to convert the digital content or digital service". IOP, on the other hand, is defined in Section 327e (2) sentence 4 BGB n.F. following Art. 2 No. 12 Digital Content Directive (EU) 2019/770 as "the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used". These definitions differ from the common technical definitions used in computer science, for example (Metzger, in: MüKoBGB, 9th ed. 2022, BGB Section 327e marginal no. 14).

According to Section 327e (3) BGB, compatibility with customary hardware and software is also one of the objective requirements for the quality of digital products, which must be present regardless of a corresponding party agreement in order for a digital product to be free of product defects. According to Section 327e (3) sentence 1 no. 2 BGB, a digital product meets the objective requirements for product quality if "[it has a quality, including [...] compatibility [...], which is customary for digital products of the same kind and which the consumer can expect, taking into account the nature of the digital product]" (“*es eine Beschaffenheit, einschließlich […] der Kompatibilität […] aufweist, die bei digitalen Produkten derselben Art üblich ist und die der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann*“). Unlike compatibility, however, IOP is only provided for as a subjective requirement and not also as an objective requirement within the meaning of section 327e(3). This is based on the consideration that the trader who provides the digital products cannot make provisions for the unmanageable variety of not regularly used combinations of the digital products with hardware and software (Schulze, in: HK-BGB, 11th ed. 2021, BGB Section 327e marginal no. 14).

The provisions mentioned here are also relevant for contracts on access to digital platforms (e.g. social media platforms) and messaging services. Accordingly, the objective requirements for messaging services to be observed under section 327e (3) sentence 1 no. 2 BGB include compatibility with the usual hardware and software environment. The extent of compatibility (e.g. the usability with different versions of an operating system) depends on which quality is "[usual for digital products of the same kind and [...] which the consumer can expect, taking into account the nature of the digital product]" (“*bei digitalen Produkten derselben Art üblich ist und […] die der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann*“) (section 327e (3) sentence 1 no. 2 BGB). An IOP with other messaging services, on the other hand, cannot generally be expected from the perspective of consumer contract law, as the IOP is not one of the objective quality requirements of digital products according to Section 327e para. 3 BGB.

# 3 Interoperability in the Platform Economy

## 3.1 Characteristic features of digital platform services & status quo of interoperability

Belleflamme & Peitz (2021) sum up that positive network effects lead to a spiral of attraction when building a platform. In the case of platforms, indirect network effects are mostly decisive, which act via two or more market sides. Thus, platforms go beyond pure networks, which results in the need for a more detailed consideration of the exact interactions of the groups, beyond the in-group externalities. Messaging services, which serve only one user group in their core function and whose exact characteristics are explained in more detail in Chapter 4.1, become more attractive via direct network effects, i.e. the more acquaintances and contacts already use this service, the more attractive the service becomes. Although pure messengers are not to be regarded as a multi-sided platform in the sense of the interpretation in Chapter 2.1.1.2, they do provide a direct explanation of how direct network effects work.[7] The number of users exerts a group-inherent ("within-group") positive direct network effect on further potential users. The same mode of action of a within-group network effect applies to social networks such as Facebook or Instagram, neglecting advertising partners between the users of the network. The more users are active in a social network, the more attractive the interaction is for other (potential) users.

In this context, asymmetric pricing structures and cross-subsidisation between different market sides by platform operators can occur in equilibrium. Wright (2004) points to nightclubs as an example of cross-subsidisation of matching platforms, where women and men are the groups with the cross-group mutual positive appreciation (Wright, 2004). Digital counterparts to this are online dating portals or other matching platforms such as AirBnB.

It should be noted, however, that network effects could also scale negatively. Assuming that a social network already suffers from a strong loss of members, it also loses attractiveness for remaining participants (users and possibly other market sides). However, users are often subject to a coordination problem, which makes a "critical outflow" more difficult.

In the case of messaging services, direct network effects lead to a spiral of attraction that can lead to concentration tendencies in the market. In this context, there are well-founded theoretical studies on the phases of strong growth and the achievement of a critical mass (Evans, 2009; Evans & Schmalensee, 2010). However, these concentration tendencies

[7] In the literature, definitions can also be found that attest to a platform property on the basis of the coordination of network effects and thus independently of multiple participating market sides (Belleflamme & Peitz, 2021). Sanchez-Cartas & León (2021) provide a comprehensive overview of the range of different approaches to defining platforms that have always existed.

must be viewed in a more differentiated way in the context of asymmetric network effects across groups, such as in the case of advertising-financed platforms. Here, although users positively influence advertisers, users do not necessarily perceive more advertisers as an enrichment (Armstrong, 2006). In the above example of a social network such as Facebook, users exert a positive externality on other users (positive "within-group" effect) and advertisers (positive "cross-group" effect). The advertisers, on the other hand, are likely to have no externality on the users at best, tending to have a negative externality (negative "cross-group" effect). This constellation of network effects leads, according to Belleflamme & Peitz (2021), to an attraction-repulsion pendulum.

Another relevant point arising from network effects is data-driven learning effects. Prüfer and Schottmüller show that data-driven learning effects lead to greater market concentration and thus also have an impact on the willingness to innovate (Prüfer & Schottmüller, 2021). Depending on whether the learning from the data is "within-user" (user-specific) or "across-user" (user-wide), data network effects may not occur (Hagiu & Wright, 2020a). In the case of user-specific learning effects, however, the individual switching costs and thus the lock-in of the individual user increases, since the corresponding provider can offer the most comprehensive personalisation. This could be countered with data portability or a data IOP. Across-user learning refers to a company being able to improve its product for each customer based on learning from data from all customers. This can lead to effects comparable to conventional network effects in certain scenarios - for example, when combined with continuous product improvements (Hagiu & Wright, 2020b). Across-user learning is present in a variety of prediction and recommendation mechanisms, as e.g. the quality of traffic predictions increases the more users use a traffic service.

Digital platform markets therefore tend to "tip" in favour of one company or service at a "tipping" point due to positive network effects, which means that the network effects and the advantage of collected data can make the contestability of a market difficult in the sense of natural monopolies.[8] Reasons for these "tipping points" can be high switching costs, which in turn lead to lock-in effects. For example, in the context of social networks, the contacts established represent a "network lock-in", which in turn increases the switching costs to other services. In addition to and outside of social networks, personal lock-in effects resulting from the personalisation of a service are a priority.[9] Until the market- and segment-specific "tipping point" is reached, however, there is a so-called "chicken-and-egg problem". This consists of the lack of initial network effects during the development of a platform, which in turn has a negative impact on attractiveness. Among other things, subsidies for the more price-sensitive side of the market, exclusivity agreements[10] but

[8] Cf. Baumol et al. (1983) on the contestability of natural monopolies. It should be noted here that classic natural monopolies are not contestable due to the cost structure, while in digital platform markets it is primarily the demand side and its positive group-inherent externality that leads to the lack of contestability (Jullien & Sand-Zantman, 2021). In turn, Belleflamme & Peitz (2021) see the possibility of multi-homing as a reduction of market entry costs as a clear distinction from natural monopolies. With regard to the "tipping" of digital markets, see, for example. OECD (2018), Jacobides & Lianos (2021a).

[9] Personalised algorithms for user-specific suggestions, playlists, watched items or similar.

[10] See Lee (2013) on the effect of exclusivity agreements in the US video game industry.

also a more open platform governance in the beginning can serve to overcome this initial stage. The background here is the development of an "ecosystem", which is formed in the course of an "envelopment" of markets affected by the network effects (Eisenmann et al., 2011). The resulting bundling of additional modular features expands the ecosystem and its own platform (Tiwana et al., 2010). If large user bases can be “locked” in digital ecosystems ("walled-gardens"), this is a "competitive bottleneck" in the sense of Armstrong (2006). The function of digital platforms as gatekeepers is also derived from this concept, as they can have exclusive access to large user groups in the absence of remedial measures.

Due to the above differences in terms of growth on platform markets, there are also corresponding specifics for the strategic use of the openness of a platform. According to the Autorité de la Concurrence & CMA (2014) open systems are defined by the provision of interfaces that also enable third parties to provide complements. In contrast, in closed systems compatibility is limited to selected complements. Eisenmann et al. (2009) define openness in the context of a software platform, at most with "reasonable" restrictions on contribution, development, use and commercialisation that affect all parties comparably. Benlian et al. (2015) formulate the strategic decision to vertically open platforms as a trade-off between diversity and control.

However, there are also strategic restrictions, e.g. eBooks and apps from the Apple ecosystem cannot usually be used on Android devices. The reasons for this are, on the one hand, targeted strategies by platform companies to prevent churn through technical and contractual design of their own services and content, but also an increased possibility of enforcement of such practices based on copyright law (Doctorow, 2022). For example, the use of reverse engineering, scraping bots or bridges is often rigorously prevented by lawsuits.

### 3.1.1 Status quo: Existing types of interoperability

The problem of concentration tendencies and the balancing act of an efficient design of frameworks is the subject of academic and political discussions. For this reason, platforms and their function as gatekeepers are increasingly being taken into account in the design of competition and regulatory law. For example, the legal basis for imposing IOP obligations on NI-ICS was created in the amended TKG (which came into force at the beginning of Dec. 2021). The 10th GWB amendment (Act against Restraints of Competition – Gesetz gegen Wettbewerbsbeschränkungen) takes into account the role of gatekeepers as well as the adopted DMA law of the European Commission. A brief overview of implemented and planned legal provisions can be found in Chapter 3.1.2. As switching costs are of great relevance for competition in digital markets, a reduction of these costs is an essential part of the remedies. From a technical point of view, low switching costs can be made possible more often by coordinating the parties involved. Compared to classic analogue and physical markets, various forms of portability, compatibility and, building on this, IOP are comparatively less frictional to realise in the context of the digital sector due to subsequent product adjustments through software and firmware adaptations. Traditional telecommunications services became interoperable via standardisation, but were slower to adapt to new consumer demands than new web-based communications services.

The status quo of existing types of IOP and strategic limitations are explained below.

#### 3.1.1.1 Meta/Facebook's handling of access via API

The division into horizontal and vertical modes of impact of IOP is also found in the current status of compatible and interoperable features. Meta, for example, offers the possibility of cross-posting across platforms for the Instagram service, although this possibility is in the options and thus not obvious (Scott Morton et al., 2021). This cross-posting is not limited to other companies of the Meta group, but also includes social services in the Russian-speaking region (VKontakte, OK.ru) and Twitter as well as Tumblr. Instagram thus strategically uses the openness of other social services via their APIs to publicise its own content, which, depending on the explicit design and use of the APIs, corresponds to asymmetric or even vertical IOP. At the same time, Meta is making efforts to further connect its own platforms with each other and thus to establish IOP between them, even if only internally within the group (cf. Yurieff, 2020). The Instagram Messenger, which was expanded at the end of 2020, is interoperable with Facebook Messenger, whereas neither currently offers an IOP with WhatsApp (Meta, 2020). Detailed explanations of the background can be found in Chapter 4.

However, Scott Morton et al. (2021) also explain opposing and thus more restrictive corporate practices using the example of Vine, a now-defunct short video service that initially offered users the ability to send videos to their "Facebook friends" using the "find friends" API. After Vine was acquired by Twitter, Facebook apparently felt that linking such an essential feature to a competing social network was a threat and unilaterally changed the API. Thus, Vine lost an attractive feature and Facebook thwarted a presumed driving reason for Twitter's acquisition. Ultimately, Vine could not hold its own in the market and was discontinued. On the other hand, the social network Facebook offers and offered many possibilities of features of its own ecosystem (for example Facebook login, Like button, "Share on Facebook") for vertical use (in the case of Facebook login) or expansion of its own platform content ("Share on Facebook"). The latter motive also seemed to be part of the original content handling of the short video service Vine until a "sharper" competitor, Twitter, took it over. The fact that Facebook has increasingly left the strong growth phase is also likely to play a role in this context. From a competitive point of view, it is interesting from this difference made on the part of the meta group that on the one hand the competitive situation between the social networks has an impact on the strategic use of openness and that asymmetrical cross-postings follow a strategic control of the flow of attention.

#### 3.1.1.2 Amazon Selling Partner API

The Amazon Selling Partner API (SP-API) can be considered as an example of vertical IOP. Among other things, this provides vertical sellers of products on the Amazon Marketplace with the option of listing their products, updating prices, contacting buyers or viewing or updating the shipping status. The exact features and structure of the API are extensively documented by Amazon (Amazon, 2022). The provision of a framework for third-party providers on its own platform is part of Amazon's change in strategy from retailer to provider of a sales platform. Amazon continues to compete as a retailer with the sellers on the Marketplace, but at the same time it offers a downstream service with shipping for Marketplace sellers.

#### 3.1.1.3 PSD2 and Open Banking

The European Commission's second Payment Services Directive (PSD2) is a regulatory framework for payment and banking services and should simplify and speed up money transfers between banks. Furthermore, payment service providers are required to provide access to individual features (e.g. account balance enquiries, identification). The Commission expected this to increase the efficiency of the European market for payment services and innovative services, which should build on these now available features (European Commission, 2015). Explicit consent is required to preserve the sovereignty of the customer. At the same time, the Open Banking Working Group was founded in the United Kingdom and tasked with establishing the framework of an open API standard. This standard should enable additional features in the sense of PSD2, but also a common technical framework for the creation of an ecosystem of services in the financial sector. On the basis of this standard, individual services in the banking and financing sector are to be disaggregated and offered on a modular basis. One possible consequence of this, apart from the reduction of lock-in effects and switching costs, would be a platform on which customers could freely choose from the offers of multiple providers (Open Banking, 2022a). For the second quarter of 2021, Open Banking reports 319 third-party providers as participants in the Open Banking ecosystem with over 800 million API calls per month (Open Banking, 2022b).

#### 3.1.1.4 Apple NFC interface

Since the 6th generation iPhones of 2014, the devices have incorporated an NFC chip, an open standard for the wireless transmission of small amounts of data at close range. The functionality of the NFC chip was reserved for Apple's own payment service Apple Pay, although the specification of the standard itself is publicly available and an implementation would also have been possible for third parties. ACM (2019) reports "dismay" on the part of app developers about the restrictions on use. At the time of the ACM report (2019), even the Dutch government was unable to gain access to the interface for an e-identification service, while this was possible for Android devices. Furthermore, ACM

(2019) reports of similar restrictions for a UK government app, which, according to a quoted BBC report, took place for security and commercial considerations (Wheeler, 2018). ACM (2019) refers to the fact that the NFC interface on Android was possible for third parties as early as 2010, but there were also comments about security concerns in the course of this. It is also reported that one payment service told ACM that it had to stop its payment service due to the lack of access to the interface. The European Commission has been investigating competitive restraints by Apple in the mobile payment services market since June 2020. In a statement on the preliminary findings, Vestager explained the suspicion that Apple had abused its market power in the iOS ecosystem to hinder competition between payment services. Furthermore, Vestager points to the fact of lack of innovation due to the restrictive access to interfaces for third parties (Europäische Kommission, 2022b). With the update to the operating version iOS 14 (2021), Apple made the use of the NFC chip possible, but restricted it to features approved and limited by Apple.[11]

#### 3.1.1.5 Voice Interoperability Initiative

In September 2019, Amazon announced that it is working on an interoperable solution for digital voice assistants in collaboration with other well-known companies such as Baidu, Microsoft and Spotify. This will focus on developing a framework to integrate multiple voice assistants using different activation words on individual devices. Lyles (2020) notes, however, that one year later, competitors Apple, Google and Samsung are missing from the 70 companies recruited for the initiative. Thus, the success of this initiative is questionable, as the relevant market players with large customer bases are not participating. Roettgers (2021) reports about the speaker manufacturer Sonos, which accuses Google of contractually preventing the above-mentioned form of mix-and-match. At the same time, Lyles points out that it is precisely these large US companies that cooperate within the framework of the IoT IOP, which is why this topic will also be briefly discussed below.

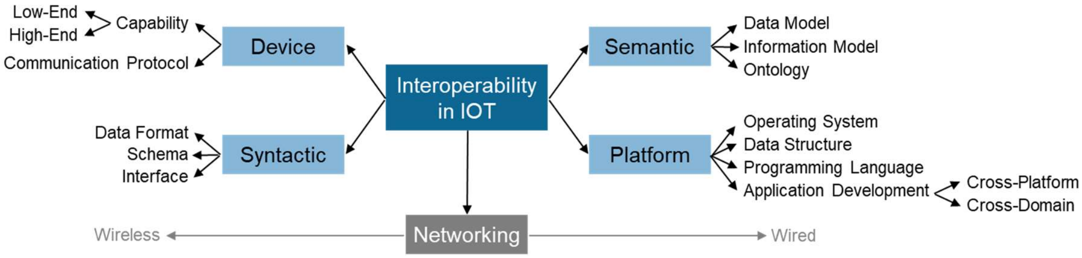
#### 3.1.1.6 Internet of Things - Interoperability initiatives

The Internet of Things (IoT) can be seen as a cosmos of smart devices with "smart" properties that set them apart from their conventional counterparts. The basis of these smart features is communication with servers and other interoperable devices. McKinsey states in a study on the economic potential of IoT implementations that 40 % of the benefits of an IoT implementation remained unused due to a lack of IOP (Manyika et al., 2015). Here, the restriction to certain devices or software of individual manufacturers is an obstacle to the utilisation of the potentials, since basic properties of the IOP are not possible beyond the platforms and converters have to be used. In the smart home sector, the use of physical devices means that there is already a lack of compatibility at the device level; for

[11] For example, App-Clips (Apple, 2021) or CarKey (Apple, 2022).

example, Bluetooth and ZigBee, two incompatible radio technologies, are used, which makes interchangeability in the sense of the above working definition impossible without converters. But different protocols such as CoAP and MQTT are also used, both of which were developed specifically for simple communication between machines (M2M). Figure 3-1 shows the multi-layered aspects that complicate an IOP in the context of IoT devices and at the same time shows that here, too, great importance is attached to the significance of platforms. With Apple Homekit, Google Brillo, Amazon AWS IoT and IBM Watson, Noura et al. name five IoT platforms whose IOP is made more difficult by the use of different programming languages or software development kits (SDKs). A manufacturer of an IoT product would have to learn the specific features of the programming interfaces accordingly. For this reason, there are efforts in the IoT industry and research that deal with adapter solutions but also interoperable standards. However, this is hampered by a lack of comprehensive documentation or a common standard, which both restricts an IOP and inhibits the development and dissemination of IoT (Noura et al., 2019).

Figure 3-1: Taxonomy of the IoT ecosystem



Source: Noura et al. (2019), p. 799.

In May 2021, the Connectivity Standards Alliance (formerly ZigBee Alliance) announced the development of an open, global standard (Matter, formerly Project Connected Home over IP, CHIP*)* for IOP between smart home devices and IoT platforms (BusinessWire, 2021). Among others, Amazon, Apple, Google and Huawei are listed as supporters of the alliance on the website (CSA, 2022).

### 3.1.1.7 Covid19 tracing

One example of collaborative IOP was the provision of the Covid19 tracing framework for iOS and Android, the mobile operating systems of Apple and Alphabet. They developed an interoperable API that allowed users to use opt-in certified apps to get a proxy for the duration of contact and spatial proximity to diseased individuals. To do this, they used the Bluetooth Low Energy wireless standard to send an anonymised ID to the surrounding devices, while also recording the IDs of the people and storing them for 14 days (Panzarino, 2020). After a positive test, the person was able to send his or her own ID to the app's database, which made it possible to match it with other users. The German Corona-Warn app was also programmed based on this API (Reelfs et al., 2020). However, so that this functionality was not limited to the devices within their own operating system, Apple and Google developed an interoperable API including data structure, syntax and semantics. At the same time, they published extensive documentation on how the API is accessed, how the exchanged data is structured and what reference structure the database of the app based on this function should have (Apple, 2020; Google, 2020).

### 3.1.2 Current legislative developments & demands for an interoperability obligation

#### 3.1.2.1 Implemented legal requirements

The amended German Telecommunications Act (Telekommunikationsgesetz, TKG) entered into force on 01.12.2021 and, in addition to extending the scope of the telecommunications regulations for interpersonal communications services, also introduced applicable regulations on IOP. In implementation of Art. 61 para. 2 subpara. 2 lit. c of Directive (EU) 2018/1972, the newly inserted Section 21 para. 2 TKG provides for the possibility that the Federal Network Agency as competent authority can oblige providers of NI-ICS to IOP under narrow conditions. An obligation to IOP can only be ordered for NI-ICS which have a "significant coverage and a significant user base" (Section 21 para. 2 no. 1 TKG). According to Recital 151 RL (EU) 2018/1972, this requires that the geographical coverage and the number of end-users reach a critical mass with regard to achieving the objective of end-to-end connectivity. It is also required that end-to-end connectivity between end-users is threatened due to the lack of IOP between NI-ICS (Section 21 para. 2 no. 2 TKG) and that the ordering of IOP is necessary to establish end-to-end connectivity (Section 21 para. 2 no. 3 TKG). In procedural terms, it is also necessary for the European Commission to adopt implementing measures pursuant to Art. 61 para. 2 subpara. 2 ii Directive (EU) 2018/1972. This in turn requires that the Commission, after prior consultation with BEREC, determines that end-to-end connectivity between end-users is threatened to a significant extent in at least three Member States. The European legislator has thus set very high hurdles for an order of IOP for providers of NI-ICS (BT-Drs. 19/26108, 258; Stamm, 2022). The restrictive regulations of Section 21 para. 2 TKG are thus in tension with the new IOP obligations from the DMA.

Section 19a of the GWB also contains legal requirements regarding the guarantee of IOP. The new provision introduced as part of the 10th GWB amendment, which entered into force on 19 January 2021, enables the Bundeskartellamt to determine by order the paramount market position of a company for competition across markets and to prohibit the company in question from certain anti-competitive conduct. In particular, the Bundeskartellamt can use the extended powers to prohibit the preferential treatment of own offers (self-preferencing), the transfer of market power to previously non-dominated markets, as well as measures to restrict IOP and portability of data (Section 19a (2) no. 5 GWB).

#### 3.1.2.2 Policy reports and planned legal implementations

In the wake of the relevance of possible IOP regulations, several policy reports have appeared: Crémer et al., 2019; Furman, 2019; Scott-Morton et al., 2019, 2021; Cabral et al., 2021; and Bourreau et al., 2022. In addition to the current academic debate, these policy reports are also related to the legal regulations now adopted in the European Commission's DMA. Among other things, this provides for mandatory rules on the provision of IOP for NI-ICS, but also contains rules for other areas that tighten the currently applicable legal basis for the possible use of obligations in such a way that vertical IOP is also addressed.

Thus, Article 6(4) requires that gatekeepers - in relation to their core platform services - "*shall allow and technically enable the installation and effective use of third- party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper*", while Article 6(7) states that gatekeepers "*shall allow business users and alternative providers of services provided together with, or in support of, core platform services, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features, regardless of whether those features are part of the operating system, as are available to, or used by, that gatekeeper when providing such services*".

Parliament proposed to extend the obligation in Article 6(7) to "*allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant”,* provided that the operating system/virtual assistant is identified in accordance with Article 3(9) as being available for the services or hardware provided by the gatekeeper. The European Parliament also supported an IOP obligation for NI-ICS, which found its way into the passed law and is being further discussed in Chapter 4.

With regard to portability, the now adopted proposal (cf. Article 6(9)) provides that gatekeeper platforms "*effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data*". The Parliament successfully proposed a further extension requiring data portability to be provided free of charge.

Similar legislative projects can be observed in the UK, where the CMA, as competition authority, is seeking expanded regulations for platforms. In this context, regulations on data portability, IOP and FRAND access are also mentioned (Batchelor et al., 2021; Belleflamme & Peitz, 2021). The ACCESS Act ("Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021"), which was introduced in the US House of Representatives on 11 June 2021, also aims to achieve more competition, lower barriers to entry and reduced switching costs. This is planned, among other things, through legal provisions on portability and IOP, which puts it in line with the comparable legal plans of the European Commission and the British government.

## 3.2 Potential desirable effects of interoperability

After Chapter 2.2 has set out the expected competitive effects of various IOP concepts in general, the following section examines their applicability to markets in the platform economy. The analysis systematically distinguishes between horizontal and vertical IOP schemes and presents concrete case studies in which IOP activities have already taken place or appear promising.

### 3.2.1 Horizontal: Reduction of market concentration and lock-in effects

Horizontal IOP in digital platform markets is primarily intended to enable interaction between users of different platforms without the need to switch providers or use multiple user accounts (multi-homing). In this respect, for example, users of one social network could view profile pages of users of a competing network, establish friendship links and place content in each other's newsfeed.[12] IOP of such core features resolves firm-specific network effects and aggregates them into market-wide effects (Scott Morton et al., 2021). Existing network effects under IOP are no longer firm-specific but act as a public good and accrue equally to all market participants. The danger of tipping markets towards only one dominant platform can thus be excluded, as core features that trigger network effects are now available to all market participants to the same extent.

Competition under horizontal IOP then no longer takes place around the platform market but within the market and between platforms (Bourreau et al., 2022). This can prevent a number of inefficiencies and create static welfare benefits such as lower prices or improved quality (Crémer et al., 2019; Furman, 2019). As competition is no longer possible in the interoperable core features, it is to be expected that differentiation will increasingly be driven in other product dimensions. Possible examples in the context of social networks are, for example, different business models (use against payment vs. use against data/attention), content moderation policies (stronger filtering of hate speech) or extended

[12] In general, the technical implementation of such cross-posting can be ensured because it is already market-driven between individual networks. For example, Instagram (meta) content can also be posted on other apps, including those outside the meta ecosystem (Facebook, Twitter, Tumblr, Ameba, VKontakte, OK.ru).

privacy and data protection settings that go beyond the defined standard of the core features. Neutralising provider-specific network effects means that the choice of platform can be made irrespective of the size of its respective user base and is instead based on the inherent preferences of users.

Thus, in the case of a potential provider switch away from the dominant platform, users no longer face switching costs due to the reduction of the network size relevant to them (Farrell & Klemperer, 2007). A lock-in situation of consumers and a strong market concentration can thus be mitigated by horizontal IOP of core features. With regard to non-core features, however, there are still partly company-specific network effects (cf. Bourreau et al., 2022). Historically, however, dominant market players have already emerged in digital platform markets (Facebook, Apple and Android App Store, Google Ads, Amazon Marketplace). Even if IOP reduces switching costs, an inefficient persistence in the status quo (status quo bias) is to be expected (Samuelson & Zeckhauser, 1988). Polites & Karahanna (2012) show that this is particularly the case when switching from one incumbent system or platform to a new one. A switch therefore only takes place if an alternative platform is significantly cheaper or better matches the corresponding product preferences. Against this background in particular, it seems important that IOP only concerns core features from which network effects emanate and thus at the same time preserves sufficient scope for product differentiation.

An important prerequisite for the effectiveness of horizontal IOP is that content must be treated without discrimination on all interoperable platforms. Scott Morton et al. (2021) refer to this aspect as "equitable" IOP, in the sense that a platform must not treat content from competing platforms differently from its own. In the context of social networks, the methodology used for moderating content, the prominence of content placement or the type of content monetisation must therefore be identical to that of the platform's own content. If the mutual embedding of content between interoperable services does not take place in a non-discriminatory manner, there is a risk that provider-specific demand externalities (network effects) will be built up again. This is comparable to historical on-net and off-net tariffs between telecommunications providers. Here the networks are interoperable (every user can be reached from every network), but there are different costs. Laffont et al. (1998) argue that this artificially creates provider-specific network effects and increases market concentration to one provider. Non-discrimination in the implementation of horizontal IOP is therefore essential to maintain the pro-competitive effect of the measure. Non-discrimination in the context of vertical IOP, on the other hand, is closely linked to the dangers of foreclosure and self-referencing and will be discussed separately in Chapter 3.3.3.

**Scenario: Horizontal interoperability obligation for Facebook**

The goal of mandatory horizontal interoperability (IOP) for Facebook, or for social networks in general, is to resolve platform-specific network effects and aggregate them at the market level.
and aggregate them at the market level. The following implementation proposals to achieve this goal are largely based on the work of Scott Morton & Kades (2021) and Scott Morton et al. (2021).

Core social networking features enabled between all interoperable platforms include linking to friends, browsing profile pages and creating and viewing content (posts). The presentation of content from other networks should be stylistically (font and size) identical and non-discriminatory to own content, but marked as non-platform content. This enables users to draw conclusions about the actual user base of the interoperable networks.

In order to create the technical conditions for such an API, standards for the transmission of the individual data formats of the core features must be defined. In the context of social networks, this includes full protocol IOP of data formats to image, video, text and calendar content.

The authorisation for data exchange to take place between two platforms is to be user-specific. As soon as a "friend request" has been mutually confirmed, content created by both persons is mutually transmitted between the networks. There is no holistic exchange of content from the entire user base. Furthermore, the design of the APIs is only intended to ensure the transmission of content. Conclusions about the usage behaviour of users on other networks, as well as insights into algorithms and other proprietary processes of competing networks must be excluded in order to preserve competitive interests.

The transmission standards should be set by an SSO (Standard Setting Organisation) with technical expertise. It seems sensible to prioritise neutral experts and the interests of smaller networks in this process in order to prevent Facebook from exerting too much influence. Likewise, ex post changes to APIs should have to be approved by regulatory authorities before they come into force in order to prevent negative competition effects. Against this background, a self-regulatory solution and

APIs under Facebook's control seems negligent, as there are strong incentives for a continuous deterioration in the quality of the API. These can be operationalised, for example, through a high adaptation frequency, poor documentation or frequent downtimes on the part of Facebook.

### 3.2.2 Vertical: Stimulating innovation

Vertical IOP enables a modular combination possibility of a platform or a system with complementary services of the most diverse value creation levels (so-called "mix and match") and thus enlarges possible sales markets of upstream and downstream providers (Matutes & Regibeau, 1988). This significantly increases the innovation incentives of complementary providers, and new business models are partly made possible by vertical IOP (Farrell & Simcoe, 2012b). A reliable IOP regulation with an obligation character also creates additional security that critical interfaces will also be available in the future (Scott Morton et al., 2021). A subsequent shutdown or deterioration in the quality of important innovation interfaces can thus be prevented.

An example of the innovation-promoting effect of open interfaces to vertical IOP can be found in the market-driven provision of APIs to the IBM mainframe in the 1990s. As a result, a variety of complementary software was developed, sometimes collaboratively (Porell, 2020). Another positive example is the recently introduced open banking standard or API, which allows a number of fintech providers to access bank accounts of UK users and thus offer complementary services (Open Banking, 2022a).

In order to maintain the positive innovation effects, regulatory control of the defined APIs is advisable, as a market-driven or self-regulatory provision of such APIs is not always incentive-compatible from the perspective of a dominant platform. Vertical IOP and emerging complementary services promote the value and attractiveness of the platform or system, but it is only possible for the platform operator to extract these rents for itself to a limited extent. As a consequence, it is often observed that platforms are vertically interoperable at the beginning, but try to reduce this as their market position becomes more established (Eisenmann et al., 2009). This is operationalised, for example, through the restriction of corresponding APIs, the acquisition of complementary providers or the development of their own similar products (so-called "sherlocking").

In addition to the necessary supervision, it must also be clarified how far-reaching vertical IOP should be designed. A release of all existing private APIs is certainly the gold standard from the point of view of promoting innovation, but is questionable from a practical and legal point of view. The provision of own APIs for a specific, complementary innovation or development project is certainly easier to operationalise in this respect. Basically, the relationship between the openness of a system and complementary innovations is not linear (Boudreau, 2010; Boudreau, 2012). An IOP standard that is too open or too easy to implement could therefore encourage a flood of low-quality complementary services. Such excess tends to reduce the attractiveness of the platform from the consumer's point of view and creates too much competitive pressure from the point of view of complementary providers with high quality services (Bourreau et al., 2022). A healthy balance of vertical IOP to promote innovation and complementary competition is advisable in this context (Aghion et al., 2005).

It should also be taken into account that under vertical IOP, innovation incentives are strongly asymmetrically distributed along the value chain. Granting access to a platform free of charge in the sense of an "essential facility" naturally reduces, ceteris paribus, the incentives to provide and invest in it (Krämer & Schnurr, 2014). In contrast, innovations are promoted or made possible by upstream and downstream complementary providers. These opposing incentives of different stakeholders need to be taken into account in the implementation process of vertical IOP schemes (Bourreau et al., 2022).

**Desirable effects of interoperability**

- **Horizontal IOP** enables the **dissolution of company-specific network effects**, so that interactions between users of different platforms can take place without switching providers or using multiple user accounts (multi-homing)
- Existing network effects then act like a public good and accrue equally to all market participants, **reducing** the **risk of tipping markets** towards one dominant platform and competition no longer takes place *for* the market but *within* the market between platforms.
- **Vertical IOP** enables a **modular combination possibility of** a platform or a system with complementary services of different value creation levels (so-called "mix and match") and thus **enlarges** possible **sales markets** of upstream and downstream providers

## 3.3 Potential undesirable effects of interoperability

In addition to some advantages, the implementation of IOP regulations also entails risks that are both fundamental and procedural. In the following, we will focus on these disadvantageous effects, which are differentiated analogously to Chapter 3.2 with regard to vertical and horizontal IOP.

### 3.3.1 Horizontal: Substitution of multi-homing and reduction of competition for the market

In Chapter 2.2.1.4 the imperfect substitutive character between multi-homing and vertical IOP regulation was already addressed, which is specified here in relation to competitive effects on digital platform markets. Through multi-homing it is also possible for demanders to use firm-specific network effects of different providers simultaneously and to fully exploit service-specific features. Multi-homing thus promotes competition within the platform market and thus prevents the "tipping" towards one dominant platform, similar to the effect of horizontal IOP.

Whether IOP obligations or multi-homing are more likely to promote competition and prevent markets from tipping or to promote the contestability of digital markets is unclear ex ante. Both multi-homing and IOP each have specific advantages and disadvantages. One disadvantage of multi-homing is that it entails additional costs compared to IOP. These can be considerable, e.g. if additional expensive hardware (e.g. another smartphone in the case of multi-homing between operating systems) has to be purchased. On the other hand, especially in the case of digital services, the direct costs of multi-homing can also be very low (e.g. installing another application on the existing smartphone) and primarily non-monetary (e.g. registration, learning and other transaction costs). This is supported by a result of the representative user survey of the Bundesnetzagentur (2020) in which 73% of users of messaging services state that they use several services in parallel. A horizontal IOP regime would significantly weaken the incentive to do so and de facto exclude a number of benefits from multi-homing (cf. Bourreau et al., 2022). If substantial costs of multi-homing can be avoided, this may well be welfare-enhancing. However, the trade-off is often unclear as Kroon & Arnold (2018) show. Furthermore, they highlight the additional consumer benefits of different features from different providers. A specific disadvantage of IOP is that in practice full compatibility cannot be achieved. This is especially true for digital services, which are subject to a high innovation dynamic. Thus, from the consumer's point of view, a noticeable incompatibility remains (e.g. with regard to new features such as self-deleting messages or reels and digital content such as certain emoticons and animated GIFs), so that significant network effects remain (also see Bourreau et al., 2022). In contrast, this problem does not exist with multi-homing, where consumers can interact with the full range of features on each network.

Both alternatives nevertheless aim at the same goal, the creation of horizontal competition within a platform market and thus the preservation of static efficiency. In contrast, however, there is the possibility of competition for the market, which is typical in the platform economy. Should an innovative provider enter the market in such a scenario, it will have a harder time generating corresponding demand effects solely on the basis of the non-interoperable features. In combination with a possible status quo bias of users (see Chapter 3.2.1), it is to be expected that the established platform will retain the majority of its users.

This weakening of competition for the market can additionally pose a threat to the dynamic efficiency of the platform market under consideration. If a supplier enters the market with a more efficient product (e.g. with more features, better technology or that can be offered at a lower cost), it is welfare-economically desirable to have a more efficient product. it is welfare-economically desirable for this supplier to gain market share as quickly as possible. Under horizontal IOP, however, it is no longer possible to reach a critical mass, since firm-specific network effects are largely negated. An economically sensible replacement of the then inefficient incumbent platform by the new provider cannot be expected in such a scenario (Bourreau et al., 2022).

Multi-homing, on the other hand, maintains competitive pressure for the market, as gaining a critical mass of consumers is still possible. Furthermore, in this case, a complete replacement or "tipping" of the market is up to the consumer decision of the users, as they can stop multi-homing at any time. This is the case if the benefits from the new superior service and possible cost savings from not multi-homing outweigh the loss of benefit from a possibly smaller network size. Multi-homing thus leads to "competition for the market", while IOP retains the opportunity for "competition in the market". Schumpeterian innovation competition in the sense of creative destruction (successive replacement of tipped markets by new innovative market entries) is thus still possible. IOP prevents the tipping of markets, but at the same time rules out the replacement of inefficient incumbents. Multi-homing thus preserves the general effectiveness of supplier-specific network effects, competition for the market and thus dynamic efficiency.

Horizontal IOP regulation and multi-homing are therefore only imperfect substitutes in the context of the platform economy and imply a trade-off. Promising factors that should be taken into account when weighing up static and dynamic market efficiency are, on the one hand, the existence of multi-homing and at what cost the parallel use of services is possible. On the other hand, the estimates of the probability and frequency of market entries as well as the disruptiveness of possible cost and product innovations (Bourreau et al., 2022). The analytical framework in Chapter 3.7 discusses these decision-relevant factors in more detail and derives corresponding recommendations for action.

### 3.3.2 Horizontal & Vertical: Patent hold-up and collusion risks in standard setting

The process of defining a technical standard should ideally standardise the objectively best technological basis. In this respect, the basic features of platform services that are essential from the consumer's point of view should be made horizontally interoperable while at the same time making the standard future-proof. At a vertical level, important innovation interfaces for upstream and downstream providers should be ensured. Nevertheless, there are incentives for companies to influence the definition process with the aim of integrating their own technologies and patents into the standard definition. The later use of the standard then only takes place under corresponding licence payments to the owner of these so-called "standard-essential patents" and ensures a constant monetisation of their own patents through the obligatory compliance with the standard. This problem is known in economics as "patent ambush or patent hold-up" and leads to the fact that such standards, contrary to their actual motivation, can act as a barrier to entry due to their high licensing costs (Farrell et al., 2007; Scott Morton et al., 2021).

In principle, outsourcing the standard setting process to neutral SSOs (Standard Setting Organisations) can be seen as a commitment device and a credible corporate strategy (Shapiro & Varian, 1998b; Sirbu & Hughes, 1986). Nevertheless, recent examples in the digital platform economy show that SSOs are in practice vulnerable to the interests of dominant providers. For example, Google is clearly overrepresented as an SSO in the World Wide Web Consortium (W3C) and is able to establish its own interests preferentially in standard definitions (Claburn, 2020). Similarly, the Majority Staff Report and Recommendations & Subcommittee on Antitrust (2020) of the US House of Representatives on competition in digital markets states that SSOs that are actually neutral are often reduced by Google to sales organs for their own features or business decisions that have already been made. Against this background, it seems sensible that not only the subsequent compliance with an IOP standard is monitored by the public, but also the process of setting it.

With regard to the process of setting an IOP standard, Chapter 2.2.1.6.2 has already explained that variable-volume payments should be avoided. However, there are additional risks of horizontal collusion that counteract the positive effects of the standard. First, communication between horizontally competing companies inevitably takes place in the course of the process, which includes exchanges about possibly accruing royalty payments. To determine such "FRAND" payments, information is shared that provides information on the respective cost structures of the companies. Sidak (2009) points out that such information significantly simplifies concerted pricing behaviour in downstream, standard-relevant retail markets. In addition to this possible channel to explicit collusion, there is also the risk of tacit collusion due to the reciprocity of possible royalty payments. If a standard contains essential patents from several horizontally competing companies, reciprocal payments for use should be avoided at all costs. From an economic point of view, this would link the profits of the respective companies, since larger profits of the competitors would flow proportionately into their own operating results through royalty payments received. In such a case, the companies internalise the effects of their own behaviour on their competitors, which inevitably leads to less competitive pressure (Shapiro, 2001). As a result, the reciprocity of such payments at the horizontal level is to be avoided in particular.

### 3.3.3 Vertical: Foreclosure trade-offs through vertically integrated platforms and "multi market contact".

Chapter 2.2.1 has already argued that incentives to provide vertical IOP differ between access-seeking and access-providing firms. The incentive dynamics, on the other hand, become increasingly complex when one or more platform companies involved are vertically integrated and compete at multiple levels of the economy (van Wegberg, 2004). Thus Bourreau et al. (2022) indicate that for an access-providing platform there is the possibility of strategic discrimination against the access-seeking complementary provider upstream. The aim of this is to achieve clear competitive advantages in downstream markets. This is operationalised, for example, through cost-driving measures to achieve a so-called "margin squeeze" (Bostoen, 2018), sabotage or quality deterioration. sabotage or degradation of the quality of APIs or their documentation (Mandy, 2000; Mandy & Sappington, 2007) or other forms of self-preference (Padilla et al., 2020). In extreme cases, these practices can lead to a complete foreclosure of downstream providers, as they can no longer cover their costs. Bourreau et al. (2022) cite as an example the competition case against Microsoft after the company made access to vertical IOP interfaces much more difficult or stopped it altogether after entering the workgroup server market. A court decision subsequently ordered the company to restore these interfaces (Kerber & Schweitzer, 2017).

In the context of vertically integrated firms, vertical IOP can therefore be seen as a double-edged sword. On the one hand, it allows competition from complementary products upstream or downstream, but on the other hand, if entirely market-driven, it provides a channel for anti-competitive and abusive behaviour by the access granting firm. On the other hand, the simultaneous presence of voluntarily provided vertical interoperabilities and vertical interconnections of a gatekeeper platform or competing companies may indicate a need to exogenously standardise corresponding IOP interfaces and monitor their compliance, if possible (similar to access regulation in telecom markets). Nevertheless, the mere existence of this fact should not justify an IOP measure to prevent foreclosure activities, as boundaries between economic levels in the digital platform economy are increasingly blurred and thus competitive effects of potential horizontal as well as vertical IOP mix with each other (Krämer & Schnurr, 2021). Taking into account the effective judgment on the above competition case about Microsoft, for example, Bourreau et al. (2022) also consider an ex post approach to the preservation of fair vertical IOP in complex vertical interdependencies as promising.

### 3.3.4 Horizontal: Less scope for product differentiation

The implementation of horizontal IOP implies that a set of core features is defined, interoperably standardised and available to users of all platform services. Competitive differentiation opportunities therefore only exist in non-standardised features. Scott Morton et al. (2021) argue that especially those features should be standardised and interoperable which on the one hand are particularly valued by consumers and on the other hand are critical to resolve existing firm-specific network effects. If the definition of standardised core features sensibly follows this argumentation, however, only less attractive product dimensions remain over which differentiation and competition can take place. Bourreau et al. (2022) point out that this results in a strong homogenisation of horizontally competing services with negative effects on product diversity and consumer benefits (see also Chapter 2.2.1.5).

The concern about too few opportunities for product differentiation is also cited by the Monopolkommission (2021) in its 12th sector report on the telecommunications market as a main argument against a mandatory horizontal IOP obligation in the market for messaging and video services, pointing to the danger that too much homogenisation through horizontal IOP could lead to customers even being less inclined to switch between different providers (cf. also Chapter 3.3.1).

### 3.3.5 Horizontal: Reduced incentives for innovation

Implications for innovation incentives under horizontal IOP work along the same impact channel of a reduced possibility for product differentiation. By defining interoperable core features, the current state of technology is "cemented" by standardisation (Bundeskartellamt, 2021). Innovations are thus channelled into product dimensions that do not belong to the standardised core features. In the case of digital platform services, these can be, for example, design aspects, easier handling, enhanced communication features (video, file transfer) or stronger encryption and privacy settings. If, however, these non-interoperable features are only valued slightly compared to core features and do not generate any increased demand effects, then corresponding innovation projects are not very attractive (Scott Morton et al., 2021).

Should innovations outside interoperable core features nevertheless be attractive to users and consequently induce significant demand effects, they could increasingly be seen as de facto essential features, although they are not included in the definition of the standard. The defined core features within an IOP standard thus structurally lag behind the actual consumer perception. Successful innovations thus weaken the impact of interoperable core features on a horizontal level and constitute a classic conflict of objectives (Bourreau et al., 2022). A rapid incorporation of successful product innovations of individual providers into the IOP standard would indeed award these features to other providers and re-establish IOP, but at the same time devalue important innovation rents. From the point of view of dynamic efficiency, horizontal IOP can thus hardly be justified.

### 3.3.6 Horizontal & Vertical: Implementation costs of standards for smaller companies

The implementation of IOP via standards requires the consultation of already active providers of platform services. At the same time, however, this poses a structural problem, as concerns of potential new market participants that do not yet exist are underrepresented in the standard-setting process. Existing providers thus basically have the possibility to influence a corresponding standard in such a way that it is difficult for small innovative companies to implement it. The technical complexity of the standardised technology, possible licence payments or even a too large number of interoperable core features that new services must satisfy can increase the costs of possible market entries. Mandatory IOP standards can thus be misused as a strategic barrier to market entry and represent an alternative "escape-entry" strategy in the sense of Aghion et al. (2009) for already established providers. First indications of this danger can be found in the survey of 44 providers of messaging and video services of the Bundeskartellamt (2021) can be found. Here it is warned that "especially smaller providers ... are disadvantaged in their competitiveness due to the high technical complexity [of standards], as larger providers would prevail in standardisation and could thus cement their supremacy" („*besonders kleinere Anbieter … aufgrund der hohen technischen Komplexität [von Standards] in ihrer Wettbewerbsfähigkeit benachteiligt sind, da sich größere Anbieter bei der Standardisierung durchsetzen würden und so ihre Vormachtstellung zementieren könnten*“) (Monopolkommission, 2021, p. 93). In the standard-setting process, it is therefore necessary to assess how realistic market entry is in order to avoid the creation of barriers to market entry.

### 3.3.7 Horizontal & Vertical: Data protection risks for consumers

From a data protection perspective, the implementation of IOP rules in the platform economy and messaging services is ambivalent. On the one hand, IOP obligations could reduce barriers to market entry for providers who place a particular emphasis on protecting the privacy of their users (VZBV, 2021, p. 24). This could have a positive impact on the level of data protection in the overall market. On the other hand, the implementation of an IOP obligation also creates new privacy risks for consumers, as both horizontal and vertical IOP require a two-way exchange of data between different providers.

From a data protection perspective, the transfer of data in a horizontal or vertical relationship qualifies as data processing within the meaning of Art. 4 (2) GDPR (General Data Protection Regulation). It must therefore meet the requirements for the lawfulness of processing under Art. 6(1) GDPR (Becker et al., 2021, p. 126). Insofar as no other permissible circumstance applies, the user's consent in accordance with Art. 6 (1) (a) of the GDPR is required for the creation of the IOP.

Particular data protection risks may arise, for example, in the case of horizontal IOP of messaging services, insofar as the transmission of messages between different providers requires the lifting of encryption. Even if end-to-end encryption (cf. Chapter 4.2.4) is ensured, metadata (information on the sender and recipient of the information, time of communication, location of the users, etc.) is generated during the transmission of messages. In an interoperable network, providers with whom the user has no direct business relationship also have access to this metadata. Thus, in a federated system, the extent of data processing by third parties is beyond the direct control of the users (Bundesnetzagentur, 2021). In view of the principle of data minimisation (Art. 5(1)(c) GDPR), the processing of metadata should therefore be limited to what is strictly necessary for the establishment of the IOP (Cyphers & Doctorow, 2021).

When assessing possible data protection risks, however, it must also be taken into account that IOP could prove to be the more data protection-friendly alternative compared to multi-homing. Depending on the design of the IOP obligation, this scenario could therefore prove to be more data protection-friendly in the end than if users install a multitude of messenger apps on their end devices in order to communicate with their contacts (VZBV, 2021, p. 27).

**Undesirable effects of interoperability**

Horizontal

- Horizontal IOP may **limit incentives for multi-homing** and thus competition for the market and **disruptive innovation,** as exploration and use of alternative services becomes less necessary
- Too much homogenisation **reduces differentiation opportunities** for companies in competition. This can lead to reduced product diversity and less supplier switching as well as less multi-homing.
- A **(flawed) definition of core features or standards** can cement existing technologies, channel innovation incentives into less relevant product dimensions (or miss the target of dissolving firm-specific network effects)

Vertical

- IOP can be **strategically restricted** and used in a discriminatory way to harm competitors in downstream markets. (Dominant) platforms or providers can increasingly copy interoperable products or features of external companies and integrate them into their own offerings (**"sherlocking"**).

Horizontal & Vertical

- Standardisation processes can cause **collusion risks** and **"patent hold-up"** if (market-) dominant companies can bring their own technologies and patents into the standard definition by exerting influence in return for licence payments.
- **Implementation costs** of interoperable standards and interfaces can be an additional **market entry barrier,** especially for small companies
- Under IOP, providers with whom users do not have a direct business relationship may have **access to (meta) data**. This creates **data protection risks,** as the extent of data processing by third parties may be beyond the direct control of users.

## 3.4 Interoperability and digital sovereignty

### 3.4.1 Dimensions of digital sovereignty

In recent years, "strategic autonomy" has emerged as a trend among policy makers in the major global economic blocs. The COVID-19 crisis has reinforced this trend, with countries increasingly reviewing their resilience and dependence on foreign suppliers of critical services and products, especially from countries outside their respective economic blocs. In relation to key ICT infrastructures, this strategic autonomy is often referred to as "digital sovereignty".

Kroon et al. (2020) compared approaches to digital sovereignty in Europe and the UK and found that policy makers ascribe different tasks and goals to digital sovereignty and use different terms, e.g. technology sovereignty or strategic autonomy. Despite these different definitions, the following common dimensions could be identified: 1) (private) data protection, 2) cyber security and 3) strategic interests (Kroon et al., 2020).

1. **The privacy** dimension is about the sovereignty of individuals to control their digital lives and personal data. The issues here range from the ability to extract the personal information collected from platforms, to transparency and control over where your personal data is stored, to encryption of personal conversations.
2. **The cybersecurity** dimension is about the sovereignty of countries and the EU with regard to cybersecurity and the resilience of the digital infrastructure. This dimension was the first to be recognised and implemented in Europe (Kroon et al., 2020). The ongoing debate on the exclusion of certain suppliers for Europe's new mobile networks due to security risks belongs to this dimension.
3. The **strategic dimension** concerns (re)gaining economic control and leadership in the digital domain. This is done by investing at EU level in key technologies such as artificial intelligence, robotics, chip production and high-performance computing, which are crucial for future economic development, but could also affect European values as large non-EU corporations become dominant in certain digital areas (e.g. from China and the US).

Although competition aspects predominate in the assessment of IOP, digital sovereignty must be taken into account in the assessment. Internal Market Commissioner Thierry Breton stated that digital sovereignty is "... not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent" (Breton, 2019).

Kroon et al. (2020) stressed that most digital sovereignty policies in Europe aim to strike a balance between achieving their own autonomy and maintaining a diversified portfolio of suppliers and international trade relationships that are important for many EU economies.

In the following sections, we will explore how IOP might affect the different dimensions of digital sovereignty.

### 3.4.2 Impact of interoperability on the dimension of personal data

The privacy dimension is about the sovereignty of the individual to determine the design of his or her digital life and thus also to be able to control the disclosure of personal data. Vertical IOP, which extends the functional scope of certain platforms with additional features and/or applications such as payment options, would result in the disclosure of certain user data in order to enable the feature of the complementary applications (cf. also Chapter 3.3.7). In addition, the integration of any trackers or advertisements or integrations such as map services as vertical additional services often sends data that is not actively communicated to the providing companies. This is an aspect that has been addressed in the context of the GDPR for websites.

The implementation of a horizontal IOP also requires that certain user data is exchanged, for example, to enable identification of the user. Currently, consumers have chosen certain services for various reasons, be it their functionality or their popularity (most acquaintances are users of that service), while higher security, better privacy or, in the context of social networks, a differentiated nature of the content are decisive for the choice of the service. These aspects of consumer interests, which are reflected in the horizontal differentiation of services, must be taken into account under sovereignty aspects when designing IOP.

Beyond product differentiation, the differentiated approach to privacy and security aspects is also relevant for the design of IOP. For example, horizontal IOP could lower the security standards of services, as it is difficult to fully reconcile two different encryption technologies and different security approaches without compromise.[13] Therefore, compromise at lower security levels cannot be ruled out. Furthermore, in the context of IOP, the subsequent implementation of interfaces, whether to realise horizontal IOP between social networks or vertically in the course of content moderation, is conceivable. Subsequent opening of services that may not have been designed for this purpose can lead to additional security risks and possibly encourage the misuse of these interfaces. In this context, the misuse of a Facebook API by Cambridge Analytica, a British consulting firm, is worth mentioning. Cambridge Analytica used an application programmed for academic purposes with access to the Facebook API, accessing not only the data of test participants who consented, but also the data of their Facebook "friends". While the terms of use only provided for the collection of data from those who consented and excluded commercial exploitation, Cambridge Analytica was nevertheless able to collect data for over 50 million users from the social network with the consent of several hundred thousand users (Cadwalladr & Graham-Harrison, 2018). In Chapter 4.2 we will classify these concerns about messaging services and analyse the technical aspects.

[13] This may include storing communications on servers, sending data to the cloud or only to servers in the relevant country and requiring personal identification for subscription.

### 3.4.3 Impact of interoperability on cyber security

Cybersecurity in the context of national sovereignty has focused on preventing cyber attacks on key national infrastructures. This has become more important due to advancing digitalisation and especially during the COVID crisis. The increasing geopolitical power play between the USA, China and Europe has brought national and European cyber security into even sharper focus.

IOP regulations could also lower the security standards of messaging services, for example. This aspect is described and 4 of this study. However, these security concerns relate more to the personal level and not to the national and European security level, which is generally considered when reviewing the cybersecurity dimension of digital sovereignty. However, there might be some aspects that are more on the national and European level: When messaging services active in the EU store their data in non-EU clouds or when IOP is implemented between messaging platforms active in the EU and outside the EU. For example, WhatsApp data is stored in US cloud services, so it falls under the US cloud law[14] , while other non-EU messaging services such as WeChat could be subject to wide-ranging interception by national security authorities in their own country, or at the physical location of the servers where some of the aggregated EU user data would be stored. But again, this aspect primarily concerns the protection of personal data.

#### 3.4.3.1 Increasing importance of robust cloud infrastructures

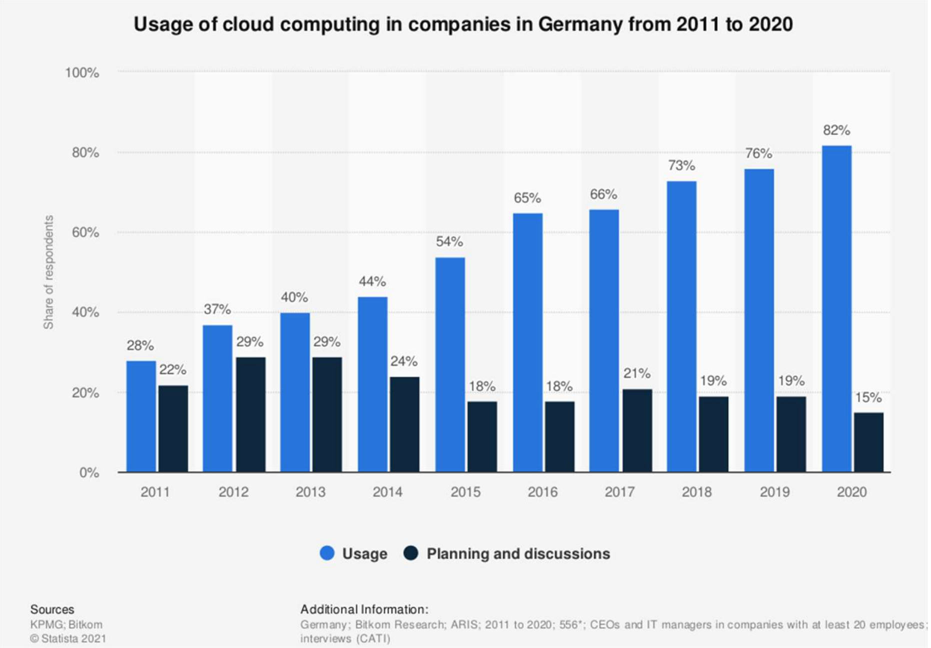
Communication services important for the EU, but also platforms, often use cloud-based infrastructures that are physically located inside and outside the EU. In addition, the same cloud services often play an increasingly important role for business customers, but also for government bodies, and can therefore be considered critical infrastructure at national and European level. These cloud services can be infrastructure, platform or service related (IaaS, PaaS, SaaS).[15] In addition to these categories of cloud services, there is also the option of operating a cloud under one's own control (private cloud) or using public cloud services from e.g. AWS or a mixture (hybrid cloud).

The following figures show the increasing importance of cloud services in Germany and Europe. The resilience of this infrastructure is thus becoming an aspect of digital sovereignty.

[14] Under the US Cloud Act, data stored in the US or by US companies is subject to US law, regardless of where the data is located. See (US Kongress, 2018).

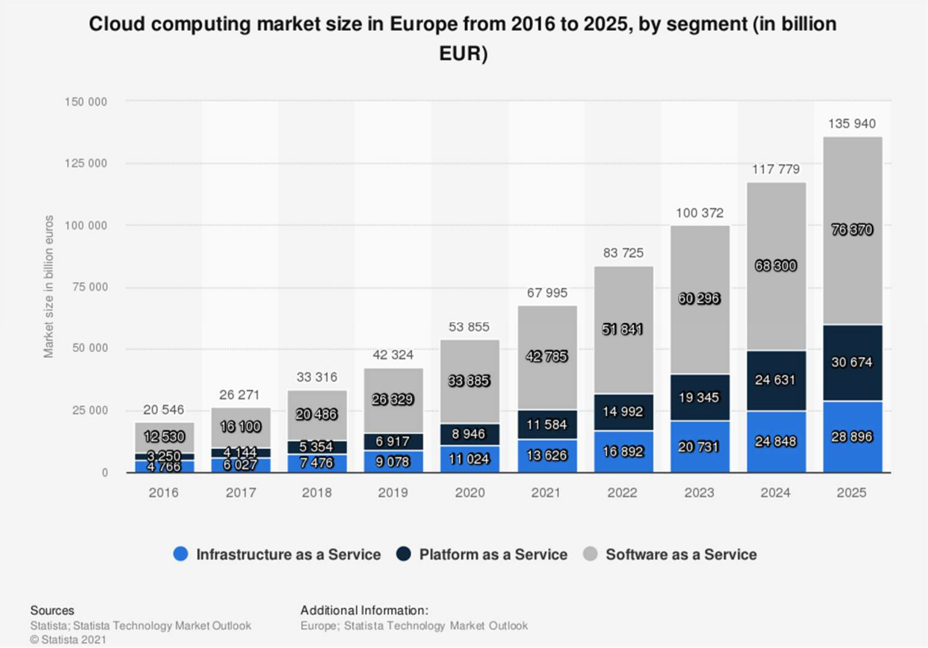
[15] Designated as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Figure 3-2: Use of cloud computing by German companies from 2011 to 2020



Source: Statista (2021)

Figure 3-3: Cloud services revenue by product type from 2016 to 2026 (forecast)



Source: Statista (2022)

### 3.4.3.2 Interoperability as a guarantee for a multi-cloud setup

In terms of resilience, not relying on a single provider (i.e. having a backup) has always been a good practice for critical digital infrastructure, which is why many companies prefer a so-called multi-cloud configuration. This requirement is being addressed by the industry, with leading players such as AWS, MS, IBM and Google offering (horizontal) IOP between multi-cloud IaaS environments. Several interrelated factors seem to be at play here: from customer preference for a multi-cloud configuration, to the existence of many standards for IaaS, to the commercial interest of vendors to offer this integration to ensure market acceptance of IaaS.

Lewis (2013) already described how horizontal IOP works for IaaS cloud services in her early research on IOP for cloud services and identified four typical IOP use cases for cloud computing such as workload and data migration, user authentication and workload management. It also found that standardisation efforts are mainly focused on these basic use cases in the IaaS segment (Lewis, 2013).

However, the impact of a further consolidation of the IaaS cloud market with the PaaS and SaaS markets remains unclear. The multi-cloud concept for the IaaS market at least seems to prevent a complete dominance of the US-based IaaS cloud services and therefore has a positive impact on digital sovereignty. Here, it is important to note that the cloud market is very differentiated and still evolving very dynamically. Therefore, (horizontal) IOP might not be a general solution, but only a future tool in relation to certain defined and standardised use cases.

A related strategic aspect of digital sovereignty is that by ensuring a multi-cloud approach for customers, European IaaS cloud providers at least have the chance to maintain their position against the mainly US-based market leaders. The proposal for the European Data Act, which proposes a new generation of EU cloud services to meet the highest standards of data portability and IOP, should also be seen in this context.[16]

However, the multi-cloud setup can also have a negative impact on the resilience of digital infrastructure. A 2019 TechRepublic article found that a multi-cloud environment doubles security risks; 52% of multi-cloud environments were attacked in 2019, compared to 24% of organisations using a hybrid cloud or single cloud (Sanders, 2019). In addition, a report by Nominet (2019) also found that multi-cloud environments are more likely to be affected by security breaches, with 69% of these organisations reporting between 11 and 30 breaches, compared to 19% of single-cloud organisations and 13% of hybrid-cloud users.

[16] The proposed Regulation on harmonised rules on fair access to and use of data - the Data Act - adopted by the Commission on 23 February 2022.

### 3.4.4 Impact of interoperability on strategic aspects

As mentioned above, the strategic aspects of digital sovereignty focus on (re)gaining economic control and leadership in the digital domain. This ranges from initiatives in AI, high performance computing to chip manufacturing and cloud standardisation/unification efforts such as GAIA-X, as well as control over "EU data".[17]

A practical problem is the very strong market position of non-EU-based companies such as cloud providers, messaging services, social networks and e-commerce plat forms based in the US, but also hardware and software manufacturers from Asia.

In the field of information and communication technology (ICT), there are several standardisation bodies, the best known of which are the ETSI (European Telecommunications Standards Institute), the ITU (International Telecommunication Union), the GSMA (Groupe Speciale Mobile Association) and the 3GPP (3rd Generation Partnership Project) for telecommunications services. The IETF (Internet Engineering Task Force) is also responsible for internet standards and the W3C for World Wide Web standards. ICT companies are members of these bodies and participate in the standardisation processes, which are based on agreements between the members of the bodies. In addition, providers of hardware and software have formed alliances in the past to bring certain technology standards to the market with the aim of establishing them as a de facto standard.

Generally, members of standards bodies provide input on proposed standards and provide representatives for working groups or so-called task forces that discuss the proposed standards in detail. These expert groups then report back to their members and the standards body's board. Consensus decisions on the proposed standards are made in dedicated meetings.[18] This process can take some time and consequently tie up considerable members' time and human resources. This means that established larger companies with more financial resources can afford to participate longer and more intensively in these standardisation processes than, for example, start-ups. Therefore, it is more likely that standards in these processes will be designed in a way that accommodates the larger market players.

Many segments of the ICT market are already highly concentrated (e.g. messaging services, social media platforms, but also software or cloud infrastructure), and US companies in particular have a dominant position. Under these aspects of digital sovereignty, the use of IOP rules can be considered to enable European competitors to expand or maintain their market position against these dominant companies. However, to enable IOP for ICT in general, one needs certain standards to ensure syntactic and semantic compatibility, making features and data integrable and/or linkable between applications and/or platforms. As described above, the large market players in particular are in a position either to delay the standardisation process or to steer it in a direction they prefer, but

[17] This refers to data originating from European businesses and/or obtained from European consumers.
[18] See for example ETSI (2022) and IETF (2022).

which need not be advantageous for smaller EU companies. Therefore, oversight and/or a regulated process for standardisation projects is needed. This can ensure that standards are agreed in a reasonable timeframe and that members' interests are adequately represented, regardless of market size and 'costs invested'.

In the context of standardisation, GAIA-X is also worth mentioning as it aims to create a European standardised data infrastructure that complies with European law, reflects data portability, the highest data security criteria, transparency on data use and applicable EU Member State rules, and promotes innovation. Standardisation plays an important role in this ecosystem, as existing infrastructures of GAIA-X members will be interoperably connected and made accessible through a common user interface, and will be subject to uniform open source standards and user rules.[19]

For European cloud providers, GAIA-X offers the possibility to provide virtual scaling within an open ecosystem and scalability of services, an aspect that has been a major competitive advantage of (mainly US) hyperscalers.

**Effect of Interoperability on Digital Sovereignty**

Impact of IOP on privacy protection

- Vertical IOP brings with it the danger of intransparency about the transfer and storage of data across company boundaries.
- Horizontal IOP for messaging services could lower the security standards and privacy level of messaging services. In practice, a similar level of utility can be achieved through multi-homing on the part of users.

Impact of IOP on cyber security

- Due to the increasing importance of cloud services, the resilience of this infrastructure is becoming an aspect of digital sovereignty that can be countered by a multi-cloud setup.
- For a variety of reasons, the industry itself offers (horizontal) IOP between multi-cloud IaaS environments. This is important both for resilience and for the market position of European IaaS cloud providers vis-à-vis the, mainly US-based, market leaders.

Impact of IOP on strategic aspects

- There is a conflict of interest as dominant parties may have a steering role in standardisation processes that are required for IOP. Therefore, there should be objective oversight of these processes to avoid delays and to ensure that the interests of all industry members are represented, regardless of market share.

[19] See https://www.data-infrastructure.eu/GAIAX/

- Horizontal IOP could theoretically help to reduce market concentration in messaging services. However, research shows that consumers in Germany use on average just under four services simultaneously despite network effects. This is due to product differentiation, innovation, low costs of multi-homing and a heterogeneous set of contacts, suggesting that IOP is not necessary.

## 3.5 Interoperability obligations as a solution approach

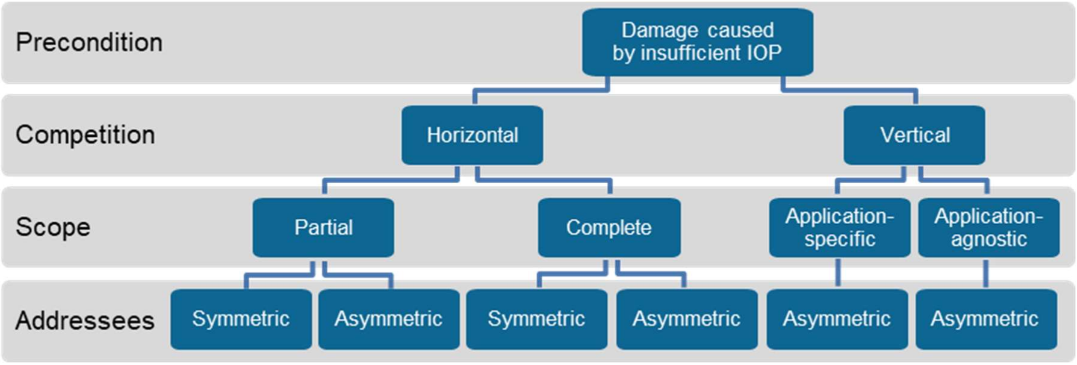
In this Chapter, we will break down the conditions under which the potential damage caused by a lack of IOP can be addressed with the help of specific IOP regulations. Therefore, an analytical framework is presented below that allows for a granular and case-specific analysis of IOP regulations based on different dimensions.

This approach has the advantage that the specific positive effects and risks of potential IOP regulations can be considered in a differentiated manner based on the prevailing market conditions and moderating factors and can be assessed in the context of any services with the help of the analysis scheme IOP. The following general analytical framework can therefore be used to make an initial assessment of IOP regulations in any category of services in digital markets.

### 3.5.1 Analysis scheme

The overview in Figure 3-4 first illustrates the general process of an analysis of possible IOP obligations. In order to do this, it is first necessary to identify damage caused by insufficient IOP and thus a market failure that justifies regulatory intervention in the form of an IOP obligation or a necessary implementation of European legislation that is already based on a corresponding assessment.

Figure 3-4: Graphical representation of the analysis scheme



Source: WIK-Consult

Next, the competitive context in a specific service category has to be assessed. If the services are primarily of the same kind at the same level of the value chain, this is a case of horizontal IOP. If access to a specific stage in the value chain through upstream or downstream services is at the core of the problem, it is a case of vertical IOP.

If, after the assessment made so far, the benefits of IOP under the prevailing market conditions and moderating factors justify the introduction of an IOP obligation, a decision on the design of such an obligation must be made further on.

This concerns first of all the scope of the IOP obligation with regard to the degree of features and application scenarios covered, as well as the addressees of the companies affected by the regulation. As already provided for in the DMA, obligations can also be imposed asymmetrically and therefore only include companies above a certain size or number of users.

#### 3.5.1.1 Competitive relations and interoperability rules

Following the identification of insufficient IOP or the need to transpose European requirements into national law, the advantages and disadvantages of an IOP obligation must be assessed in the context of the competitive environment. Table 3-1 systematically summarises the moderating market conditions as well as the positive and negative effects. The assessment column contains an initial general assessment of IOP obligations under the relevant competitive conditions.

Table 3-1: Competitive relationships and IOP regulations

| | Cause | Moderating Conditions | Positive effects of IOP | Risks of IOP | Assessment |
|---|---|---|---|---|---|
| **Horizontal** | **Market concentration** through company-specific (data-driven) network effects | • Availability of voluntary IOP<br>• Prevention of "adversarial“ IOP<br>• Costs of multi-homing<br>• Level of multi-homing<br>• Probability of innovative market entries<br>• Innovation dynamics<br>• Existing level of data protection / privacy / security<br>• Technical complexity of the service | • Reduction of market concentration (company-specific network effects)<br>• Innovation incentives for non-interoperable features and quality<br>• Advantage for small enterprises (to the disadvantage of larger enterprises)<br>• Reduction of lock-in effects | • Less scope for product differentiation<br>• Reduced incentives for innovation in interoperable features (entrant)<br>• Patent hold-up and collusion risks during standardisation<br>• Inhibiting competition for the market<br>• Reduced data protection / privacy / security<br>• Reduced incentive for multi-homing (dependency on IOP standards for entrants)<br>• Implementation costs | Risks outweigh if<br>• Costs of multi-homing low<br>• Level of multi-homing high<br>• Market interest low, e.g. indicated by low efforts to achieve/prevent "adversarial" IOP. |
| **Vertical** | **Lack of innovation interfaces** prevents access to value creation stages | • Availability of voluntary IOP<br>• Prevention of "adversarial“ IOP<br>• Vertical integration of ecosystems<br>• Probability of innovative market entries<br>• Innovation dynamics<br>• Existing level of data protection / privacy / security<br>• Technical complexity of the service | • Stimulation of innovations (planning security)<br>• Reduced barriers to entry and increased competition for complementary services<br>• Reduction of lock-in effects | • Patent hold-up and collusion risks (in case of multi-market contact) during standardisation<br>• Lower innovation incentives for access providers<br>• Double marginalisation (across several stages of the value chain)<br>• "Sherlocking"[20]<br>• Reduced data protection / privacy / security<br>• Implementation costs (standardisation)<br>• Regulatory costs (implementation, monitoring, compliance, redress) | Advantages outweigh if<br>• Vertical integration high (ecosystems)<br>• Low availability of voluntary IOP |

Source: WIK-Consult

[20] "Sherlocking" means that the operator of a platform/service/operating system adapts and integrates functions that make the installation of an existing (popular) third-party tool superfluous. The neologism goes back to the first prominent case of the Mac software "Watson", which offered information from the internet in a native search interface in Mac OS as a complement to Apple's own search interface "Sherlock". The Watson application was very popular until Apple released Sherlock 3 with Mac OS X 10.2. In this version, Apple replicated almost all the features of the Watson software, effectively making Watson obsolete from the user's point of view.

### 3.5.1.2 Scope and addressees of interoperability rules

In Table 3-2 we summarise the findings on the scope of possible IOP regulations. As already explained, IOP in various dimensions (e.g. functional scope, time, etc.) is to be seen as a continuum. At this point we therefore discuss the trade-off between partial and full IOP in the case of horizontal competition, or application-specific and application-agnostic IOP in the case of vertical competition. In the former case, the focus is on developing interfaces between different stages of the value chain for specific use cases. To a certain extent, these can also be used "for purposes other than their intended purpose", but they also reach their limits because not all desirable features are mapped for use cases not previously considered. Thus, application-agnostic IOP requires considerably more general and thus more extensive interfaces in order to be able to map new application scenarios.

Table 3-2: Scope of IOP regulations

| | Scope | Moderating conditions | Positive effects of IOP | Risks of IOP | Assessment |
|---|---|---|---|---|---|
| Horizontal | Partial | • Speed of standardisation<br>• Technical complexity of the service | • Greater scope for product differentiation and innovation | • Can render IOP regulations ineffective<br>• Difficulty of identifying and dynamics of relevant core features | In case of separability of demand-relevant core features and other additional features for niches. |
| | Complete | • Speed of standardisation<br>• Technical complexity of the service | • Balanced competitive environment | • No scope for product differentiation/innovation (only in the market / not for the market)<br>• Implementation costs | If separability of demand-relevant core features and other additional features for niches is not sufficiently possible. |
| Vertical | Application-specific | • Availability of open APIs<br>• Existing application scenarios in vertically integrated ecosystems | • Competition with vertically integrated services possible<br>• Innovation within existing application categories<br>• New compositions of existing applications | • Complex access pricing<br>• Implementation costs<br>• Disintermediation of matchmakers | If<br>• Competition (prices) in upstream and downstream value creation stages low (high)<br>• Implementation costs and complexity high. |
| | Application-agnostic | • Existence of private APIs without public access<br>• Restricted access to hardware interfaces | Additional:<br>• Innovation through new application categories | • Complex access pricing<br>• Implementation costs | If<br>• Innovation in upstream and downstream value creation stages low<br>• Implementation costs and complexity moderate. |

Source: WIK-Consult

In Table 3-3 the scope or addressees of an IOP obligation is clarified in relation to the competitive relationships. First of all, it should be noted that in the case of vertical competition, symmetrical IOP is not possible, as the focus here is on access to an essential part of the value creation under the control of a company. In the case of horizontal competition, it must be clarified whether the IOP obligation should only apply to certain companies that have a strong market position (e.g. financial strength, number of users, etc.) or equally to all providers of a certain type of service (e.g. messenger).

Table 3-3: Addressees of IOP regulations

| | Horizontal | Vertical |
|---|---|---|
| **Asymmetric**<br>(Affected from threshold value e.g. for company size, number of active users, turnover etc.) | Competitive advantage for smaller companies. | Access for third-party providers to core services possible. |
| **Symmetric**<br>(Affects all companies in a service category equally.) | Balanced competitive environment for small and large companies. | Not possible |

Source: WIK-Consult

### 3.5.2 Analysis parameters for the specific case analysis

When assessing specific service categories or the position of individual companies in the value chain, other factors should also be taken into account. Depending on the sector, market structure and competitive environment, different parameters can influence the assessment, e.g. to what extent in particular multifunctional services and/or services belonging to vertically integrated ecosystems are (possibly even simultaneously) in horizontal or vertical competition. Other factors are explained in more detail below.

#### 3.5.2.1 Existing interoperability and standards

First of all, it should be assessed which forms of IOP are already possible or offered voluntarily in a market economy environment and whether they are also made use of. It should also be examined whether a targeted prevention or artificial impediment of IOP (adversarial) can be observed. The use of existing (commercial) offers can also be deliberately restricted by disproportionate conditions of use or prices.

Equally relevant appears to be the availability of standards in a particular service category or for particular applications. IOP can also be prevented by companies through the targeted implementation of (or insistence on) proprietary technologies despite the availability of adequate standardised alternatives. In this context, it should also be examined whether companies have already offered IOP in the past and only stopped it, for example, when they made their own forays into adjacent business areas.

### 3.5.2.2 Business models and data

Business models in multi-sided markets are often based on matchmaking, i.e. bringing two (or more) market sides together through a platform. This is the case, for example, with app stores (end users/developers), online advertising (end users/advertisers) and mobile payment services (buyers/sellers). Mandatory vertical IOP can therefore threaten such business models through "disintermediation". The term describes a loss of importance of intermediaries due to the loss of control over individual essential stages of the value chain.

Furthermore, there is a fundamental difference in monetisation between ad-financed and paid services. While data-driven network effects have a direct impact on the monetisation of ad-supported services, this is only indirectly the case for paid services through quality improvements. IOP and access to data in real time can therefore have a different effect on services in these categories.

For example, an algorithm optimised "within-user" leads to an increase in personal lock-in. This lock-in can, however, be resolved relatively easily through a one-time portability process. In contrast, the result of an "across-user" optimising algorithm (e.g. recommendations based on trend analyses of all users) is not easily transferable through data portability. However, even IOP cannot directly transfer such a data network effect, but may induce greater use of alternative services (switching and/or multi-homing) and thus indirectly transfer these data-driven network effects.

### 3.5.2.3 Switching and multi-homing

Depending on the market conditions and situation, switching and multi-homing can substitute each other in their effect, but this is not generally the case.

In a broader sense, switching also enables multi-homing. In a narrower sense, switching refers to the changing of providers in the case of single-homing, i.e. switching to another, comparable service, whereby the original service is no longer used. Therefore, a low level of multi-homing is not problematic per se, especially if it is easy to switch providers. Therefore, a key question in the assessment of specific services or value creation stages is whether switching providers and multi-homing is even practically possible and what costs are actually incurred in switching or parallel usage.

(Data) IOP can nevertheless also help in the case of existing multi-homing, i.e. the continuous parallel use of several services, to keep data such as address books or playlists synchronised and up-to-date. In the case of pure switching, on the other hand, a one-time, one-sided porting of the data would be sufficient.

Furthermore, the actual observed level of multi-homing is relevant as it shows whether customers make practical use of this option to avoid missing IOP. For example, high costs may explain low levels of multi-homing, but are not sufficient to do so (e.g. if the cost of missing IOP is very high). These costs can also be controlled directly and indirectly by providers, for example through user interface design or contract design.

## 3.6 Technical requirements for various interoperability solutions

In the context of digital platforms, with regard to the technical requirements of IOP, it should be emphasised that the digital platforms under consideration are based on modular components that work together to fulfil a function. Tiwana et al. (2010) define software-based platforms such as operating systems as a comprehensive basis of software code whose basic functionality is extended by interoperable modules that make use of interfaces. Operating systems in particular are based on an extensive expansion of features through modules. Tiwana & Konsynski (2010) describe this as a process of softening monolithic architectures towards modularity. De Reuver et al. (2018) see the applications in the context of mobile operating systems, which provide features for the end user, as a combination of different layers of modular resources. These modular resources are features of the operating system, hardware, software development kits and features of programme interfaces (APIs). However, in order for new apps to be programmed, they must establish a syntactic and semantic IOP to the features and interfaces. In addition to this interchangeability and compatibility, detailed documentation is also required to ensure usability. The extent to which a digital platform provides this and to what extent is characterised in the literature with the "openness" of digital platforms. This openness of a platform is related to the governance structure of a platform and, according to Benlian et al. (2015), requires a careful balancing of control and autonomy of complementary services. Table 3-4 shows the criteria proposed by Benlian et al. for categorising the degree of openness of digital platforms. Although this categorisation refers in particular to mobile operating systems, the concept of openness can also be applied to other platforms and thus other vertical relationships.

Table 3-4 Indicators of the degree of openness of digital platforms

| | Transparency | Accessibility |
|---|---|---|
| **Technical Platform** | • The platform offers features that allow developers to communicate and exchange with other developers (*exchange among developers*)<br>• The documentation of the technical platform includes all relevant information for the development of applications (*technical documentation*)<br>• The platform offers features to receive instant technical support from the platform provider (*technical support by provider*) | • It is easy to make oneself familiar with the platform's technical standards (*learnability of technical standards*)<br>• The platform offers helpful tools that make the development of applications easier (availability of development tools)<br>• The platform supports technical interoperability (i.e., compatibility) with other systems or platforms (*technical interoperability*)<br>• The scope of functionalities that is made available to developers (via APIs) is limited (*functional scope*)*<br>• The technical performance of the platform constrains the functioning of applications (*technical performance*)*<br>• The initial costs for technical requirements (e.g., annual fees for the developer community, hardware requirements) are limiting the access to the platform (*cost of required technical equipment*)* |
| **Distribution Channel** | • The platform provider openly communicates the review and marketing guidelines (*communication regarding app review and marketing guidelines*)<br>• The terms and conditions of the platform's marketplace (i.e., about promoting and selling apps) are transparent (*transparency of terms and conditions*)<br>• The notification practices of the platform provider (e.g., about planned changes in the terms and conditions) are transparent (*notification practices*)<br>• The search, filter, and ranking mechanisms of applications (i.e., application discoverability) on the marketplace are clear to developers (*transparency of market mechanisms*)<br>• The platforms marketplace allows and supports communication between application developers and end-users (*communication with end-users*) | • The costs of selling applications on the platform's marketplace (e.g., revenue share paid to platform provider, fees for billing system, etc.) constrain developers in distributing their applications (*cost of selling*)*<br>• The terms and conditions of the marketplace (e.g., on payout schedules and thresholds) constrain developers in their sales activities (*distribution restrictions in terms and conditions*)*<br>• The application review and marketing guidelines constrain developers in distributing their applications (*constraints through app review and marketing guidelines*)* |
| ** Reverse-coded items* | | |

Source: Benlian et al. (2015, p. 10)

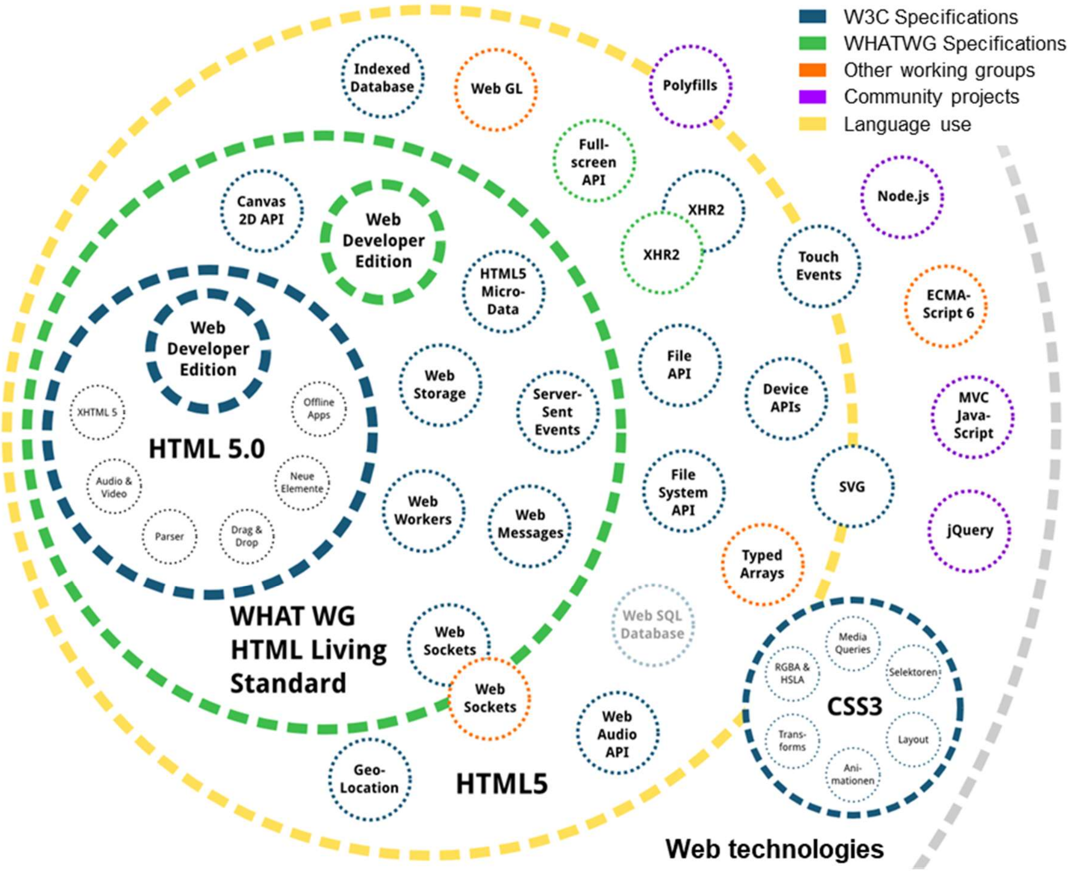
Digital platforms are subject to the paradox of change according to De Reuver et al. (2018), a trade-off between stability and durability of the system while adapting to dynamic processes of growth and functional expansion. In the example of mobile operating systems, software development kits (SDKs) are made available for this purpose as comprehensive frameworks that provide third-party providers with structured and controlled access to the (current) features of an operating system. There is also usually extensive documentation for publicly accessible services that can be reached via web services, although system security aspects are less relevant here.[21] Due to the increasing use of web and cloud services realised via computer languages such as HTML5, whose visualisation is provided in the browser and thus independent of the underlying operating systems, platform-independent applications and services have become increasingly important. While active content and videos used to be realised via Flash or dedicated apps, modern videos and some active content are based on HTML5. In contrast to Flash, this is also natively supported by mobile browsers and does not require any additionally installed plug-ins. Figure 3-5 shows the extensive functions that the W3C as a standardisation organisation and the WHATWG (Web Hypertext Application Technology Working Group founded as an industry working group) on the one hand define as a standard and on the other hand use as a term in the context of HTML5. The orange circles represent functions that are sometimes used in browser applications but are not part of the standard. In addition, the graphic also shows the modular structure of modern standards, which work together for the realisation of web services, through the relation of the individual features.

The data generated and exchanged in the context of the service provision of web-based applications can be distinguished into three forms from the procurement perspective according to Crémer et al. (2019). The volunteered, in part also necessary[22] , data provision by the user is data that is actively provided by the user. This can include, for example, e-mail addresses for identifying and contacting users or voluntary information such as addresses or telephone numbers. Observed data, on the other hand, can only be collected by the services through active use and can, for example, represent histories of visited articles, profiles or the frequency of mutual contact. Building on this voluntarily provided and observed data, a large part of the strength of the digital economy lies in the linking of data and the subsequent inference of new data. Inferred data can consist of new product suggestions based on a user's preference profile. This process is related to the 'learned' data-driven network effects as described in the Chapter 3.1. Crémer et al. (2019) however point out that a precise distinction between these forms is unambiguous and not trivial.

[21] Security services such as Cloudflare and authentication keys for APIs can be used to secure open interfaces of web services.

[22] In this context, necessary is not to be understood in opposition to voluntary, as data to be provided is accepted by the user as part of the contractual usage agreement. Furthermore, necessary can also be understood as necessary for the provision of the service, for example if an email address is required for resetting a password.

Figure 3-5: The relationships between web technologies and standards in the context of web services



Source: Kröner & Divya (2013)

Furthermore, the extent to which these forms of data are used in a personalised manner is also relevant. Here, Crémer et al. (2019) distinguish between the identifiable and the anonymised use of personalised data at the individual level. Above the level of personal data, aggregated data and contextualised data are to be located. This distinction in the use is not only relevant with regard to competition, but also under aspects of data protection, since in the case of access there is a risk of unintended data disclosure.

Furthermore, data is usually available in three typifications in the corresponding platforms and digital services (Salinas & Nieto Lemus, 2017). Structured data follows a standardised schema. This data can, for example, be stored in data structures and managed and queried in databases using standardised languages such as SQL. As an example, JSON is mentioned here as one of the most common structured data formats, which can store and transmit hierarchically structured data in particular. Other structured file formats are explained in more detail in Chapter 3.6.2 in more detail. Structured data are higher in quality and processability than unstructured data, which, according to Salinas and Nieto Lemus, can be repeated over time (e.g. sensor data) or not repeated over time (e.g. texts, images, videos).

Unstructured data is often associated with large data volumes and Big Data and can be collected via sensors, for example, or can arise as observed data when using a service. However, this requires processing or interpretation. The first step is to "clean" the data in order to then structure it consistently. Due to the widespread use of common file formats and a multitude of converters and adapters, syntactic compatibility is generally to be expected. Databases are needed to store the data, which are either relational or non-relational, depending on how the data is structured. A conglomerate of databases is referred to accordingly as a data warehouse (structured) or data lake (unstructured), for example in the case of context-free raw data. March et al. (2000) describe the data warehouse approach as the result of the syntactic and semantic aggregation of several distributed operational databases. The process here requires extraction followed by the correction of errors, the addition of missing observations and the subsequent conversion into a uniform format for syntactic, structural and semantic unification.[23] The difficulty here, according to March et al, is to take into account the differences necessary to maintain compatibility with specific systems and the usability of information across the boundaries of these systems. At this point, it should be emphasised that this approach is a necessity for the efficient design of internal processes due to the distribution of data-processing processes across different areas of the digital platforms. For this reason March et al. (2000) emphasise the relevance of *flexible schemas with versioning including documentation.*

While Article 20 (1) of the GDPR provides a legal framework for the portability of personal data, IOP, as already explained in Chapter 2.1 is to be understood in a more far-reaching way. Above all, the temporal immediacy and, where applicable, the reciprocity in the exchange of data increases the need for coordination of IOP compared to pure data portability. Nevertheless, data portability as a legal framework that has already been implemented serves as an example of the greater challenges associated with IOP in terms of technical requirements.

As already discussed in Chapter 2.1.1.1 data IOP should be understood as a continuous variant of data portability (Bourreau et al., 2022). According to Syrmoudis et al. (2021), a first analysis already shows discrepancies between the requirements and implementation of data portability. For example, the requirements of Article 20 (1) of the GDPR are limited to data portability in a "structured, commonly used and machine-readable format", whereas Article 20 (1) of the GDPR does not contain any further specifications, which is

[23] March et al. (2000) cite examples such as internal conventions for naming variables or the conversion of different units (e.g. currencies, units of measurement).

why, according to a preliminary empirical study, more than 70% of the data imports carried out do not function completely (Syrmoudis et al., 2021). To improve data portability, the "Data Transfer Project" of the companies Microsoft Google, Twitter and Facebook was created, which provides features and interfaces as well as file typing on the basis of an open source code. Krämer et al. (2020) compared the number and proportions of source code changes and found a large share of over 80 % on Google's part, while the project and also the number of changes lag significantly behind other open source projects with 44 thousand lines of code compared to popular machine learning applications such as Tensorflow (2.5 million lines of code). Krämer et al. (2020) conclude that the Data Transfer Project is not being pursued with a strong allocation of resources.

Taking into account the modular composition of services in the platform economy described at the beginning, the "openness" of the platform becomes more important with regard to the mix-and-match approach. If one applies the "Equivalence of Inputs" approach proposed by Bourreau et al. (2022), access to the documentation of interfaces, transparent communication of adjustments and a comprehensive semantic explanation of the data is necessary from a purely technical point of view, just as it would be available for a vertically integrated company. Only in this way could all providers in the platform economy provide the same product or service on the same terms and conditions (including price and service levels) via the same systems and procedures.

Benlian et al. (2015) point out in this context, however, that transparency and accessibility are by no means always in sync in practice. This distinction can be illustrated by Apple's handling of the NFC interface on its mobile devices. While the contactless data transmission NFC itself follows a publicly accessible standardisation, access by third-party apps to this interface within Apple's mobile operating system iOS was initially largely impossible. Therefore, Benlian et al. (2015) conclude that both aspects are to be defined independently of each other, but are nevertheless in a complementary relationship to each other, since a platform can only be defined as fully open by both dimensions.

The most extensive form of IOP and also the most technically demanding is protocol IOP, in which direct, complete and immediate interaction of the systems takes place on the basis of jointly selected or defined standards. This also enables a complete substitution of services, but also requires the highest degree of coordination and documentation.

As a prerequisite for all forms of IOP and in distinction to pure portability, usable programming interfaces and open or standardised data formats must be mentioned, which is why these two aspects will be considered in more detail below.

### 3.6.1 Continuous access to data and features in real time

Application programming interfaces (APIs) provide a functional bridge between a software or service and further use. They are to be understood as the communication interface of one programme towards another. They are an association of predefined methods and objects that can be used to access the product of the previous level without having to fully implement the process or the original objects. With this abstraction of individual processes, it is possible to represent distributed, complex programmes as a collection of individual models. The resulting modularity changes the task of programmers from basic programming to "stitching together" features, according to Stylos (2009). Because of this simplification, the widespread use of APIs is common in the course of digital platforms (Stylos & Myers, 2006). Bloch (2006) already highlighted the importance of well-functioning APIs for the success of the enterprise. He also notes that software and features have to be thought about and programmed in a modular way. Each module should be provided with an interface so that the modules can be reused elsewhere. He defines the characteristics of good APIs for the user side as being easy to understand and simple to use, even without documentation. This requirement reflects the criterion of usability as a prerequisite for IOP. At the same time, consideration should be given to limiting wilful or unintentional misuse. For the technical audience, he says, easy readability of the code, with simultaneous easy maintenance and expandability, is essential. He also emphasises the importance of good documentation, which provides the basis for the above-mentioned further use (Bloch, 2006).

In the context of web services and the use of digital services, it should be noted that a relevant part of additional features is realised via visible or "hidden" (private) APIs that are retrieved by the browser. On the other hand, there are also dedicated public APIs, such as the Google Maps Geocoding API, which can be used to convert address information into geocoordinates (Google, 2022b). This can be understood as an example of an API for modular functionality that can be implemented by third parties in their service without having to replicate the functionality of these components in their own service composition. A data-focused API would be the Twitter API, for example, which can be used to retrieve collected short messages from Twitter on a specific topic. The topic and scope can then be narrowed down using selection criteria (Twitter, 2022). In more complex APIs, the features or data are grouped into "endpoints" to enable targeted and efficient queries.

In commercial APIs, the use of a personalised key (token) for identification and billing is common. This is also done in the context of avoiding uncontrollable overloads. Typically, calls for features or data are understood as a "call"/"hit" that can be billed according to underlying pricing schemes. The economic aspects of APIs and their billing are discussed in Chapter 3.7 in the context of efficient implementation. Extensive documentation is usually provided, especially for commercial offerings. In addition, there are also internet platforms such as Stack Overflow and specific discussion forums that extend official documentation (Stack Overflow, 2022).

### 3.6.2 Standardised data and metadata formats

In the context of digital platforms, the common data formats for structured, sometimes hierarchically organised data are, for example, JSON or XML, and for simple structured data CSV (comma-separated values) or text files. Common formats also exist for image and video files. In contrast to closed-source formats, open file formats are those whose specifications have been published. In the case of proprietary data formats, the specification of the format is sometimes published, but the ownership and thus the rights of use are held by the developer. If proprietary data formats are to be processed within software, licence agreements must be made with the developer. With a published specification, software providers can ensure interchangeability with these formats. However, this only provides syntactic compatibility, but in no way guarantees semantic compatibility. This is why, for example, file models are proposed and implemented within the framework of the Data Transfer Project, some of which are based on publicly available schemata (Data Transfer Project, 2021). These schemas establish semantic compatibility through coordination and provide additional information on the interpretation of the data via metadata. The investigation of Syrmoudis et al. (2021) with regard to the file formats of selected data portability exports shows, however, that while open and machine-readable data represented a large part of the formats, in some cases more difficult-to-process formats such as PDF were also used.

Recommendations for the uniform definition of metadata were summarised in the Resource Description Format (RDF), which was conceived by the W3 consortium and has since become part of a framework for the semantic web. With the format JSON-LD (JSON for linked data), the recommendations of RDF are embedded as a metadata format in the open standard format JSON.

## 3.7 Implementation of interoperability arrangements

### 3.7.1 Design of interoperability regulations

The design of concrete IOP regulations is technically demanding, as these must do justice to the complexity of specific services and their existing implementations. This results in different requirements with regard to horizontal and vertical IOP.

Under horizontal IOP, the requirement profile and existing features of different applications can be relatively easily collected, catalogued and classified according to e.g. frequency of use and distribution. In this way, a relatively clear picture of the relevant and essential core features at a value creation level can be gathered. It is therefore always a matter of an application-specific requirement profile for IOP, which can only be partially or fully standardised.

In the case of vertical IOP, existing (private) APIs, which are already used by vertically integrated services of a platform, for example, are also relatively easy to open for competitors at other levels of the value chain. However, existing APIs were originally developed for specific purposes and can therefore only be used for other application scenarios to a limited extent. These APIs are thus only rarely developed in an application-agnostic way. Since in the platform economy new services are also provided through the composition of existing modules and applications, this limitation restricts the development of new innovative services to the existing range of features. Accordingly, in the case of vertical IOP, in addition to surveying the existing application scenarios (e.g. ancillary services), the potential scenarios and uses for which IOP is to be produced in the future must also be surveyed. Only in this way can the innovation potential of vertical IOP be raised. In this case, IOP defines the scope of possible service compositions for a variety of application scenarios, whereas in the case of horizontal IOP the application scenario (even if not all conceivable future features) is already defined.

### 3.7.2 Design of standardisation processes

Standardisation, or agreement on a standard, is at the core of all IOP efforts. As already explained in Chapter 2.1.3, standardisation is however fraught with various imponderables. Companies often have vested interests in the technologies used, especially in the case of horizontal IOP, the processes are time-consuming and costly, and the formation of alliances can influence the outcome.

Standardisation organisations have already proven their worth as institutions for the creation of standards and are therefore best suited to accompany such a process and to bring about a result acceptable to all parties involved.

However, a number of aspects have to be taken into account. As standardisation is a cost-intensive process, there is a risk that financially strong market players will be able to assert themselves better in such processes than, for example, SMEs. Furthermore, there is the possibility that such processes could weaken the quality and security of existing solutions through compromise solutions. Consumers are usually not involved in such processes and can therefore only indirectly express their wishes.

These concerns need to be addressed through barriers and specifications in the process of producing IOP when designing IOP regulations (cf. also Chapter 3.3.2). Compared to the problems mentioned with classic SSOs, a final decision-making power may be necessary here with the regulator. In addition to the incumbents, other stakeholders such as potential competitors, consumer organisations and independent technological expertise should also be involved (Scott Morton et al., 2021).

# 4 Interoperability for number-independent interpersonal telecommunications services

## 4.1 Classification of NI-ICS

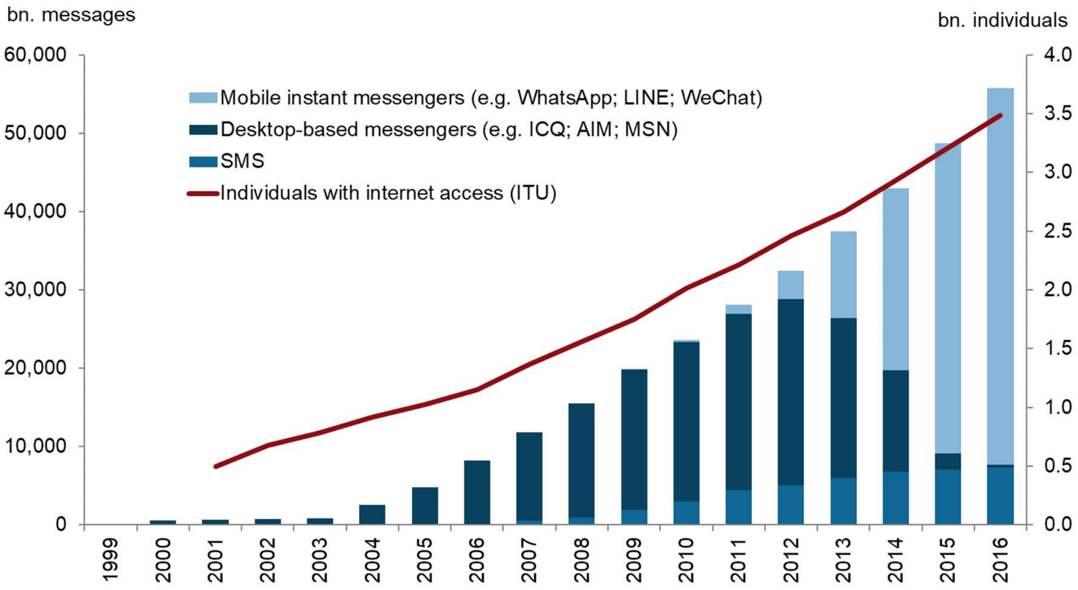
### 4.1.1 Definition

With the **amendment to the TKG** entering into force in December 2021, NI-ICS was included in parts of the regulatory regime, as explained in Chapter 3. 3.1.2. According to the definition of the term, a NI-ICS is "an interpersonal telecommunications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable telecommunication with a number or numbers in national or international numbering plans". The second group of interpersonal communications services, number-based interpersonal communications services (NB-ICS), are distinguished from NI-ICS by the very use of such public numbering resources.

Both types of interpersonal communications services are included for the first time in 2018 in the amended European Electronic Communications Code (EECC) under the definition of electronic communications service (ECS) (Article 2(4) of Directive (EU) 2018/1972). This modification represents an extension of the previously applicable ECS term under Article 2 c) of Directive 2002/21/EC of the European Parliament of 7 March 2002, as now not only OTT-0 services, but to a large extent also OTT-1 services are covered by the ECS definition. The designations OTT-0 and OTT-1 originate from the taxonomy of BEREC (2016) prior to the EECC revision. The taxonomy was used to distinguish electronic communications services under Directive 2002/21/EC from services that enable communication over the (open) internet (over-the-top (OTT) services). In this context, an OTT-0 service referred to an OTT service which was nevertheless able to establish a connection to classic telephone services via call number. An OTT-1 service without this capability, on the other hand, was not considered an ECS, but could potentially compete with it (BEREC, 2016).

Already in the early development stage of the internet, the first communication protocols for interpersonal communication emerged. E-mail is widely used as a standardised and thus fully protocol-interoperable means of communication. In order to be able to interact directly in real time, the IRC protocol (Internet Relay Chat) was created as a way to communicate bilaterally and in groups. The first desktop-based chat clients such as AOL Instant Messenger, ICQ and MSN Messenger were based on this principle. Figure 4-1 shows the strong growth in messages sent via these services, especially between 2004 and 2011. With the spread of smartphones and increasing data volumes in mobile phone contracts, mobile instant messengers have relativised the importance of classic short messages (SMS) and marginalised desktop-based messengers. Starting in 2010, a steady growth of messages sent can be observed, at the expense of the above-mentioned communication services.

Figure 4-1: Number of messages sent annually via SMS and online communication services (worldwide in billions of messages; Individuals with internet access in billion)



Source: Arnold et al. (2017)

If one follows the BEREC definition, products such as Skype with differentiated sub-features can be assigned to different OTT categories. Thus, in addition to the feature of making a video call between two Skype users (OTT-1), it is also possible to call classic telephone connections as a Skype user (OTT-0). Accordingly, according to BEREC (2016) the service providers of OTT-0 services are usually not exclusively ISPs, a distinction that is becoming less relevant in the context of the increasing use of VOIP services. Parallels to the current definition of NI-ICS and NB-ICS in the EECC are noticeable here. Nevertheless, compared to the OTT taxonomy according to the BEREC definition of 2016 (BEREC, 2016), NI-ICS are a subset of, but not necessarily congruent with, OTT-1 services.

Overall, the EECC sets out requirements in several recitals that individual services must meet in order to be generally considered as an interpersonal communications service or to fall specifically into the category of NI-ICS or NB-ICS. At times, NI-ICS and NB-ICS cannot be fully distinguished from each other or from other services that also allow communication.

Both for the definition and the assessment of whether there is vertical competition in a service category in addition to horizontal competition, it is decisive, among other things, whether there are open (mass communication, e.g. social media) or closed (individual communication, e.g. simple messengers) user groups (Taş & Arnold, 2019). However, the boundaries between these two forms are not always clear-cut due to the multifunctional design of many services. Similar to messaging services, social networks offer features that enable the exchange of direct messages between individual users as well as closed user groups.

Even the criteria of an interactive exchange or a response option and the restriction to a finite number of persons (cf. EECC, Directive (EU) 2018/1972) do not always lead to a clear classification. The lack of an unambiguous dichotomy is particularly evident in the example of Telegram, which is also being discussed persistently beyond the topic of the IOP (cf. Jäschke, 2021). Here, among other things, the question arises as to what extent groups with up to 200,000 users can still be described as "closed", but at the same time the service is also used in large parts, analogous to WhatsApp or Signal, for bilateral or private communication in groups. Through Telegram's channel feature, even an unlimited public is accessible, which means that Telegram aims at open user groups and implements social media features. Unlike in classic social networks, however, such channels must be visited proactively and are not accumulated, for example, through a news feed. The definition problem addressed here is also taken up in *recital 14 of the Digital Services Act (DSA).* On the one hand, it is emphasised there that interpersonal communication services within the meaning of Directive (EU) 2018/1972 do not fall under the concept of a platform within the meaning of the DSA. On the other hand, it is clarified that the platform rules of the DSA apply to services that enable information to be made accessible to an indefinite number of recipients, for example through public groups and open channels. In this context, groups are to be considered public if users can be registered automatically without a human being deciding on their admission to the group (Busch, 2022).

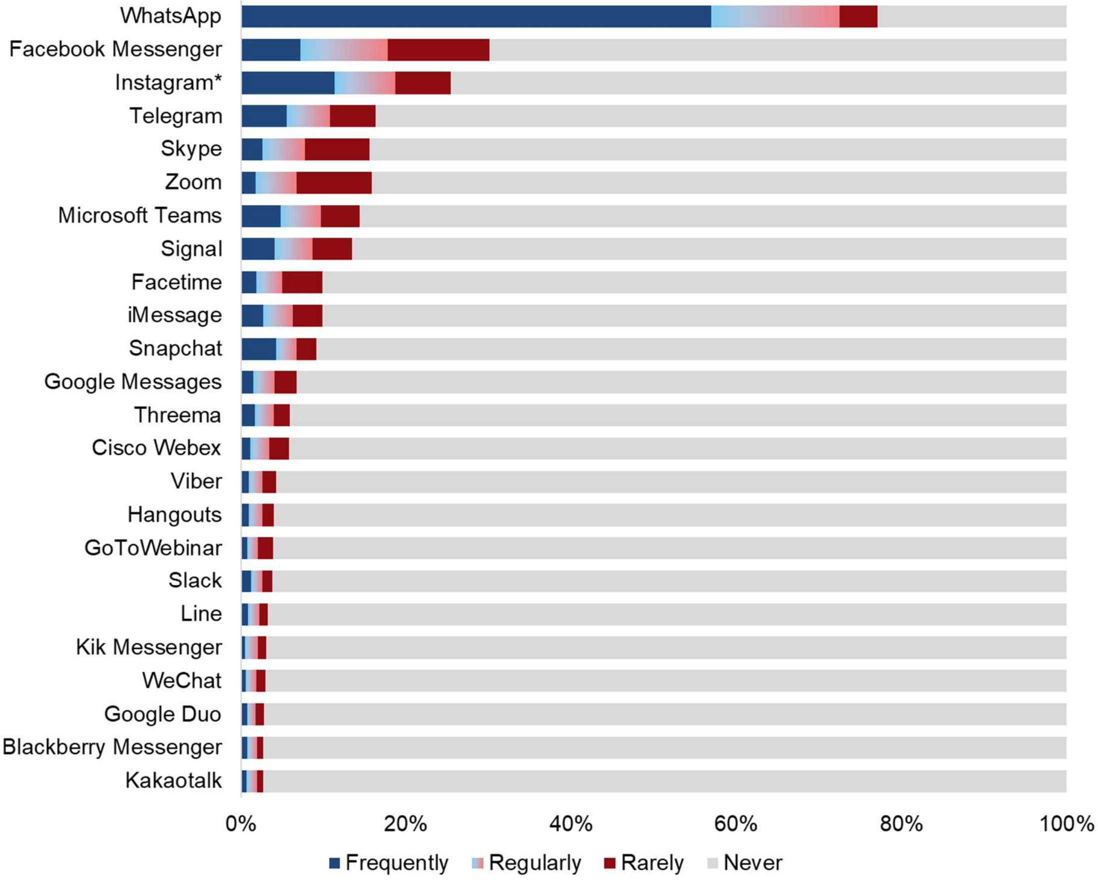
Also excluded from the legal definition, e.g. within the framework of the *EECC (Art. 2, para. 4) or TKG (Section 3 No. 24),* is communication that is only a "minor ancillary feature" and is inseparably linked to another service. Apart from clear cases such as the chat feature of an online game, however, there may also be borderline cases or perspective circumvention possibilities. An assessment of whether, for example, the private messaging feature of the Instagram service is to be regarded as a minor ancillary feature of Instagram as a social network cannot always be determined on the basis of technical criteria and may depend on the dynamic usage habits of customers. The definition is also complicated by the proliferation of services that belong to vertically integrated ecosystems. This aspect will be taken up further in Chapter 4.1.3.5.

Due to this problem, the term "online communication services" is used in the following market overview. Online communication services is a broader term that is intended to summarise communication services generally provided via the internet, regardless of their respective regulatory classification (also cf. Bundesnetzagentur, 2022), of which NI-ICS represent a subset with a more concrete legal definition.

### 4.1.2 Market situation for online communication services

WhatsApp is one of the most popular online communication services in Germany. According to the results of the annual WIK survey on the use of communication services, which was last conducted at the end of 2021, the user share of WhatsApp amounts to 77% of the adult population.[24] WhatsApp's user share is thus far above the shares of other well-known services such as Facebook Messenger and Instagram, which like WhatsApp belong to the Meta group, or Telegram. The WhatsApp service is not only used by most consumers in Germany, but also clearly sets itself apart from other online communication services on the market in terms of frequency of use. Most users use the service almost daily.

Figure 4-2: Use and frequency of use of selected online communication services



Source: WIK-Consult. Special evaluation of the annual WIK survey. 2021: N=3,178. German Population aged 18+. Frequently: At least once a day; Regularly: 2-6 times a week; Rarely: Max. once a week. *Related to direct messages sent or received (direct messages).

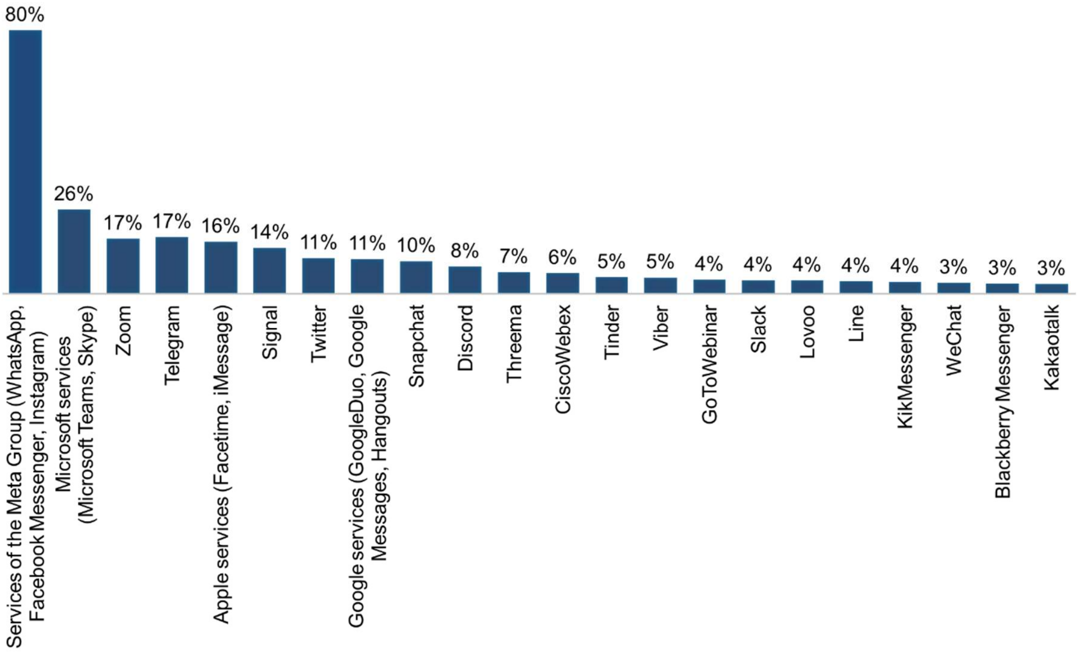
[24] Users are those respondents who stated that they had contacted another person via the service or had been contacted by another person.

In principle, however, consumers do not limit themselves to a single service, but tend to use several services.

The data from the annual WIK survey on the use of 24 selected online communication services show that about 83% of the respondents use at least one of the 24 online communication services considered.[25] Either the users are contacted via the respective services or they contact other people. A total of 75% of these users reported using at least two services and are thus classified as multi-homers. On average, users from the 24 online communication services considered use about 3.7 different services. Users in the age group 18-24 use on average about 6 services, while users older than 55 use on average only about 2 services.

Three of the services considered belong to the Meta group, namely WhatsApp, Facebook Messenger and Instagram, and are the three most frequently used services in Germany. Around **80%** of respondents in Germany in the WIK survey in 2021 stated that they use at least one of the Meta group services. This contrasts with 52% who say they use at least one of the remaining 21 online communication services (see Figure 4-3).

Figure 4-3: Use of selected online communication services - by company



Source: WIK-Consult. Special evaluation of the annual WIK survey. 2021: N=3,178. German population aged 18+. Selected online communication services: Snapchat, Threema, Signal, Telegram, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Slack, Zoom, GoToWebinar, Cisco Webex

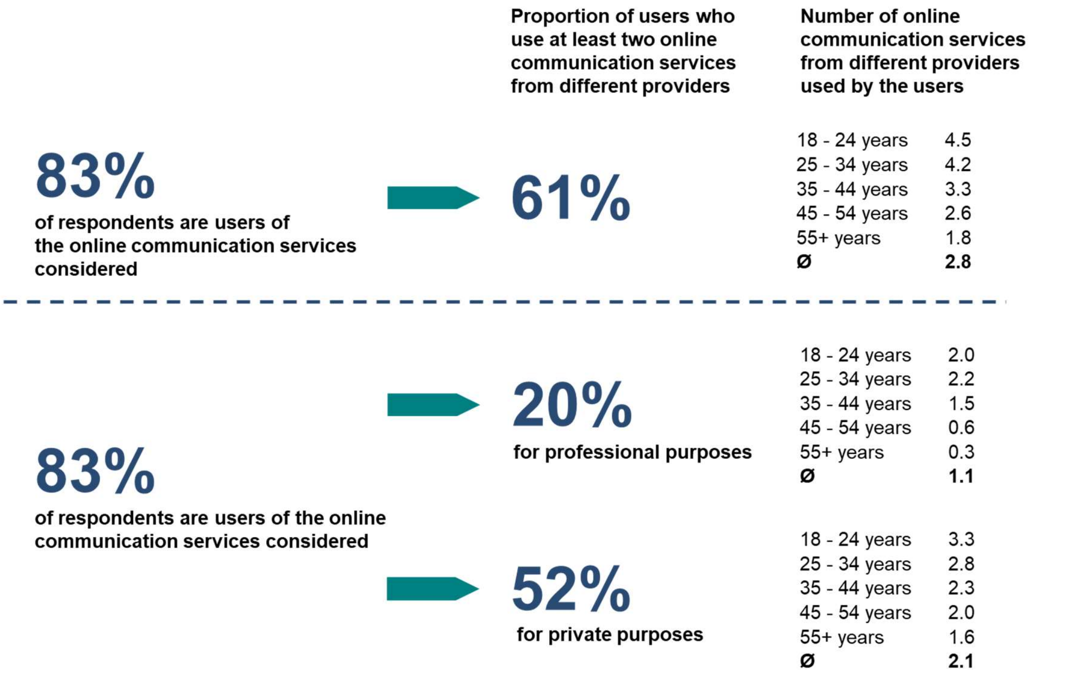
[25] Selected online communication services: WhatsApp, Facebook Messenger, iMessage, Hangouts, Instagram, Snapchat, Threema, Signal, Telegram, Skype, Facetime, GoogleDuo, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Google Messages, Slack, Microsoft Teams, Zoom, GoToWebinar, Cisco Webex.

as well as services from Microsoft (Microsoft Teams, Skype), services from Apple (Facetime, iMessage), services from Google (GoogleDuo, Google Messages, Hangouts) and services from the Meta group (WhatsApp, Facebook Messenger, Instagram), which are each evaluated as one unit for the evaluation.

Figure 4-4 shows the extent of competition-relevant multi-homing. For this purpose, the 24 selected online communication services, are summarised as one unit when belonging to the same company. Compared to the above, the share of multi-homers is **14 percentage points** lower in this evaluation. The number of services used on average is also reduced by one.

The multi-homing seems to be at least partly due to the distinction between professional and private use of online communication services. The figure below shows that one of the three online communication services used on average is likely to be used for professional communication and two for private communication.

Figure 4-4: Multi-homing of selected online communication services - Total and by purpose of use



**Proportion of users who use at least two online communication services from different providers**

**Number of online communication services from different providers used by the users**

**83%** **of respondents are users of the online communication services considered** → **61%**

| | |
|---|---|
| 18 - 24 years | 4.5 |
| 25 - 34 years | 4.2 |
| 35 - 44 years | 3.3 |
| 45 - 54 years | 2.6 |
| 55+ years | 1.8 |
| **Ø** | **2.8** |

**83%** **of respondents are users of the online communication services considered**

→ **20%** **for professional purposes**

| | |
|---|---|
| 18 - 24 years | 2.0 |
| 25 - 34 years | 2.2 |
| 35 - 44 years | 1.5 |
| 45 - 54 years | 0.6 |
| 55+ years | 0.3 |
| **Ø** | **1.1** |

→ **52%** **for private purposes**

| | |
|---|---|
| 18 - 24 years | 3.3 |
| 25 - 34 years | 2.8 |
| 35 - 44 years | 2.3 |
| 45 - 54 years | 2.0 |
| 55+ years | 1.6 |
| **Ø** | **2.1** |

Source: WIK-Consult. Special evaluation of the annual WIK survey. 2021: N=3,178. German population aged 18+. Selected online communication services: Snapchat, Threema, Signal, Telegram, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Slack, Zoom, GoToWebinar, Cisco Webex as well as services from Microsoft (Microsoft Teams, Skype), services from Apple (Facetime, iMessage), services from Google (GoogleDuo, Google Messages, Hangouts) and services from the Meta group (WhatsApp, Facebook Messenger, Instagram), which are are each evaluated as one unit for the evaluation.

However, consumers do not only use online communication services. In a survey conducted by WIK in 2020, about 91% of respondents said they still use landline and/or mobile telephony. However, compared to WhatsApp or the other services of the Meta group, fixed-line and mobile telephony are used less frequently. While 68% of WhatsApp users said they use the service several times a day, this share is only just under 30% for landline and mobile telephony. Classic short messages (SMS), on the other hand, are used even less frequently, although 63% of respondents are still users of this service. The latter indicates that the classic short message has developed into a fall-back channel (Taş et al., 2021).[26]

**Multi-homing in Germany**[27]

- Services of the Meta group are among the most used online communication services in Germany. Around **80% of consumers in Germany aged 18 and over communicate via WhatsApp, Facebook Messenger or Instagram** with their contacts**.** Services from other companies each have a user share of partly far less than 30%.
- Multi-homing at service level: About 75% of users of online communication services use two or more different services. On average, consumers use about 3.7 different online communication services.
- Multi-homing at company level: The proportion of users of online communication services who use at least two online communication services from different companies is 61%. On average, consumers use 2.8 services from different companies.

## 4.1.3 Economic characteristics

### 4.1.3.1 Network effects

Especially in the case of (non-interoperable) services, the behaviour of end users influences market concentration via network effects. In the area of messaging services, the direct network effects are of particular importance (cf. inter alia ACCC, 2020). The more users use a particular messaging service, the more attractive it tends to be for new users to join it.

[26] Individual results also come from a special evaluation of the annual WIK survey from 2020.

[27] Based on an annual survey by WIK. 2021: N=3,178. German population aged 18+. Selected online communication services: Snapchat, Threema, Signal, Telegram, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Slack, Zoom, GoToWebinar, Cisco Webex as well as services from Microsoft (Microsoft Teams, Skype), services from Apple (Facetime, iMessage), services from Google (GoogleDuo, Google Messages, Hangouts) and services from the Meta group (WhatsApp, Facebook Messenger, Instagram). Without e-mail.

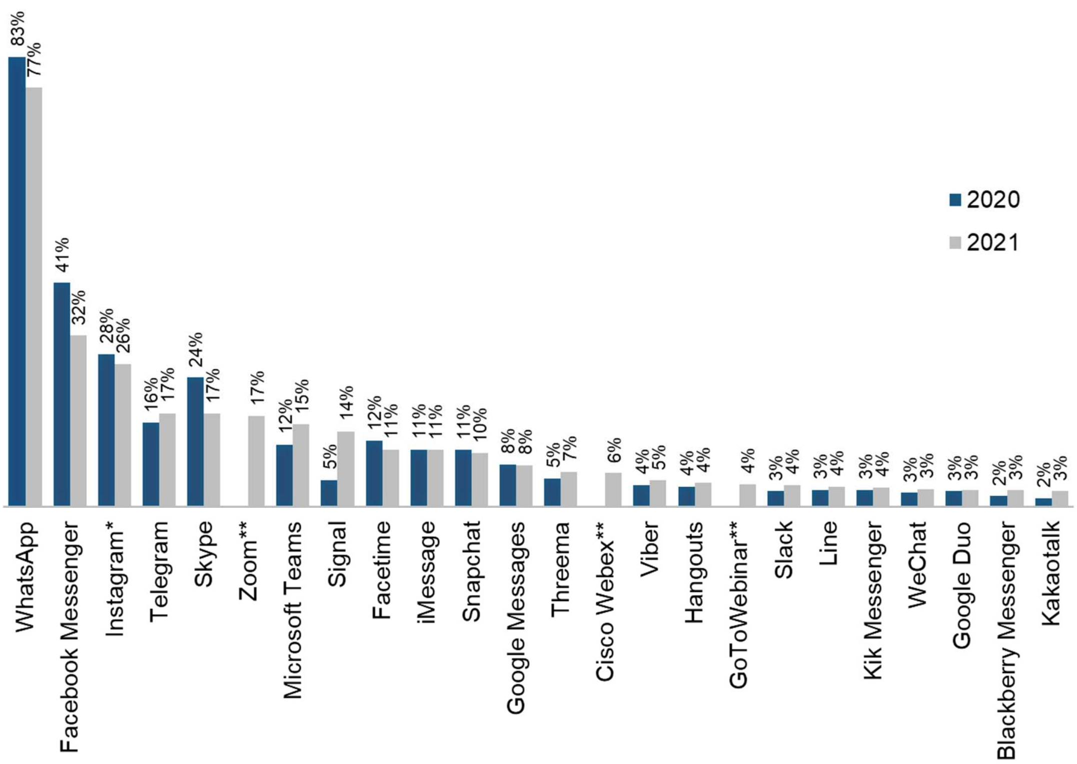
Compared to classic examples of network goods, where the benefit tends to depend on and increase with the pure absolute number of other users, the network effects in the area of messaging services often appear more heterogeneous and specific. Personal contacts and existing "networks" in the sociological sense play a stronger role here. This means that the installation or use of a particular service tends to be shaped more by the use of very specific people from the family or close circle of friends and not by the total number of other users. In the literature, this is sometimes referred to as **"identity-based network effects"**, see e.g. Colangelo & Maggiolino (2018). This is also a crucial difference to "social networks" in the current sense of "social media", which is comparable to the distinction between closed and open user groups. For the use of digital services with closed user groups such as WhatsApp, the presence of certain persons/contacts is more decisive (ACCC, 2020), whereas for open user groups the presence of an absolute number of people also plays a greater role.

In principle, the individual importance of certain contacts can also facilitate switching to other services. In case of doubt, even the switching of a single user "U" from provider "A" to provider "B" can directly lead to the contacts of user "U" also switching to provider "B" in order to continue to be able to reach him. In the case of identity-agnostic network effects or higher switching costs, on the other hand, a critical mass is classically necessary to make adaptation or switching worthwhile for further users (cf. Rohlfs, 1974). Nevertheless, in both cases a problem of collective action remains, as will be discussed further in the following Chapter.

#### 4.1.3.2 Multi-homing and switching costs

Recent developments related to WhatsApp show that consumers may be willing to use alternative services. According to media reports, with the implementation of new privacy policies and terms of use on the part of WhatsApp, millions of users installed alternative services such as Telegram, Signal or Threema at the beginning of 2021 (Taş et al., 2021). The data of the annual WIK survey also show an increase in the use of these services (see Figure 4-5) as does the consumer survey of the Bundesnetzagentur (2022) which also shows strong growth in Discord and the video conferencing services Zoom and Microsoft Teams. The share of WhatsApp users declined slightly compared to 2020.

Figure 4-5: User shares of selected online communication services



Source: WIK-Consult. Special evaluation of the annual WIK survey. 2020: N=3,090. 2021: N=3,178. German population aged 18+. *referred to direct messages sent or received (direct messages). **No reference values available for 2020.

**Switching & Multi-Homing Case Study: Change in WhatsApp Privacy Policy**

Despite an increased (parallel) use of alternative services and expressed willingness to switch, only a very small proportion of users (0.5%) actually left the WhatsApp service in the end. Griggio et al. (2022) empirically investigated specifically the willingness and activities of WhatsApp users to switch after the change in data protection conditions.

Griggio et al. (2022) conducted two surveys 2 months apart. In February and May, 1525 WhatsApp users in Mexico, Spain, South Africa and the UK were asked about their plans to switch services. About 25% of respondents said they planned to move at least some of their communications from WhatsApp to other apps. However, less than a quarter of users felt they were at least somewhat successful in their plan, and almost half were dissatisfied with their current situation. By May, 27% had increased their use of other apps and only 16% were using WhatsApp less. One of the reasons respondents continued to stick with WhatsApp was that not enough of their contacts had switched to the alternative services. Apart from the network effects, users found it difficult to make an informed choice between alternative apps, which sometimes differed in privacy policies, design and their features. These differences also create costs as users have to deal with the policies, get used to the new interface and possibly adapt to the different ways of communicating. Lastly, for some respondents, switching also entails the loss of control over the separation of contacts across different services. Overall, only about 0.5% of respondents did actually uninstall WhatsApp. Griggio et al. (2022) conclude that it is easy for consumers to install and use additional services, but that it is less easy for them to actually leave a service completely.

Another possible reason for this is the prevalence of group chats, e.g. within school classes or sports groups and other clubs. Here, the classic **"collective action" problem** also plays an important role when switching between networks. Since in this case not only individual conversational partners, but entire groups would have to be directly convinced to switch, this can be considered a form of **"collective switching costs"** (cf. Shapiro & Varian, 1998a). However, previous research on the use of communication services has shown that most consumers use several services for different reasons. These range from access to different features, to convenience, to the ability to reach different social groups. This suggests that horizontal IOP is not necessary from this perspective. The recent WIK research confirms this and shows that the use of multiple communication services is stimulated by product differentiation, innovation as well as a heterogeneous set of contacts (Taş et al., 2021). The study further finds that the number of communication services used increases with the number of social groups with which consumers interact privately.

In communication sciences, several approaches exist that explain the choice as well as the use of multiple communication channels. In the Channel Complementarity Theory according to Dutta-Bergman (2004) for example, they postulate that individuals who choose communication channels to satisfy a particular interpersonal or instrumental need will also use other channels to satisfy the same needs (Dutta-Bergman, 2004; Ruppel et al., 2017). Communication channels are thus mostly used in a complementary way.

The type of relationship with communication partners therefore also has an influence on the use of communication channels. Arnold & Schneider (2017) investigated the choice of communication services using semi-structured interviews with users. Participants associated different communication services with specific social contact groups. For example, some participants emphasised that WhatsApp and Snapchat are rather reserved for close contacts; Facebook and / or Facebook Messenger, on the other hand, are more often used to communicate with acquaintances with whom the participants do not have a close relationship. Arnold et al. (2020) confirmed these findings in an extensive empirical study comparing a total of 22 online communication services, traditional ECS and email as communication channels. They found that individuals proactively use the boundaries between communication services to divide their social contacts according to how close the respective relationship is.

In the social media context, Tandoc et al. (2019) also illustrate that social media users use multiple platforms for the purpose of relationship management and switch back and forth between them. Switching between platforms allows users to segment and socially demarcate their networks. This can also facilitate the handling of contacts, messages and corresponding notifications. Along with this or as an alternative, services and channels can also be used for thematic segmentation, e.g. according to work, school, sports or other hobbies.

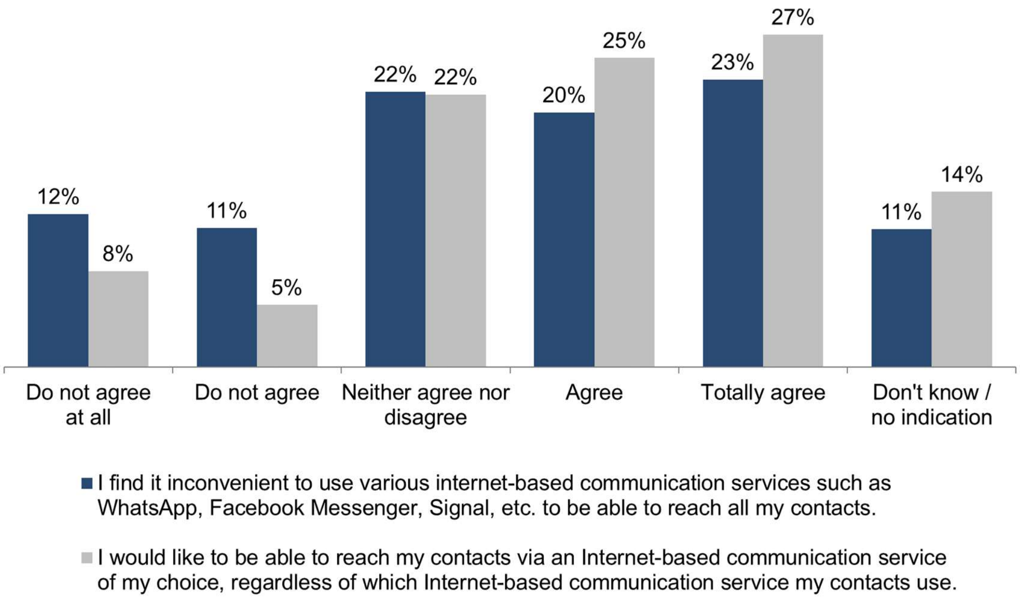
Quan-Haase & Collins (2008) and Nouwens et al. (2017) describe, on the one hand, consumers' desire to control who they are contacted by and through which service, and, on the other hand, the effort they put into maintaining control over this. Quan-Haase & Collins (2008) conducted interviews and focus groups with students in Canada on the topic of online presence and social availability in instant messaging. Some participants described that undifferentiated and long contact lists can be problematic if the person does not want to be available to every contact to the same extent via instant messaging. A few of the participants solved the problem by creating new lists with selected contacts. Others blocked or deleted contacts with whom they did not want to interact via the service. Nouwens et al. (2017) also illustrate that consumers control and monitor their contacts for communication services and that individual consumers feel uncomfortable when contacts contact them through a communication channel that they do not associate with them. In view of a potential IOP for communication services, participants in the study of Arnold & Schneider (2017) expressed the concern of being deprived of their privacy. Participants reported fearing that even contacts with whom only a casual relationship is maintained might suddenly invade areas reserved for closer relationships.

It can be generally concluded that the degree of multi-homing in the market thus strongly depends on how users distinguish social groups from each other and which services they prefer for communicating with the individual groups. The more different the attitudes and preferences of communication partners, the higher the number of communication services that tend to be used.

Another reason for multi-homing can be access to different features. Although most online communication services and traditional ECS ensure the same basic features, individual services also provide some niche features that are quite attractive to consumers. Taş et al. (2021) show that respondents who use at least two services, and thus multi-home, value access to a large number of different features and different forms of communication, as well as a choice of images, skins and emoticons, more than consumers who use only one communication service.

Because the use of online communication services is rarely associated with monetary costs, the hurdle for consumers to use one or more of these services is also particularly low. Nevertheless, multi-homing is associated with costs. These arise primarily from the management of different services. According to the results of the annual WIK survey on the use of communication services, which was last conducted at the end of 2021, many respondents find it cumbersome to use multiple internet-based communication services to reach their contacts (see Figure 4-6). This is also accompanied by the fact that respondents would tend to prefer to be able to contact their contacts via an internet-based communication service of their choice, regardless of which service their contacts use. If the categorisation of social groups and the preferences for the services used differ greatly per group in the circle of contacts, this may well complicate the use of internet-based communication services. Overall, 43% think that using multiple online communication services is cumbersome, while about 52% would welcome IOP, at least if they are the contacting person.

Figure 4-6: Attitude towards multi-homing

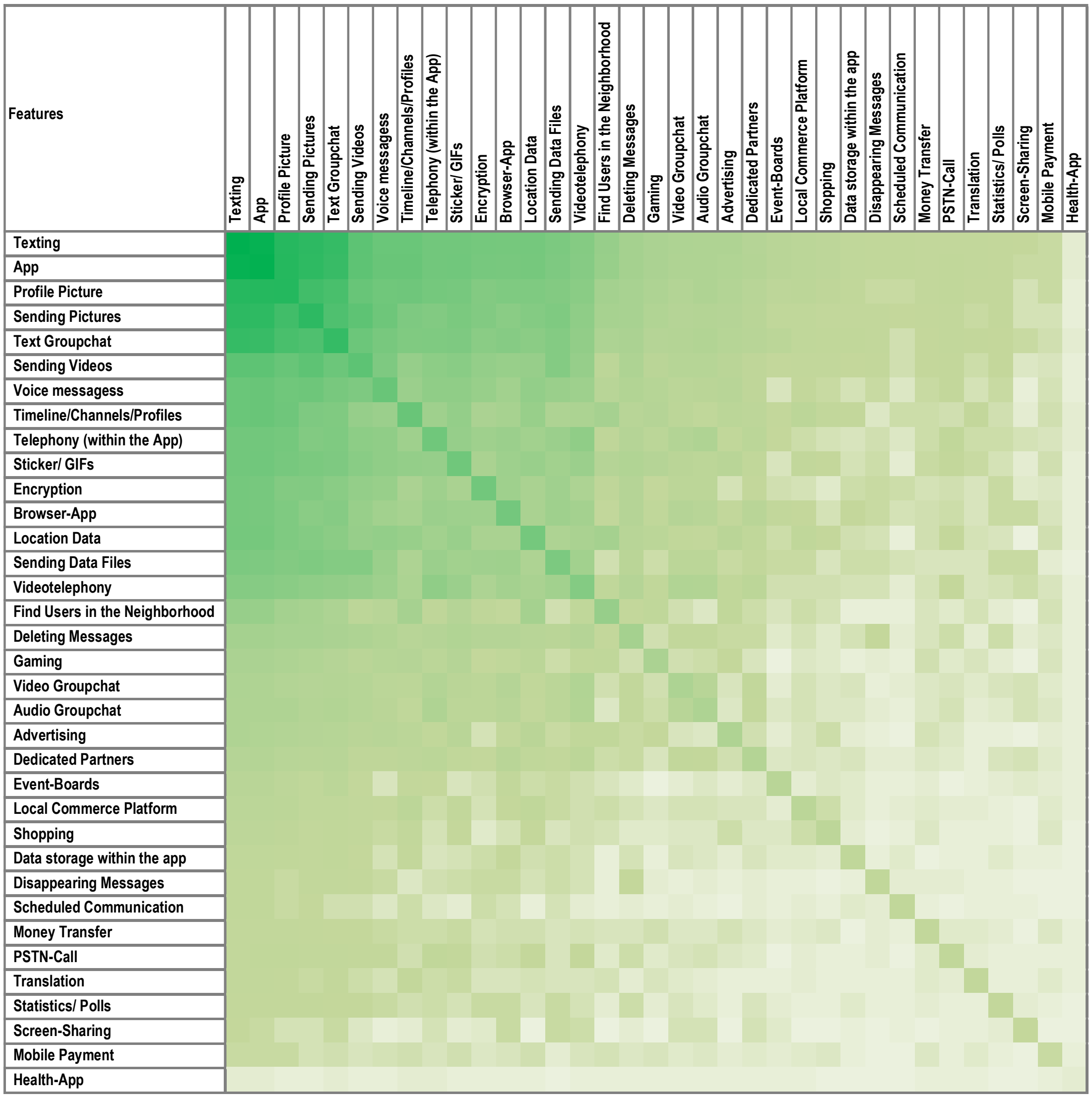


Source: WIK-Consult. Special evaluation of the annual WIK survey. 2021: N=3,178. German population aged 18+. Basis: users of selected online communication services.

#### 4.1.3.3 Overview of features incl. current development

Online communication services allow for diverse and rich communication, not least due to the multitude of different features that these services provide. In recent years, individual services have introduced a broad repertoire of different features. Overall, online communication services seem to be developing more and more into comprehensive platforms (Taş & Arnold, 2019). By 2020, services such as WeChat, Facebook Messenger and KakaoTalk already had well over 20 different features. WIK examined 180 internet-based communication services worldwide in 2020. Figure 4-7 shows the distribution of the 35 features identified across the online communication services considered. Nearly all services at this time allowed text messaging (98%). Features that allow audio-visual communication were also widespread. Almost 77% of the services allowed sending pictures; 54% allowed sending videos. Telephony or video telephony was enabled by about 46% and 36% of the services, respectively. In addition to these primary communication features, other features were also enabled by some services. About 13% of the services entered into partnerships with other platforms; for example, it was possible to book ride or car sharing services via individual online communication services. Again, 5-7% of the services allowed making payments or transferring money. 6-7% of the services considered integrated the feature of screen-sharing or the sending of self-deleting messages into their offer. On average, internet-based communication services had about 10 features in 2020. In 2016, WIK-Consult had recorded an average of only 8 features in a comparable survey (Arnold et al., 2017). The rising trend seems to be continuing, as shown for example by new response and business features of WhatsApp (WhatsApp, 2022), a stronger integration of the messaging feature on Instagram (Instagram, 2022) or by the efforts of Apple and Meta in private payment transactions.

Figure 4-7: Features of internet-based communication services worldwide



Reading aid: The shading gives an indication of the proportion of the 180 internet-based communication services considered that each provide a combination of the features listed horizontally and vertically. The darker the area, the higher the share of the specific combination of features. The diagonal indicates how often the respective individual feature is offered in our database of internet-based communication services.

Source: Own illustration; data come from an ongoing monitoring of the market for internet-based communication services (as of 2020).

As just described, text messages and features that enable direct communication are part of the standard repertoire of internet-based communication services. Among consumers, sending picture and voice messages are also particularly popular. According to a survey that Taş & Arnold (2019) published, about 60-72% of consumers in Germany use each of these features.

Table 4-1: Proportions of use of different features

| Features - Total | |
|---|---|
| Photo messages | 72,1% |
| Voice messages | 60,8% |
| Receipt and read confirmation | 59,2% |
| Profile picture | 58,4% |
| Group chat | 48,7% |
| Voice and/or video telephony | 42,4% |
| Status, Stories, Day, Mood, Moments etc. | 40,5% |
| "Last seen/online" feature | 38,4% |
| Video messages | 35,4% |

Source: Taş & Arnold (2019), S. 38.

#### 4.1.3.4 Business models

Not least due to different underlying company structures, various messaging services differ greatly in their monetisation or business models (Bundeskartellamt, 2021). Some services or the corresponding apps are sold for direct one-off or regular payments (Threema, Element), while the use of many other services is primarily free of charge. Here again, there are fundamental differences; the Signal system, for example, is financed through a foundation- and donation-based model, while for other services various secondary direct or indirect revenues are to be generated or are planned. Not only in terms of legal definitions (cf. Chapter 4.1.1), which aim at service provision "*normally provided for renumeration*", the handling of other forms of financing often remains unclear. As a rule, however, the inclusion of services with forms of indirect revenue seems necessary, e.g. through "payment" with consumers' own data or through synergies or cross-subsidisation with other in-house services or hardware (cf. also Chapter 4.1.3.5).

Meta is currently expanding its offer of a business API for communication between companies and end users, among other things (WhatsApp, 2022). This is also possible via Telegram, but has so far taken place without a commission for Telegram, just like the payment feature that is made possible between users and companies. In addition, it is now possible to place advertisements in public channels on Telegram (Telegram, 2022). In addition, according to a freemium model, which is also pursued by Twitch or Discord, i.e. features that go beyond the free basic offer are offered for purchase (Clover, 2022).

In the assessment of competitive constellations and the evaluation of possible regulatory measures, individual services should neither be overlooked due to their (possibly seemingly missing) monetisation strategy, but on the other hand, possible special aspects and risks of each business model must always be taken into consideration. In particular, advertising models based on user attention and/or data bring about an increased level of complexity. Through the business side of the advertisers, an additional party comes into play, which at the latest then creates a platform in the classic economic sense and leads to interactions or indirect network effects vis-à-vis the user side. In addition, various cognitive distortions are known from the literature, e.g. in the context of data sharing

(Kokolakis, 2017) or the "zero-price" effect (Shampanier et al., 2007) which can lead to increased vulnerability on the user side. Secondary misguided incentives can also occur at the societal level, e.g. if polarisation and disinformation lead to increased attention (and thus possibly advertising revenues) (Marsden et al., 2020).

#### 4.1.3.5 Ecosystems & vertical integration

Furthermore, although individual services can be primarily assigned to a service category (here: messengers), they often only represent one value creation stage in a wider vertically integrated ecosystem. Figure 4-8 illustrates this case. The coloured cells show the value creation stages in which the respective companies are active. In the case of messaging services, for example, services that are primarily represented at the same level of value creation (companies B & C, e.g. Threema, Signal) also compete with messaging services that are part of a vertically integrated value creation (company A, e.g. WeChat).

Figure 4-8: Horizontal IOP (level 3) with a vertically integrated platform (company A)

| | Company A | Company B | Company C |
|---|---|---|---|
| Level 3 | ■ | ■ | ■ |
| Level 2 | ▒ | | |
| Level 1 | ▒ | | |

Especially in cases where individual market participants, who are in horizontal competition at one stage of the value chain, have further vertical interdependencies, complex interdependencies can arise and thus, in addition to the pure network size, also other levers for exercising market power. For firms in these cases there is the possibility to stabilise collusion beyond the boundaries of individual segments or markets and to strategically choose their own level of IOP depending on the frequency of contact with other firms (Choi & Gerlach, 2013). An example of this is illustrated in Figure 4-9. In the case of messengers, several services from vertically integrated providers (e.g. iMessage, Facebook Messenger) also compete with each other. The providers of these services therefore also have contact with their competitors in other parts of the value chain and in other markets.

Figure 4-9: Horizontal IOP (level 3) with multi-market contact (level 2) of companies A and B

| | Company A | Company B | Company C |
|---|---|---|---|
| Level 3 | ■ | ■ | ■ |
| Level 2 | ▒ | ▒ | |
| Level 1 | | ▒ | |

Particularly in the case of the most widespread messaging services, the frequent lack of direct monetisation (cf. Chapter 4.1.3.4) is due to the multi-product ecosystems behind them. In the German and English-speaking countries, the Meta group with its messaging services and features WhatsApp, Facebook Messenger and Instagram as well as iMessage from Apple are in the foreground. Meta, for example, was accused of linking WhatsApp data with the corresponding Facebook and Instagram accounts (cf. Bundeskartellamt, 2019) in order to be able to increase the advertising revenue generated there. Another example of cross-subsidisation is iMessage, which is firmly anchored within Apple's operating system. In the American market in particular, in addition to simple and integrated handling across the operating system, the exclusive character of the company's own messaging service is also actively promoted for the decision to buy iPhone hardware (Higgins, 2022).

Even if a messaging service does not fulfil the classic definition of a platform in the economic sense by being limited to direct/one-sided network effects, in practice this market is characterised by "real" platforms, as various forms of indirect network effects can also play an essential role through being embedded in platform ecosystems.

The movement towards the prevalence of ecosystem messengers is taking place from both directions, especially internationally: original single-purpose messengers are themselves becoming platforms and/or ecosystems through the addition of features, types of monetisation and company orientations, while existing multi-sector ecosystems are expanding their portfolios to include messaging features (RTR, 2020).

### 4.1.4 Status quo & positions on interoperability

According to Julia Weiss, spokesperson for Threema, there is a concern that IOP would cement the position of dominant providers instead of creating market contestability: "If existing users of free messenger A with bad privacy practices could communicate with users of privacy-conscious paid messenger B, they will not pay money for messenger B, effectively depriving it of its only source of revenue" (Meaker, 2022). Signal, too, has recently publicly rejected cooperation or IOP with other apps such as WhatsApp and iMessage, pointing to a possible threat to existing data protection standards, among other things through the resulting possibility of accessing metadata (Reuter, 2022). In the past, Signal has already publicly spoken out against federated systems and in favour of closed, proprietary protocols (cf. Marlinspike, 2016a).

A number of positions are summarised in anonymised form in the report of the Bundeskartellamt (2021). In general, IOP is recognised as a fundamentally desirable goal and reference is also made to own efforts, be it the joint development of standards (e.g. MLS - Messaging Layer Security) or at least internal efforts to establish IOP between in-house services (cf. also the linking of the various group-owned messaging services announced by Meta). However, a broad IOP obligation up to a standardisation is largely viewed critically. The risks and challenges mentioned include possible negative effects on differentiation opportunities and innovation (cf. also Chapter 3.3), burdens for smaller market participants if they were obliged to sector-wide obligations, as well as technical feasibility. Effective broad IOP would only be possible through comprehensive standardisation, which in turn would bring its own set of problems and would be extremely costly. Some aspects of technical feasibility and standardisation are further discussed in Chapters 4.2 and 4.3.1.1.

According to a market consultation in the UK, market participants are quite positive about IOP and data obligations in particular as part of so-called pro-competitive instruments (HM Government, 2022). However, there is no further breakdown of the different types and levels of such requirements.

Within the industry, however, the overall picture regarding mandatory IOP provisions in the messenger sector is mixed. In particular, many market participants and observers are critical especially of a broad IOP regulation at the horizontal level (see e.g. Barczentewicz, 2022; Bundeskartellamt, 2021). On the other hand, there are also a number of voices that see targeted IOP obligations, not least for messaging services, as a potentially important instrument for the benefit of market contestability and consumer choice. These voices include researchers (Crémer et al., 2019; Scott Morton & Kades, 2021) as well as current alternative providers such as Element and Beeper, which are already pursuing an interoperable approach to messaging services based on the Matrix protocol (Element (2022b), cf. also Chapter 4.2.1 ff.), as well as consumer organisations (Doctorow, 2019; EDRi, 2018) and also market regulators (ACCC, 2020; CMA, 2020).

## 4.2 Basic technical features of messaging services

As the previously presented positions also show, there is a particular focus on technical and data security aspects. In this context, it is often questioned whether the technical requirements for an efficient exchange of features and data in the sense of an IOP for messaging services are achievable at all. The technical complexity of messengers and in particular of end-to-end encryption, which many sides are striving for, therefore seem to be developing into a neuralgic point for the assessment and practical development of IOP requirements such as those found in the DMA. Technical requirements for efficient feature and data exchange and the data needed for a technically feasible and efficient IOP implementation are mutually dependent.

There are currently a large number of different messaging protocols and standardisation attempts on the market, but none of them has been able to establish itself uniformly over the years.

**Rich Communication Services (RCS)** is a communication protocol between network operators and smartphones that was intended to replace standard SMS services for sending and receiving messages, not least as a fallback option for online communication services. Originally implemented by network operators as a reaction to the emergence of OTT messengers in separate applications linked to mobile phone numbers and contracts, it was discontinued by most network operators after unsuccessful attempts and has now been integrated by Google as a network operator-independent service in the Android messaging app (Bohn, 2019; Oestreich, 2018). In addition to the transmission of messages via a data network, RCS also offers multimedia support, a "typing indicator" and group chat features. Currently, Google uses an RCS implementation for its own and Android-native messaging apps, and most recently publicly called on Apple to implement RCS support for iMessage. Despite unilateral efforts by Google to implement end-to-end encryption with RCS for its Google Client based on the Signal protocol (Google, 2022a) [28], RCS is considered inferior to other possible standards and implementations (CMA, 2021). The Signal protocol, as a possible gold standard for encryption, provides the basis for a number of implementations and is discussed in more detail in Chapter 4.2.4. The two free protocols Matrix and XMPP represent examples of federated systems, which are explained in the following Chapter.

### 4.2.1 Architecture types

Messaging services can first be differentiated in terms of their structure into centralised and decentralised architectures[29], the latter in turn into federated systems and peer-to-peer systems.

**Centralised** services are services whose functionality is provided exclusively by one provider. Thus, communication via centralised services always takes place via this intermediary. Messaging services that have a centralised architecture, such as WhatsApp, Facebook Messenger, Telegram and Signal, represent the most widely used messengers. Federated systems, on the other hand, in this case in the form of **decentralised** messengers, offer the possibility of using a similar service via several providers without foregoing the direct network effects. As a messenger protocol, Matrix follows the approach of a communication way distributed over several providers. Federated systems are based on a standardised protocol and can be compared to classic telecommunication services, where each customer is assigned to a provider through which he can reach other users as an intermediary. This applies to both telephone calls and short messages and requires a unique telephone number for identification in order to be processed smoothly. E-mail as a communication channel is also federated via the e-mail providers and also offers unique identification via the provider ID. This is where DeltaChat comes in, a messaging service that is based on the existing e-mail infrastructure and thereby enables messaging. Since this service is realised via the IMAP e-mail protocol, it does not require a separate infrastructure. However, since IMAP as a protocol was designed for asynchronous communication, there are, according to Grüner (2019), problems with regard to the spam

[28] No end-to-end encryption is possible or provided for in the standard implementation of RCS, as it is considered a network operator service and thus subject to "lawful interception" requirements (Amnesty International, 2018).

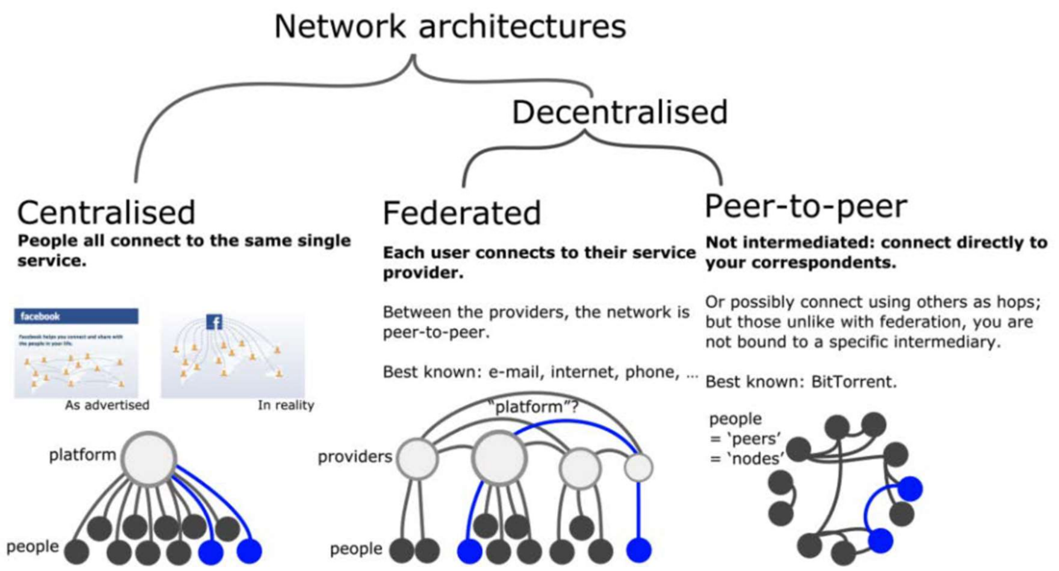
[29] The form of the architecture is to be considered independent of infrastructures, so modern digital services are provided decentrally in the sense of load distribution or geographical differentiation, but are centralised to one service operator with regard to the provision of the services.

restrictions of some providers in the case of clustered messages within short periods of time.

A decentralised messenger without infrastructure supplied by the provider is realised as a peer-to-peer network. While this method became known in particular through file-sharing networks such as BitTorrent, special difficulties exist in the use case of messaging services due to the temporal asynchrony of communication. Inasmuch as one of the parties to the conversation cannot receive the message immediately, there is no infrastructure for temporary storage in decentralised P2P networks (peer-to-peer connection). Briar is such a P2P messenger and relies on a self-hosted mailbox structure to solve this problem (Briar, 2021). This concept shows similarities to self-hosted e-mail applications, since in this case, too, client-side synchronisation with a permanently running server is necessary. Thus, the user must provide his or her own infrastructure if this functionality is to be used.

In Figure 4-10, the decreasing dependence of users on intermediaries is visualised, generalised to digital services, from centralised to federated systems to the departure from intermediaries in the form of P2P networks. While centralised services concentrate all users on one intermediary, federated systems have a two-tier structure. In addition to the interaction with one's own intermediary, a network of intermediaries is created at the level of the intermediaries. This creates a "network of networks", which, however, makes interoperable services via standards or converters necessary**.**

Figure 4-10: Architecture types of digital networks


Network architectures
Decentralised
Centralised
People all connect to the same single service.
facebook
As advertised
In reality
platform
people
Federated
Each user connects to their service provider.
Between the providers, the network is peer-to-peer.
Best known: e-mail, internet, phone, …
"platform"?
providers
people
Peer-to-peer
Not intermediated: connect directly to your correspondents.
Or possibly connect using others as hops; but those unlike with federation, you are not bound to a specific intermediary.
Best known: BitTorrent.
people
= 'peers'
= 'nodes'

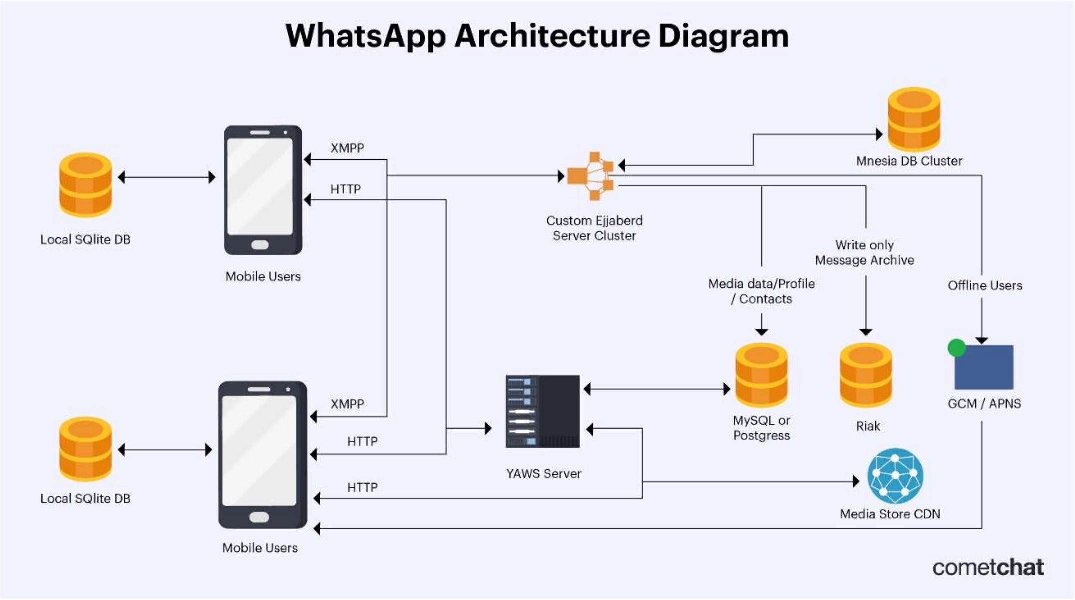
Source: Brown (2020, p. 8)

In addition to the type of architecture, the established messenger solutions also differ in their design, which is why the structure of WhatsApp, Signal, Matrix and Briar will be presented here as examples.

#### 4.2.1.1 WhatsApp

WhatsApp was developed as a messenger in 2009 and has been part of the Meta ecosystem since its acquisition in 2014. On the server side, WhatsApp is based on the Erlang programming language and used FreeBSD as its operating system. WhatsApp uses adapted versions of FunXMPP and ejabberd as a text communication protocol and respectively for server operation. It should be noted that FreeBSD as well as ejabberd and FunXMPP are fundamentally open source, FunXMPP is even an iteration of a standardised communication protocol. However, changes made by WhatsApp for performance reasons and presumably also strategic considerations have made them proprietary and thus no longer reproducible without adversarial reverse engineering. This unilateral adaptation, from which an incompatibility with the original standards arises, is examined by Simcoe & Watson (2019) as a strategic decision and coordination problem. They point to the strategic shielding of their own user groups through the implementation of incompatible communication protocols in the early days of instant messaging. Files are sent on WhatsApp via the HTTP protocol and a separate server structure. Figure 4-11 represents the server structure on which WhatsApp is based.

Figure 4-11: Schematic representation of the WhatsApp architecture



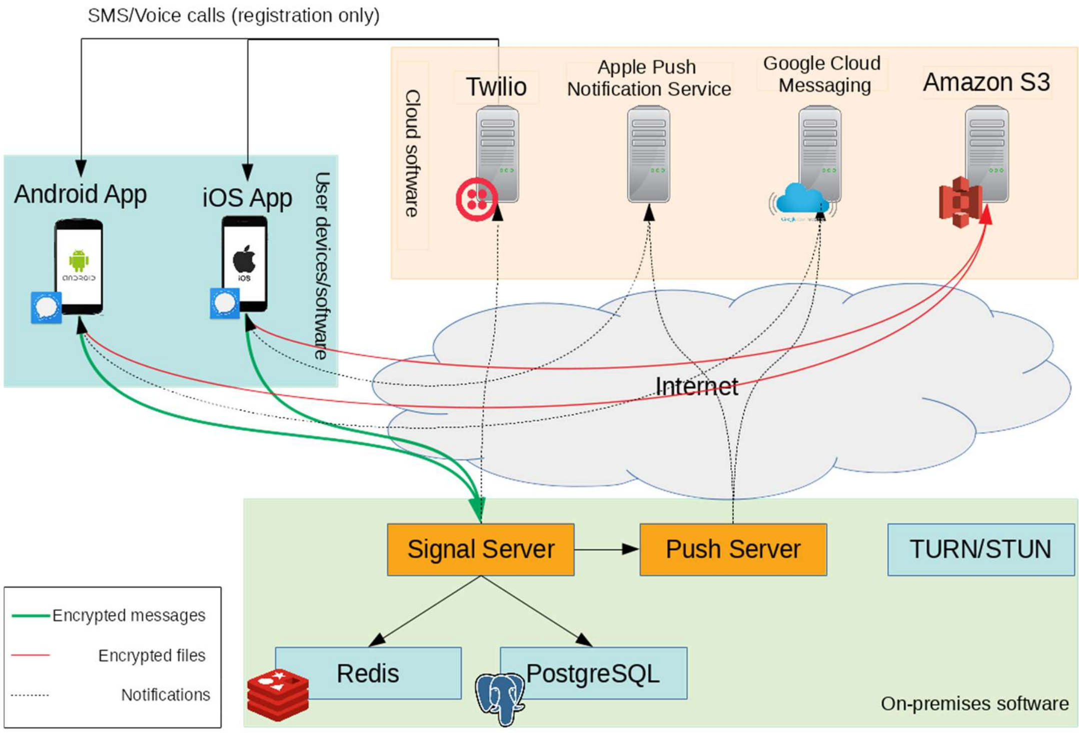
Source: Cressler (2021)

Cressler (2021) thus illustrates the separation of the structure for text-based communication and the sending of data, which results from the different requirements of the sub-services in terms of storage and sending. According to Eugene Fooksman, the choice of a strongly Erlang-based technology with ejabberd, Mnesia and YAWS lies in the scalability of this structure (D'Incau, 2013).

#### 4.2.1.2 Signal

In Figure 4-12 the basic infrastructure of Signal is shown, from which a setup of a split infrastructure can also be seen. To enable user verification, Signal uses Twilio for SMS verification[30] in addition to the operating system-related push servers from Apple and Google for app notifications. Signal also uses Amazon Web Services' cloud infrastructure (S3) for caching content yet to be delivered.

Figure 4-12: Schematic representation of the Signal architecture



Source: Cocorada (2018)

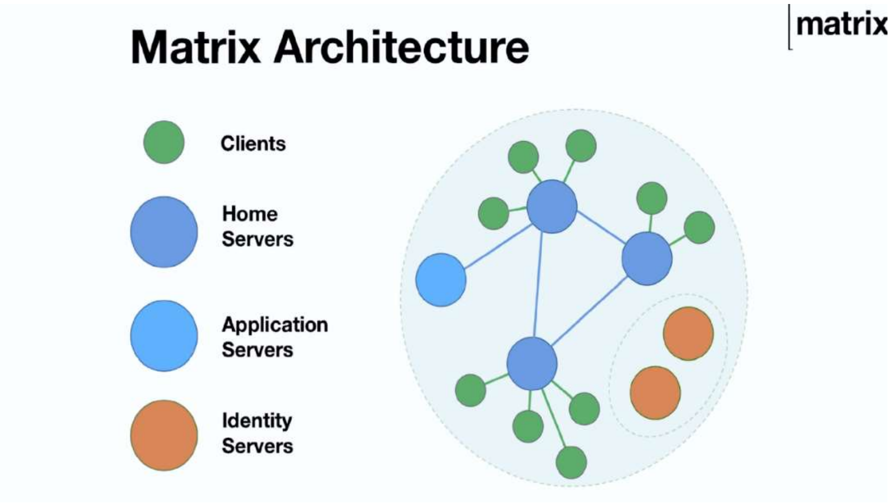
[30] See (Signal, 2021)

The TURN/STUN server component is required to switch the IP address of audio/video calls, insofar as no direct connection can be established [31] (Anturix, 2018). To store unstructured data, Signal uses Redis as a non-relational database and PostgreSQL for structured data in a relational database.[32] By publishing the client- and server-side source code, the dependencies presented can be reviewed transparently. The server and the Android app are written in the Java programming language and the iOS app in Swift.

### 4.2.1.3 Matrix

Matrix (see Figure 4-13) is not a singular messaging service due to its federated structure, but a protocol that enables federated messaging services. Thus, the structure of the Matrix system is structured into "home servers", which are operated by users, groups or services and each provide the digital infrastructure in the sense of an e-mail provider.

Figure 4-13: Schematic representation of the Matrix architecture



Source: Hodgson (2019)

The shared protocol offers the possibility to realise the network effects beyond the own home server. Following the logic of e-mail, the assigned Matrix IDs correspond to the pattern "@NAME:*HOME-SERVER*", which makes a connection to telephone numbers avoidable even in the course of registrations. In order to nevertheless connect identifiers outside of Matrix with the internal IDs, there are "Identity Servers" which, conceptually

[31] According to the forum post, this is particularly necessary if the mobile phone is behind a NAT. This is usually the case in the context of shared public IP4 addresses (carrier-grade NAT IPv4 address).

[32] More detailed information on data types and handling with regard to storage can be found in Chapter 3.6.

similar to the Domain Name Resolver[33], establish a connection between external and internal identifiers. The text messages are structured data in JSON format and are exchanged between the instances via HTTP and APIs. The APIs are versioned in the sense of decentralised and non-coordinated update cycles.

#### 4.2.1.4 Briar

In accordance with the decentralised P2P approach, Briar has no infrastructure, but is based exclusively on the devices on which Briar is installed. To establish a connection between the devices and thus enable communication, Briar uses either the wireless technologies WLAN and Bluetooth or alternatively the Tor network. One problem with infrastructure-free messengers arises as soon as a conversation partner is not connected and messages cannot be delivered. While in the case of groups, the members can serve as "hops" that hold a message until it is delivered, this involves compromises in the case of bilateral conversations. To solve this problem, Briar gives two approaches, one is to send messages via "multi-hub" through one's own contacts or to let users provide a mailbox architecture themselves. The former would limit the protection of metadata to the extent that at least the contacts would know when a connection takes place and between whom. An individually provided mailbox architecture increases the effort for the user and creates inefficiencies in infrastructure provision. The mailbox architecture is also unsuitable for synchronous communication (e.g. video chats). Due to the architecture, the functional scope of pure P2P messengers is therefore limited.

### 4.2.2 Source openness

Another aspect to be considered when looking at the different structures of messaging services is the open source nature of the services. From the user's point of view, there are two core functions that can be derived from open source software. On the one hand, open-source programmes provide transparency with regard to the exact mode of operation, which external services are contacted and which encryption is implemented. This also makes it possible to trace the collection and handling of metadata. On the other hand, open-source software makes it possible to operate the infrastructure independently, insofar as this is not only done for reasons of transparency, which strengthens the autonomy of the users. If, in addition to the pure openness of the source, the publication licence also provides for the adaptation of the software, it is also possible for users to make adaptations (taking into account the standard) or to connect further complementary services in addition to the pure operation of their own instance. As also explained in Chapter 3.6 there are basically three classifications of source openness:

[33] DNS servers are a kind of address book of the Internet and are responsible for providing the assigned IP address(es) from the voice-based Internet addresses.

- Proprietary systems that do not publish source code and may use security audits as a signal about the quality of the implementation.
- Open source systems that only publish the source code for transparency reasons, but prohibit the use of the source code.
- Open source systems that allow varying degrees of use and/or customisation.

### 4.2.3 Data protection and security

Horizontal IOP between the same types of applications also requires that certain user data is exchanged so that, for example, in the context of messaging services, messages and/or video calls can function across multiple services. Here, it is not necessarily the actual content (possibly end-to-end encrypted) that is relevant, but rather the accruing metadata. Currently, consumers have chosen certain messaging services for various reasons, be it their functionality, their prevalence, or higher security and/or a better level of data protection. These aspects of consumer interests, which are reflected with horizontal differentiation of services, must also be taken into account under sovereignty aspects when designing IOP regulations.

In this context, messaging services such as Threema or Signal differentiate themselves from other services through aspects of security or data protection, such as end-to-end encryption, no storage of personal data after delivery on their own servers or the general absence of collection of personal data. Horizontal IOP for messaging services could lower the security standards of messaging services, as it is difficult to fully reconcile two different encryption technologies and different security approaches without compromise.[34] Therefore, for communication between messaging services, the lowest common denominator at lower security levels cannot be excluded as a compromise. A survey of market parties by the Bundeskartellamt confirms this assumption, especially with regard to end-to-end encryption, as it would be impossible to maintain this "... [under IOP. To do so, all providers of interoperable functions would have to use the same protocol]" *(„... unter IOP beizubehalten. Dazu müssten alle Anbieter der interoperablen Funktionen das gleiche Protokoll verwenden.*“) (Bundeskartellamt 2021).[35] Experts interviewed by WIK-Consult also ultimately shared the assessment that there could be no end-to-end encryption under messenger IOP without complete standardisation or agreement on a uniform encryption standard. Aspects of end-to-end encryption are addressed separately again in the following Chapter.

[34] This may include storing communications on servers, sending data to the cloud or only to servers in the relevant country and requiring personal identification for subscription.

[35] Translated from: V Ermittlungsergebnisse, 1. Interoperabilität, d) Auswirkungen von Interoperabilität, cc. Datensicherheit, p. 64.

According to a recent article, major messaging companies such as Google and Apple have already expressed their concerns that IOP could create unnecessary privacy and security vulnerabilities (Wooden, 2022).

In addition, apps that are interoperable with a privacy-focused messaging service can collect personal user data that is shared between apps to enable communication between them. Overall, users of a service such as Threema would therefore have the advantage of being able to communicate with users of other applications such as WhatsApp (i.e. benefit from the network effects), but at the same time would have to put aside their preferences regarding the chosen security and the non-collection of personal data, which were presumably significant for the choice of such an alternative messenger.

Practically, the same advantage of network effects for a user can be achieved through multi-homing via the simultaneous use of another service. From the point of view of the more privacy-conscious providers, e.g. Threema or Signal, this horizontal IOP is also not advantageous, as their unique selling proposition is diluted. In a corresponding survey by the Bundeskartellamt, one provider, who particularly targets users who attach great importance to data protection, sums up, "...[all this is certainly not in the consumers' interest. For users, the security of communication would become intransparent and uncertain...users would not know which app the other party was using]" *(„...all dies sei sicherlich nicht im Sinne der Verbraucher. Für die Nutzer werde die Sicherheit der Kommunikation intransparent und ungewiss…die Nutzer wüssten nicht, welche App das Gegenüber verwendet")* (Bundeskartellamt, 2021). The messaging services with less security and/or more personal and user data collection, on the other hand, would benefit because they could collect even more data than before.

Regardless of the content encryption discussed below, a certain minimum amount of metadata is generated when sending messages. Registration with messaging services is largely done by disclosing voluntary data for unique identification, although there are services that do not make this a requirement.[36] Telephone numbers in particular are suitable as a common identifier, as these are often available in the local address book of the mobile phone and thus a comparatively simple "contact discovery" can be carried out. "Contact discovery" is a relevant component of the usability of messaging services, as this is a prerequisite for recording the possible conversational partners on the basis of one's own address book. Here there is a conflict of goals between the usability of recognising all possible contacts, i.e. the social graph of a user, and data protection. The complexity of a data-protection-friendly technical implementation of "contact discovery" is explained in Chapter 4.2.4. In addition to the telephone number, the email address is an alternative way to identify users and enable account recovery. Further voluntary data that can be shared by the user consists of the first and last name or alternatively a user name. Depending on the service, there is the option of a personal profile picture, date of birth,

[36] Even if some services declare the provision of the telephone number as a mandatory requirement, the acceptance of this requirement is a voluntary decision by the user to accept this as part of the terms of use.

gender or nationality. These details are usually not mandatory. If the address book of the device is shared, this is also voluntary information on the part of the user, although depending on how the service handles data protection, not all contacts in the address book necessarily agree to this. In the case of a full IOP, a transparent description of the handling of metadata would be necessary, as well as a demarcation of which metadata may be stored by the services of the respective contacts. If this demarcation is unclear, there is a possibility that the metadata of users of more data protection-friendly services will nevertheless be stored via the contact to users of other services.

Another part of the data that can be collected is generated during the use of the app and can be categorised as observable data. These include device and configuration files and/or location data, i.e. passively generated data. Observable data, which is actively generated through use, includes group memberships and usage behaviour. In particular, usage data such as frequency and duration of use, times of use and contact with other users supply the provider with information about the flow of attention and the "social graph" of its users. The BSI (2021) has summarised the classification of metadata as shown in the following Table 4-2.

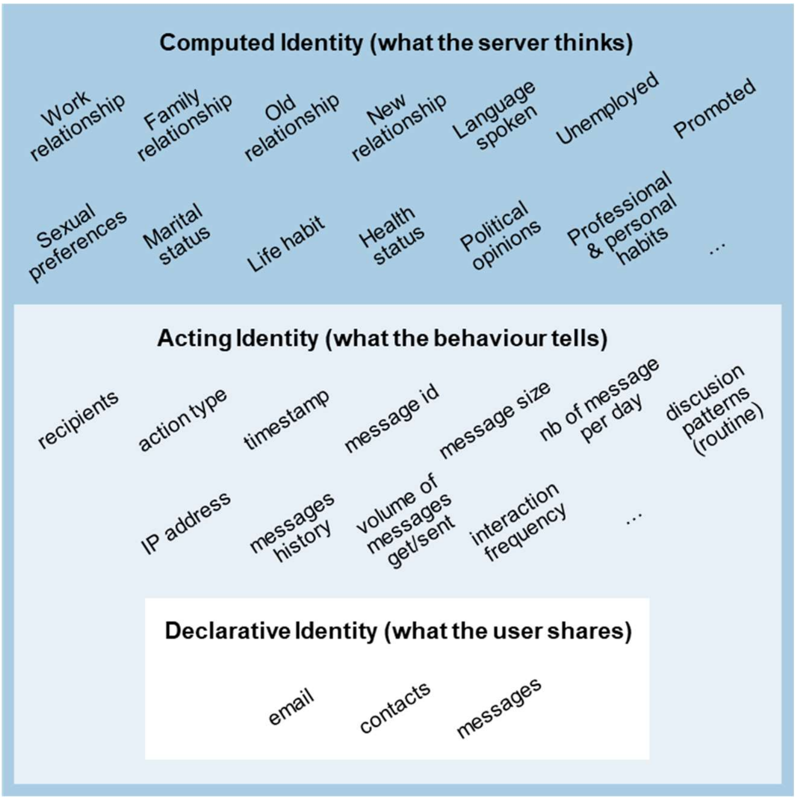
Table 4-2: Classification of metadata of modern messengers

| | |
|---|---|
| Personal data:<br>*Volunteered data* | Profile pictures, first or last name of the user, user name or pseudonym (e.g. nickname), date of birth, age, gender, nationality, email address, telephone number, account information. |
| Device / configuration data:<br>*Observed data* | IP address, operating system, network operator, device type, device IDs, user accounts, passwords, certificates, installed apps, region and language settings |
| Location / movement data:<br>*Observed data* | Whereabouts, time of stay, duration of stay, movement profiles |
| Third party contacts / data:<br>*Volunteered data* | Contact directory, address books |
| Group memberships:<br>*Observed data* | Participant or host in chat groups, telephone conferences, video conferences |
| Usage behaviour:<br>*Observed data* | Frequency and duration of use of a messenger app, online/offline status, browser history, use of different end devices, times / duration / participants of an exchange via text message / phone call / video call |

Source: BSI (2021); classification of volunteered/observed data according to Crémer et al. (2019)

One of the monetisation options presented in Chapter 4.1.3.4 is indirect funding through advertising in other services or on platforms. In order to generate a benefit from the information accrued in the course of registration and use, it needs to be connected and attributed to individuals. Pujol et al. (2019) defines these as different degrees of digital identity and classifies them into declared, representational and deduced identities. Under the declared identity, the authors summarise the voluntarily shared information. According to the table above, this includes all information (personal data, contacts/third party data) that the user voluntarily shares. The representing identity extends this to include the observed information (device/configuration data, location/movement data, group memberships, usage behaviour). However, part of the value creation is the deduced identity, i.e. the identity that emerges from the models, which forms expectations about the characteristics and traits of the users based on the preceding data. In particular, this includes the social graph of the users, enriched with information about the frequency of contact. Based on this, it is possible to form an iteratively approximated image of the users on the basis of this deduced information, which can be used for contact suggestions in social networks and for the personalisation of advertising for composite products. Figure 4-14 visualises the overlap of the gradual expression of digital identities.

Figure 4-14: Degrees of digital identities in the context of messaging services

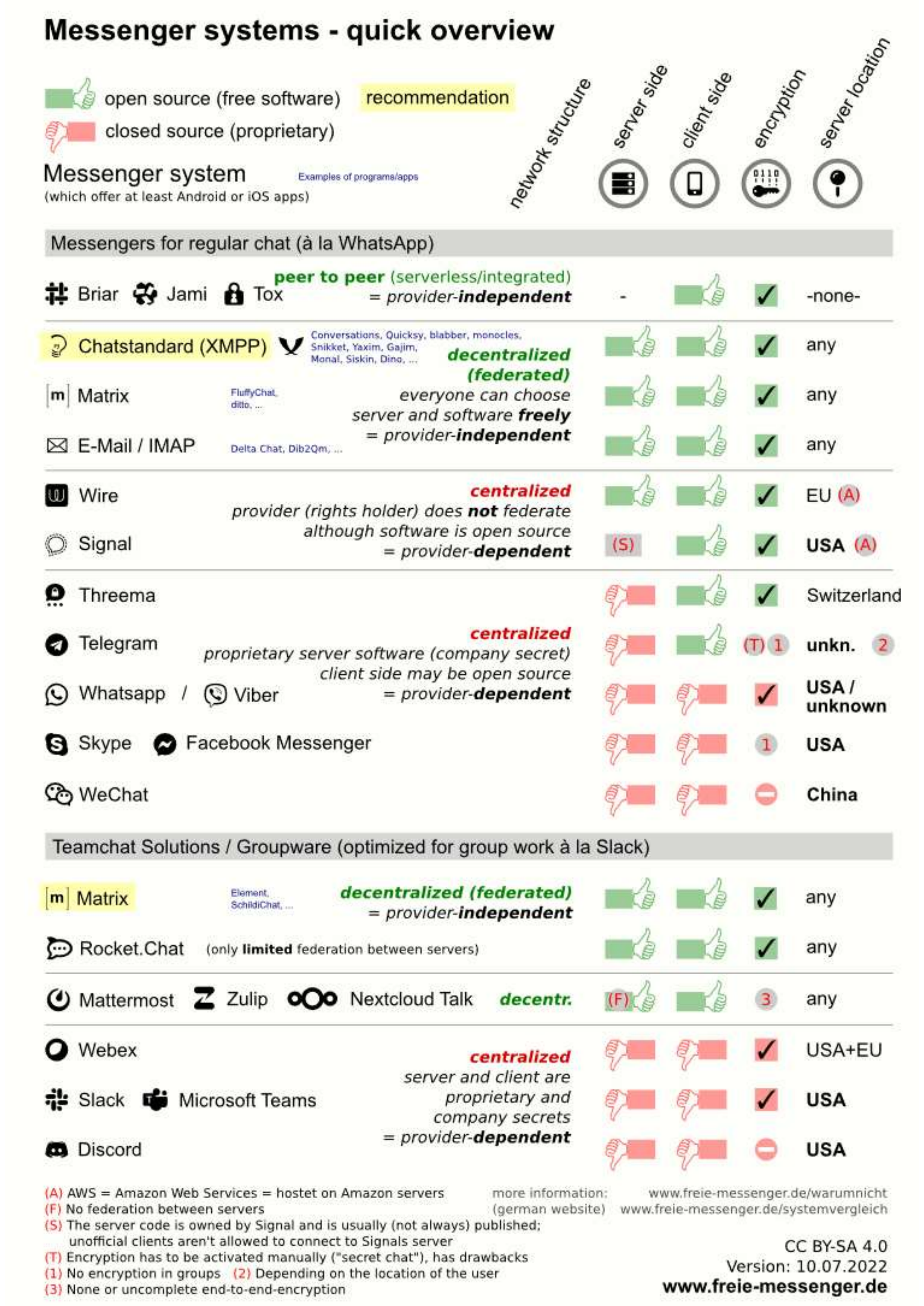


Source: Pujol et al. (2019, p. 180)

### 4.2.4 End-to-end encryption

End-to-end encryption (also: E2E or E2EE - end-to-end-encryption) of messages plays a special role in the context of data protection and data security (cf. also Chapter 4.4 on the current discussion within the framework of the DMA).

Figure 4-15: Comparison of selected messaging services from a security perspective



## Messenger systems - quick overview

🟩👍 open source (free software) recommendation

👎🟥 closed source (proprietary)

Messenger system (which offer at least Android or iOS apps) — Examples of programs/apps

| Messenger system | Examples of programs/apps | network structure | server side | client side | encryption | server location |
|---|---|---|---|---|---|---|
| **Messengers for regular chat (à la WhatsApp)** | | | | | | |
| Briar, Jami, Tox | | **peer to peer** (serverless/integrated) = *provider-**independent*** | - | 👍 | ✓ | -none- |
| Chatstandard (XMPP) | Conversations, Quicksy, blabber, monocles, Snikket, Yaxim, Gajim, Monal, Siskin, Dino, ... | ***decentralized (federated)*** *everyone can choose server and software **freely** = provider-**independent*** | 👍 | 👍 | ✓ | any |
| Matrix | FluffyChat, ditto, ... | | 👍 | 👍 | ✓ | any |
| E-Mail / IMAP | Delta Chat, Dib2Qm, ... | | 👍 | 👍 | ✓ | any |
| Wire | | ***centralized*** *provider (rights holder) does **not** federate although software is open source = provider-**dependent*** | 👍 | 👍 | ✓ | EU (A) |
| Signal | | | (S) | 👍 | ✓ | **USA** (A) |
| Threema | | ***centralized*** *proprietary server software (company secret) client side may be open source = provider-**dependent*** | 👎 | 👍 | ✓ | Switzerland |
| Telegram | | | 👎 | 👍 | (T) 1 | **unkn.** 2 |
| Whatsapp / Viber | | | 👎 | 👎 | ✓ | **USA / unknown** |
| Skype, Facebook Messenger | | | 👎 | 👎 | 1 | **USA** |
| WeChat | | | 👎 | 👎 | ⊖ | **China** |
| **Teamchat Solutions / Groupware (optimized for group work à la Slack)** | | | | | | |
| Matrix | Element, SchildiChat, ... | ***decentralized (federated)*** = *provider-**independent*** | 👍 | 👍 | ✓ | any |
| Rocket.Chat | | (only **limited** federation between servers) | 👍 | 👍 | ✓ | any |
| Mattermost, Zulip, Nextcloud Talk | | ***decentr.*** | (F) 👍 | 👍 | 3 | any |
| Webex | | ***centralized*** *server and client are proprietary and company secrets = provider-**dependent*** | 👎 | 👎 | ✓ | USA+EU |
| Slack, Microsoft Teams | | | 👎 | 👎 | ✓ | **USA** |
| Discord | | | 👎 | 👎 | ⊖ | **USA** |

(A) AWS = Amazon Web Services = hostet on Amazon servers
(F) No federation between servers
(S) The server code is owned by Signal and is usually (not always) published; unofficial clients aren't allowed to connect to Signals server
(T) Encryption has to be activated manually ("secret chat"), has drawbacks
(1) No encryption in groups (2) Depending on the location of the user
(3) None or uncomplete end-to-end-encryption

more information: (german website) www.freie-messenger.de/warumnicht www.freie-messenger.de/systemvergleich

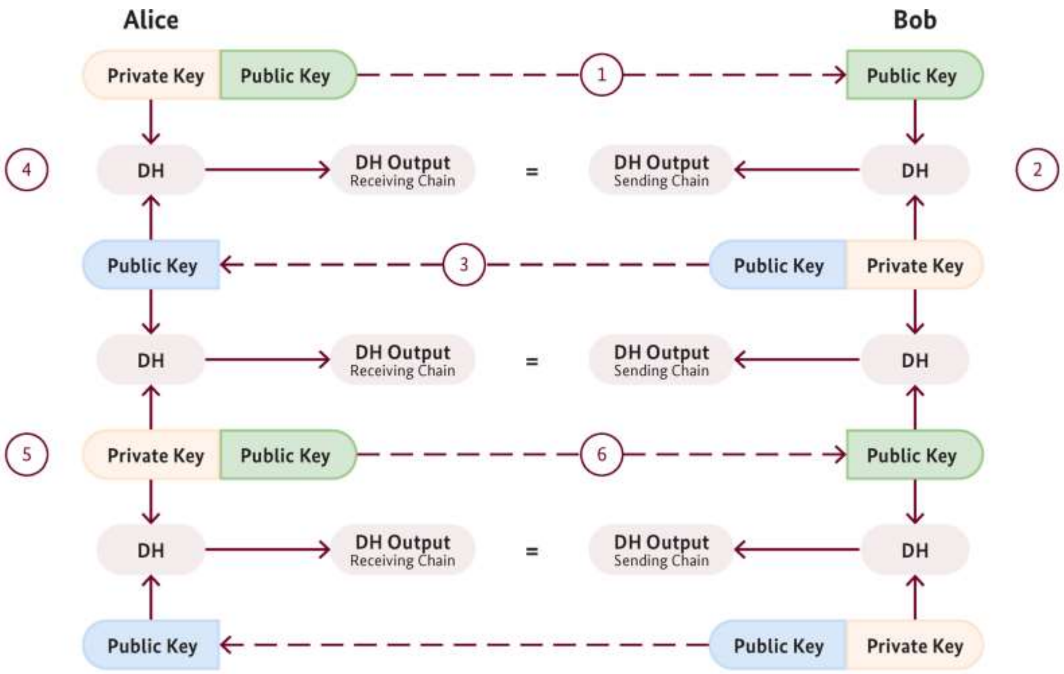
Version: 10.07.2022
**www.freie-messenger.de**

Source: Gekeler (2022)

Due to multiple revelations by Edward Snowden, among others, many users have become more security-conscious. In response to pressure from users and public reporting, WhatsApp implemented end-to-end encryption of the Signal protocol in April 2016 and thus ensured within a short period of time that a large part of communication via this service was encrypted (Marlinspike, 2016b). The Signal protocol is considered a further development of the previous encryption methods Pretty Good Privacy (PGP) for e-mail and Off-the-Record Messaging (OTR) and combines essential features of modern communication encryption. In the first place, encryption must ensure that the contents are subject to *confidentiality*. If this property is given, neither third parties nor operators of the service can trace the content apart from the intended recipients. For this reason, end-to-end encryption offers a higher level of data protection than can be guaranteed with transport encryption such as TLS (Transport Layer Security). Furthermore, encryption must also be able to ensure that the *authenticity and integrity* of the message is guaranteed, i.e. that all recipients of the message can undoubtedly identify the sender and that messages are also received in unmanipulated form, as sent by the respective sender (Unger et al., 2015). Further security features refer to the case of key compromise and are defined as *Forward Secrecy* and *Post-Compromise Security*. Forward secrecy ensures that in the event of knowledge of the master or long-term keys, no content can be subsequently decrypted. This is achieved by means of independent session keys, from which at time $t_0$ no inference to past keys from the time period $t_{-1}$ is possible (Rösler et al., 2018). An even higher level of security can be achieved with post-compromise security, which guarantees a "self-healing" effect of the encryption. This is achieved by ensuring that an encryption that is compromised at time $t_0$ also does not allow any conclusions to be drawn about future keys in $t_1$.

These secure properties shown above are usually solved for messengers with asymmetric Double Ratchet Diffie-Hellman keys. Diffie-Hellman keys are the result of a mathematical procedure in which an identical key is generated reciprocally from the combination of the private and public keys. This shared Diffie-Hellman secret is only known to the two parties and does not allow any conclusions to be drawn about the respective private keys that were originally used to generate it. If this process is iterative on both sides, it is called a "double ratchet". This is "turned" each time in order to generate a new shared secret. In Figure 4-16 the derivation of an asymmetric ratchet is shown in a simplified way. As a basic prerequisite, both parties to the conversation have a public and a private key. This can be illustrated in an example. Alice sends Bob her public key with the first message, which enables him (together with his private key) to calculate a Diffie-Hellman secret. In the next step, Bob also sends his public key to Alice with his message, so that she can also calculate the Diffie-Hellman secret (together with her private key). This Diffie-Hellman secret contains derived information of the private keys of both parties to the conversation, which remain exclusively local on the devices and thus cannot be seen by the service operator. This means that the service operator cannot calculate the joint key of Alice and Bob by observing the exchanged public information. Mathematically, this is guaranteed by modular arithmetic or elliptic curves, in the case of the Signal protocol by the elliptic curve Curve25519 (Bernstein, 2006). These elliptic curves can be understood mathematically as one-way functions, where the calculation is simple, but the inversion of the function is only possible with very great computational effort. Through a uniquely generated Diffie-Hellman secret, the property of confidentiality is achieved. However, in order to protect past and future messages, double ratchet protocols provide for the generation of a new key pair at regular intervals (in the case of the Signal protocol with each message) according to a function known only to Alice and Bob. This is compared to two ratchets that are rotated once with each message. An indicator in the encrypted message tells both parties at which position of the "ratchet" the respective party is located, so that no asymmetry arises even if messages are not received.

Figure 4-16: Simplified representation of double ratchet encryption



1. Alice sends a message together with her public key to Bob.
2. Bob calculates a common Diffie-Hellman secret (DH) with Alice's public key and his private key.
3. Bob sends his public key together with his next message to Alice.
4. Alice uses Bob's public key and her private key to calculate the common Diffie-Hellman secret.
5. Alice generates a new key pair.
6. Alice sends a message together with her new public key to Bob (etc.).

Source: BSI (2021, p. 8)

The necessary coordination effort between the two parties must be made by the service used, which must explain the framework parameters of the protocol to the parties involved. Without this coordination, it would not be possible to encrypt a message in such a way that the content would not be visible to third parties and both parties would also "agree" on a common encryption. This also has implications for the IOP, insofar as the encryption of the messages is to be guaranteed.

The exact implementation of end-to-end encryption differs between messaging services, although certain trends can be identified. For example, Ermoshina & Musiani (2019) describe an ongoing process of partial quasi-standardisation of the Signal protocol, which is used by a large proportion of services, sometimes with slight adaptation, but which, unlike PGP, has not undergone any official standardisation procedure.

Table 4-3: Overview of encryption protocols used by selected messaging services

| **Service** | **End-to-end encryption bilateral:** | **End-to-end encryption group:** |
|---|---|---|
| Discord | N | N |
| Element (Matrix) | Olm (Signal-based) | Megolm (Signal-based) |
| FB Messenger | Proprietary (Signal-based) | N |
| Google Chat (Hangouts) | N | N |
| iMessage | Proprietary | Proprietary |
| Instagram DM | Proprietary (Signal-based) | N |
| Kik | N | N |
| Signal | Signal protocol | Signal protocol |
| Skype | Proprietary (Signal-based) | N |
| Slack | N | N |
| *SMS (trad. TC)* | *N* | *N* |
| Snapchat | N (Images only) | N |
| Telegram | Proprietary (MTProto 2.0) | N |
| Threema | NaCl | NaCl |
| Viber | Proprietary | Proprietary |
| WeChat | N | N |
| WhatsApp | Proprietary (Signal-based) | Proprietary (Signal-based) |
| wickr | Proprietary (source code visible) | Proprietary (source code visible) |
| Wire | Proteus (Signal-based) | Proteus (Signal-based) |

Source: WIK-Consult

Table 4-3 shows that, insofar as message encryption is guaranteed, it is often derived from the Signal protocol. These include in particular the products of the Meta group (WhatsApp, Facebook Messenger and Instagram), the Microsoft service Skype and the derivatives Olm (Matrix protocol) and Proteus (Wire). With Facebook Messenger, Instagram and Skype in particular, encryption is only possible for bilateral communication and must be switched on by the user.[37] Telegram has built the encryption proprietary similar to the concept described above and calls it MTProto. This end-to-end encryption must also be activated by the customer. Threema's encryption, on the other hand, is based on the NaCl library and is activated by default for all chats. According to an article by Spektrum, NaCl is considered very secure, but unlike the Signal protocol, it does not offer post-compromise secrecy, which is why the Signal protocol is considered "state-of-the-art" (Wolfangel, 2021).

Encryption in groups, if implemented, is currently based on bilateral encryption between each member of the group with all other members according to the above principles. This results in a disproportionate increase in the necessary key exchange procedures with each additional member in the group, which is why the groups in WhatsApp, for example, are limited to 512 members and in Signal to 1000 members. This is where the new MLS protocol comes in, which is supposed to achieve efficient scaling without compromising security. The name of this encryption protocol, which is still under development, is based on the TLS protocol, which is a transport encryption and is used in particular for HTTPS connections in the browser. Nevertheless, there are contrasts to TLS, where bilateral encryption is negotiated between server and clients, since more parties are involved in groups in messengers and the duration of a session sometimes extends over several years. Furthermore, TLS as a protocol considers direct and synchronous encryption, where both parties need to be online, whereas encryption in messaging services must also work under asynchrony. For these reasons, group encryptions in MLS are arranged in a tree structure called TreeKEM, so that when a group member leaves, the corresponding strand in the tree structure updates the encryption. The exact procedure is described by Bhargavan et al. (2018) in more detail in a proposal for the MLS standard.

In contrast to Signal, whose protocol is deliberately not structured in a federated manner (Marlinspike, 2016a) however, the examples of Matrix and e-mail show that identity and key management can generally also be implemented in a decentralised manner, as experts interviewed by WIK-Consult also confirm. Still, the widespread use of the Signal protocol to date would be a good starting point for further standardisation approaches. However, it must be taken into account for possible implementations with regard to IOP between messengers that the Signal protocol provides for a central identification server, which is required for the public keys and a bundle of one-time keys for the initial negotiation of encryptions (Marlinspike & Perrin, 2016). Accordingly, such an implementation of IOP must take into account ways to access these identity servers.

[37] On Facebook Messenger, this function is called "Secret conversation", on Instagram it can be found under the function "Start end-to-end encrypted chat" and Skype calls this function "Private conversation".

In addition to the content, the Signal protocol also encrypts the header. The telephone numbers of the contacts are "hashed"[38], so that a comparison[39] can take place, but the process of "contact discovery" does not directly lead to a reduction in data protection for third parties (Marlinspike, 2017). Beyond the matching of telephone numbers, messaging services also have the option of using social graphs to track the interaction of users. Especially in the context of ecosystems, identifiers such as phone numbers can be used to draw conclusions about interactions across services. For the IOP approaches discussed below, end-to-end encryption presents a particular hurdle in its technical complexity. As encryption experts interviewed by WIK-Consult confirm, true end-to-end encryption between interoperable messengers can ultimately only exist with complete standardisation or agreement on a common encryption standard. Since these are mostly proprietary systems that use mutually incompatible encryption methods, the necessary agreement and implementation effort would be extremely high and, according to one of the experts, would be equivalent to the development of a new interoperable messaging platform.

## 4.3 Interoperability approaches & obligations

### 4.3.1 Different types & approaches to interoperability

#### 4.3.1.1 Standardisation as protocol interoperability

The most technically robust solution would be to jointly agree on a standard by defining the necessary encryption, semantics and technical details as part of a cross-sector agreement process. This would require negotiating the scope of the standard with the features to be considered. All of this would have to be defined in a process, which could then lead to achieving a "protocol IOP", as explained in Chapter 2.1.

It also follows from the above discussion on encryption that insofar as messages are to be end-to-end encrypted, a need to coordinate on an encryption protocol arises. Table 4-3 shows a widespread use of protocols based on the Signal protocol. WhatsApp, Facebook Messenger as well as Instagram have implemented this protocol with the collaboration of Signal, although without source code there is no actual traceability (Marlinspike, 2016b). Other messengers are based on forks and further developments of the Signal protocol, such as Wire and Matrix. Ermoshina & Musiani (2019) infer from this a de facto

[38] A hash function encrypts the content using a one-way function that has the same values as output given the same input parameters. For example, the number "1234567890" is turned into the hexadecimal hash "c775e7b757ede630cd0aa1113bd102661ab38829ca52a6422ab782862f268646" by the SHA256 function of the Python library "hashlib", regardless of the instance used. From this hash, no conclusion can be drawn without knowing the number, but if another person wants to match this number, they send this hash to the server and find the contact with this number.

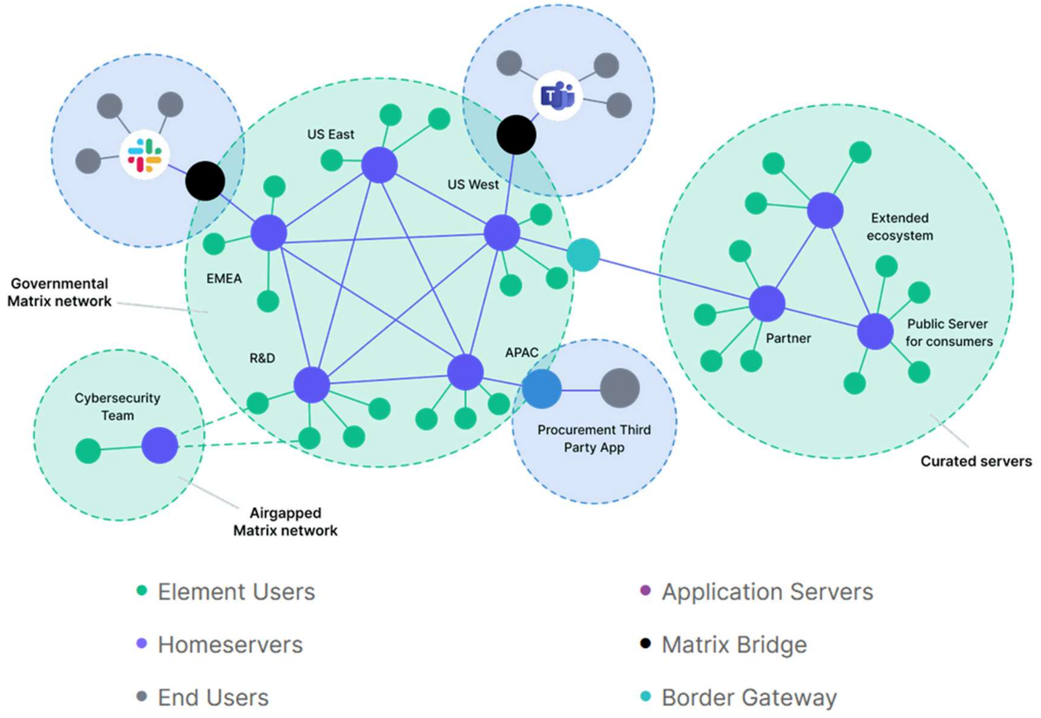
[39] Since 2017, Signal has made it possible to run this process in an encrypted enclave on the server, so that this process runs completely separately from Signal's database of registered users.

standardisation for the area of end-to-end encryption. It should be noted, however, that due to the technical complexity of encryption, unlike file formats such as PDF or DOCX, IOP does not result as a “by-product” from this. For this, they describe a process of "quasi-standardisation", which follows an asymmetric standardisation. This process is based on a working code that only subsequently becomes a "quasi-standard" through implementation. This tendency towards standardisation follows the logic of developers that a standardisation process reduces the "silo effect" and enables a reference implementation. However, Ermoshina and Musiani also describe an increasing dissatisfaction of developers with standardisation processes. According to interviews, the criticism is based on the slowness of standardisation committees such as the IETF and W3C. For this reason, Signal’s approach is first to move beyond the programming of functionality to documentation, which could then potentially be the basis for standardisation. A similar approach is taken by the Matrix developer, who would like to get the service "stable"[40] before a standardisation process could be considered (Ermoshina & Musiani, 2019). The MLS standard, which is currently still under development, should also be mentioned in this context, as it aims to improve scalability for groups.

Since Matrix follows the principle of federation from its basic conception, this concept would be suitable in principle for a standard for IOP. Figure 4-17 shows an example of a federated network, which could also be transferred to interoperable networks of different service providers in this sense. The blue points here would be the different "home servers" as the interoperable services, which can all communicate with each other on the basis of a protocol.

[40] In the development of software, there is a graduated description of the programme status, which can be understood from alpha as the first functioning version, through beta as a test version, to stable or final. In non-final programmes, essential parameters for standardisation can still change, so that premature standardisation either restricts the autonomy of the developers or the standard would have to be adapted iteratively.

Figure 4-17: IOP of federated systems in the Matrix protocol



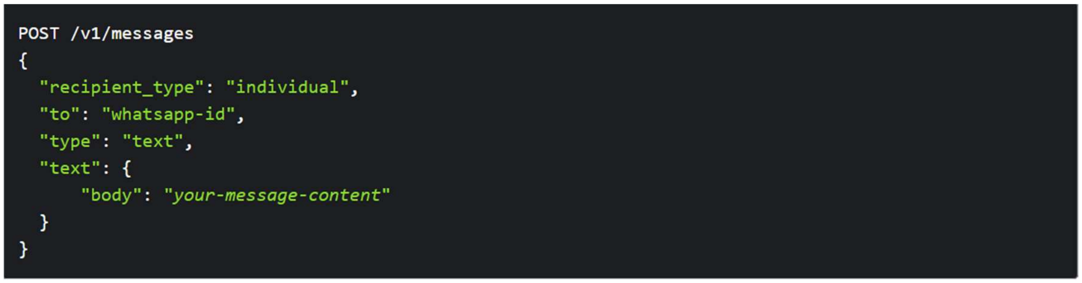
Source: Element (2022a)

One problem here, however, could be the standardisation of the identity servers, which currently establish a connection between third-party identities (telephone number, email address) and the Matrix-inherent ID in federated Matrix systems. This process would be necessary for the so-called "contact discovery", where it becomes recognisable which contacts in the local address book can be reached via which service. Since this database contains personal data, it would have to be coordinated whether and to what extent access by the different services to this identity database can be regulated. Alex Stamos, director of the Stanford Internet Observatory and former CSO at Facebook, is quoted in an article by the news portal TheVerge as follows: "There is no way to allow for end-to-end encryption without trusting every provider to handle the identity management... If the goal is for all of the messaging systems to treat each other's users exactly the same, then this is a privacy and security nightmare" (Faife, 2022).

### 4.3.1.2 Interfaces and API access

While converters use the usual interfaces of the service, in the environment of C2B communication ("consumer-to-business") many services offer interfaces in order to contact their customers via them on a larger scale. Dedicated API endpoints, as explained in Chapter 3.6.1, are suitable in a commercial context through authentication, as mapping can take place. However, as an interface usually does not negotiate encryption of the content beyond the transport encryption TLS, in this case the messages are not subject to end-to-end encryption. The WhatsApp Business API solves this circumstance by having the client using the API run the software on the corporate network, which means that the message remains encrypted between the API endpoint and the recipient. Figure 4-18 shows how a pure text message is sent via the API. In addition to the "text" option, more complex interactive messages, voice messages, videos and files can also be sent. The possibilities offered by WhatsApp Business are explained in a comprehensive developer portal.

Figure 4-18: Example from the WhatsApp Business API documentation



```
POST /v1/messages
{
  "recipient_type": "individual",
  "to": "whatsapp-id",
  "type": "text",
  "text": {
      "body": "your-message-content"
  }
}
```

Source: Facebook (2022)

Furthermore, WhatsApp points out in its whitepaper on encryption that as soon as an intermediary runs the software or the cloud service is used without an own server, end-to-end encryption only takes effect between this software or cloud instance and the recipient of the message (WhatsApp, 2021). The whitepaper contains the following wording: "WhatsApp does not consider chats with organisations who choose to use Facebook to operate their API endpoint to be end-to-end encrypted” (WhatsApp, 2021, p. 26).

The OECD report (2021) on competition in digital markets mentions the possibility of "Personal Information Management Systems" (PIMS) for the management of personal data, which can act as trustees (OECD, 2021). In principle, a digital trustee would also be able to take over the function of an intermediary, but there are likely to be differences in the requirements between the management of identities and the provision of a permanently running messaging service with many messages exchanged.

Considering the proposal of individual proprietary interfaces in the non-paper of the European Commission (2022a) it must be taken into account that in principle the risk of emerging security gaps and points of attack for misuse can be created. Opening up a system that was previously designed to be closed to interfaces is more complex than systems that were originally designed to be open. In the case of Cambridge Analytica and Facebook, it should also be noted that existing interfaces can also result in data protection risks for users through misuse or improper use.

#### 4.3.1.3 Bridges

As explained in Chapter 2.1.2 above, adapters and converters are a way to establish compatibility between incompatible products or services. In the case of messaging services, this is a "translator" from the data model of messenger A to the data model of messenger B, which aligns any differences in the data models. Bennaceur et al. (2012) call this process an aggregation of disparate systems with the help of mediators. Although from an economic point of view messaging services are relatively homogeneous in terms of the basic features discussed above, the technical implementation is very different, as discussed in the previous Chapters. Thus, a process of conversion implies both technical and semantic "translation". Technical differences can be understood as file formats, semantic differences are data that go beyond the actual message, i.e. metadata, and the type of declaration and explanation. Through this translation process from one data model to another, it is inevitable that the original message is provided unencrypted or decrypted before conversion, which violates the concept of end-to-end encryption. According to the experts interviewed by WIK-Consult, this can therefore only be guaranteed if the same standard is used (cf. also Chapter 4.2.4). Since most messengers are not designed to "communicate" with a converter on the other side, it is also necessary that this converter is designed as a "puppet". The converter thus imitates the other side and behaves accordingly as if the converter were another instance of this messenger. This results in a fragility in the case of changes, which must then be imitated by the converter, insofar as there is no source openness. Depending on the complexity of the service to be "translated", not all features can be made compatible. Furthermore, a separate converter must be programmed and kept up to date for every other messenger that is to be contacted. This effort increases with the diversity and complexity, especially of the features offered by the messengers (e.g. exchange of image, audio or video files as well as audio/video calls). In the area of messengers, converters are a common solution for providing adversarial IOP, sometimes rather adversarial compatibility due to a lack of direct "usability".

The development of Matrix is in the context of decentralised messenger providers, which is why services that are not based on the Matrix protocol must be made (partially) compatible via converters using so-called "bridges". These are also provided open-source for implementation and currently each include their own "bridges" for Facebook Messenger, iMessage, WeChat, Instagram, Signal and WhatsApp, among others (Matrix, 2022). With regard to the sometimes limited "usability" explained above, the implementation of iMessage to Matrix should be mentioned at this point. Thus, to establish the functionality, a separate Mac computer or a modified iOS firmware is necessary, on which a separate server runs that accesses the local message database and sends the messages. For this bridge, Matrix also indicates that the encryption is exclusively between end user 1 and the bridge. In addition to the publicly provided bridges maintained by the Matrix community, Element (formerly Riot) offers a commercial SaaS offering for end users and companies. The Bridges, for one, are more comprehensive and seamless integration is advertised (Element, 2022b). A similar Matrix-based service is offered by Beeper, which also shares the problem of incompletely compatible bridges (Beeper, 2022).

Due to the fact that the bridges are not recognisable as such to the conversational partner, Kuketz (2020) identifies data protection concerns. Especially since the protection of metadata is treated very heterogeneously and is part of product differentiation, differences can arise here. For example, Kuketz points out that if a user of Messenger A contacts a user at Messenger B via a bridge, this user B has not given consent to Messenger A's data processing. However, since at least the metadata relating to this communication exchange can also be collected by Messenger A, this is questionable in terms of data protection law, as Kuketz concludes.

Another obstacle to the operation of these bridges are the terms of use of the messaging services. For example, in the terms of use of WhatsApp there is a paragraph that prohibits both reverse engineering and derived services. In this respect, the use of bridges is likely to be critical from a legal point of view without an official IOP obligation. So far, there have been no reports of attempts to actively prevent the legal use of these bridges. However, there are reports of WhatsApp attempting to have modified apps removed from the app stores (Johannsen, 2015).

### 4.3.1.4 Multi-Messengers as an aggregation service

Aggregation services have gained relevance especially in the area of price comparison portals and offer in the initial form the possibility to compare prices on a graphical interface and to be redirected to the separate page of the provider after the decision. Search engines reduce the user's search costs from this point of view. A similar concept is pursued by the application DM Me, which combines messengers available locally on the device in one interface. Since the device and thus the user himself is the respective end point of the encryption, this implementation can circumvent the problem of violated end-to-end encryption.

Here, too, implicit "search costs" are to be reduced by the question of which contact is usually contacted via which service, by creating a common uniform user interface. From a technical point of view, however, there is no connection between the services through a separate application, which means that no compatibility is established and it is not technically a genuine IOP. The low penetration of these services suggests that only little added value is created. It is unclear to what extent this circumstance can be counteracted by specifications for the opening of interfaces. Despite the problems described in Chapter 4.3.1.3 on the use of bridges that are used for aggregation, such services can be seen to a certain extent as messengers that simplify multi-homing and can therefore be assessed positively in this respect.

### 4.3.2 Current proposals

The following analysis focuses primarily on the IOP regulations discussed and envisaged within the framework of the DMA. In addition to the approaches shown in Chapter 3.1.2.1, similar demands for IOP obligations or at least prohibitions of disproportionate prevention of IOP are also increasingly taking place at the international level, including in the area of messaging services (ACCC, 2020; CMA, 2020),ACCESS Act (H.R. 3849), most of which, however, have not yet been fully specified. Thus, the DMA represents the currently relevant approach of a concrete design, especially for messaging services or NI-ICS.

According to the DMA, the IOP obligation in relation to NI-ICS is primarily intended to increase market contestability by allowing to overcome strong network effects (cf. also Chapter 3.2.1). With regard to the addressed gatekeepers, which usually operate as a multi-product ecosystem, the switching costs for end users, which are increased in a special way by corresponding integration and interconnection advantages, and thus increased market entry barriers for alternative providers are also mentioned (cf. also Chapter 4.1.3.5).

According to internal documents, various options were initially discussed (Europäische Kommission, 2022a). In addition to an IOP obligation for social media services of the gatekeepers, a complete standardisation measure at the messenger level was initially abandoned. Instead, a comparatively mild approach is found in the final version, which at the same time is intended to preserve as much freedom of choice as possible for end users and alternative providers, possibilities for differentiation and a high degree of data protection. It is an asymmetric obligation in which appointed gatekeepers must grant other providers free of charge access to NI-ICS operated by them. However, this must only be done upon active request by another provider, so that for them any connection is based on complete voluntariness.

In addition, the access obligation is limited to basic features, which will be expanded in a staggered manner over time. Initially, this applies only between individual users for text messages, voice messages, exchange of files, especially photos and videos. Two years after classification as a gatekeeper, the same feature is to be guaranteed for group chats, and after four years, voice and video calls are to be added.

The text of the law places a high value on maintaining data security and data protection. This includes a data minimisation requirement in which the collection and exchange of data must be limited exclusively to the level necessary to ensure effective IOP. The same level of protection offered to own users must also apply to IOP with external providers. This explicitly includes the preservation of end-to-end encryption, if applicable.

In order to facilitate possible enquiries for third-party providers, gatekeepers are also to provide reference offers that explain in particular the necessary technical requirements and details for an IOP connection. Here, too, the topics of security and end-to-end encryption are explicitly mentioned. These may also require an exceptional extension of the access period, whereas access should normally be granted within three months of the request. In general, however, behaviour that softens the IOP or makes it more difficult for requestors, such as discriminatory conditions or unjustified technical measures and copyright claims, is prohibited.

In addition to the voluntary decision for alternative providers, the preservation of freedom of choice for users is also emphasised. End users of both the gatekeeper and the requesting provider should remain free in their decision to use the features interoperably, e.g. to actually be reachable (and discoverable) for users of the respective other provider.

Furthermore, another question that has not been conclusively resolved in the general case of IOP obligations is the nature and pricing of access, while the DMA requires access to NI-ICS features to be free of charge. On the question of appropriate payment, in the general context of mandatory access to digital platforms, the "FRAND" mechanism is often discussed as a possibility (Matos & Torres-Sarmiento, 2022), which has mainly been established in the area of patent payments. Particularly in the case of asymmetrical obligations vis-à-vis "dominant" providers, free access is sometimes demanded or provided for (Heim & Nikolic, 2019). This is also the case in the IOP regulation for gatekeepers in the DMA further discussed below.

To what extent the overall rather limited regulations may alleviate concerns about horizontal IOP in particular (cf. inter alia Chapter 3.3 & 4.1.4) as is the case in the messenger sector, but may also bring problems of their own, will be discussed in the following Chapter.

## 4.4 Assessment and recommendations

### 4.4.1 Economic and technical assesment

Not least in the run-up to potential IOP obligations in the DMA, a number of concerns have been raised about an IOP obligation for messaging services in particular and for horizontal obligations in general (cf. Chapter 3).

Here, the main warning was against overly comprehensive regulations, both in terms of the group of addressees and the scope of features, which could weaken opportunities for differentiation and distinction and thus also incentives for innovation. Concerns about too few opportunities for product differentiation are expressed, among others, by the Monopolkommission (2021) in its 12th sector report on the telecommunications market as a main argument against a binding horizontal IOP obligation in the market for messaging and video services. In its analysis, it also refers to the survey of the Bundeskartellamt (2021) of 44 companies in the industry. It shows that the existing competition on the horizontal level is already perceived as intense and that differentiated product features such as hand raising, emojis in the conference chat, content sharing, importing visual backgrounds etc. are important competitive factors. By homogenising services through horizontal IOP, customers would be less inclined to switch between different providers.

Since the decision of the DMA is initially limited to the basic feature of the simple exchange of messages and files, a greater possibility for differentiation via various additional features is obtained here. However, this also leads to a conflict with the original goal of reducing company-specific network effects, as these are thereby retained within the framework of these additional features. On the other hand, the innovation incentive to stand out through exclusive features or not to fall behind in comparison to competing providers is maintained. An example from the past may be the end-to-end encryption on WhatsApp as well as emoji reactions for messages, which services such as Signal or Beeper have been offering for a long time and were only introduced in a recent update of WhatsApp. However, the extent to which such and other features may also become "basic features" over time remains a question that cannot be answered unequivocally, especially in the dynamic environment of messaging services.

There is also the risk that planning is overtaken by the dynamic development of the market and that necessary adjustments become all the more costly later on. As a result, development can be inefficient if a technical foundation is created at the beginning that does not allow for certain functional extensions later on. Especially such complex systems then bear the risk of expensive amendments or the need to renew the substructure.

On the other hand, IOP can also make innovations in the core area of the functional scope more difficult. For example, the introduction of a higher level of encryption or self-deleting messages would require an update of the IOP interface and could therefore not be carried out decentrally by the interoperable messengers. Even in the status quo, there is a lack of agreement on the definition of actually “basic” features. For example, the Internet Society (2022) implies that not only end-to-end encryption should constitute such a basic feature, but points out that agreement also on the detailed technical design of this would be necessary in order to establish IOP. Specifically, it gives the example of whether pending messages are still transmitted if the authentication key of the conversational partner changes halfway through. Since this is handled differently by Signal and WhatsApp, for example, it is not possible to speak of a uniform "basic feature" and IOP cannot be achieved without reaching an agreement here. However, this would require one of the two developer sides to give up its actually preferred approach in the trade-off between security and usability (Internet Society, 2022).

Mandatory IOP standards could also be misused as a strategic barrier to market entry and thus even protect already established providers from the entry of innovative competitors. First indications of this danger can be found in the survey of 44 providers of messaging and video services of the Bundeskartellamt (2021). Here it is warned that especially smaller providers may be disadvantaged in their competitiveness due to the high technical complexity of standards, as larger providers could prevail in standardisation and could thus even cement their dominance. In the standard-setting process, it is therefore necessary to assess how realistic market entry is in order to avoid the creation of barriers to entry. This aspect is mitigated in the DMA by the asymmetric obligation exclusively for gatekeepers and the voluntary nature for alternative market participants as well as by the provisional renunciation of standardisation in the narrower sense.

However, especially with regard to effective end-to-end encryption, complete (de jure or de facto) standardisation is considered necessary on the other hand to ensure secure encryption under IOP, as also shown by the assessment of the experts for encryption technologies interviewed by WIK-Consult (cf. Chapters 4.2 and 4.3). This implementation approach would therefore, if consistently enforced, make the introduction of IOP for previously end-to-end encrypted features impossible or, alternatively, jeopardise existing security levels. However, a re-assessment and the subsequent setting of standards will be reserved in the DMA and would then be subject to the corresponding risks that standardisation processes can generally have (cf. also Chapter 3.7).

First, however, according to Andreas Schwab, rapporteur of the European Parliament, it is envisaged that the gatekeepers will offer APIs for competitors in order to be able to enable interoperable messaging features (Europäische Kommission, 2022a; Lomas, 2022). In this asymmetrical arrangement, other providers are therefore neither obliged to open up to gatekeepers nor to each other. Only the gatekeepers are obliged to establish a bilateral connection to the requestor, if any. The simplest option will most likely be public versions of proprietary interfaces (APIs) and corresponding functionality that gatekeepers already use in their own systems. However, as mentioned above, this technical implementation of IOP is not compatible with previously end-to-end encrypted features. A voluntary agreement on open technical standards such as Matrix or MLS would be possible in principle, but is currently not to be expected. This also means that, in case of doubt, interested competitors would have to support a number of different APIs and associated messaging protocols per gatekeeper and users might have to accept restrictions in security.

In view of the potential inefficiencies due to the staggered implementation of IOP for certain features and the potentially necessary simultaneous use of various protocols, it can also be stated here that the resulting cumulative costs, both for providers and in monitoring, could probably even exceed the costs of a systematic complete standardisation. However, reliable planning and consideration of features to be included in the future would also be necessary in such a process in order to avoid undesirable developments in the path-dependent process, which is also afflicted with the usual problems of standardisation processes (cf. Chapters 2.1.3 and 3.7.2). In any implementation of IOP, both gatekeepers and competing providers must ensure that all consumers remain free in their decision to be contacted by users of the other service, even in the case of an agreement between providers. This also addresses the concern that access to (meta-)data of customers of other services could further strengthen gatekeeper positions. This is additionally to be prevented by the simultaneous "ban on personal data combination"

(Art. 5(2)(b)), by which, for example, the use for targeted advertising requires the explicit consent of the users for such use. In practical implementation, however, the logistical and technical complexity of these aspects could lead to constellations that are difficult to manage for users, which in the worst case could even discourage the use of smaller, alternative services.

Horizontal IOP could theoretically help to reduce market concentration in messaging services. However, studies show that consumers in Germany use several services simultaneously despite network effects (see e.g. Bundesnetzagentur, 2020, as well as Chapter 4.1). This is due to product differentiation, innovation, low costs of multi-homing and a heterogeneous set of contacts, suggesting that IOP is not necessary or could even lead to a negative effect as described above. Parts of the network effects can be realised on the part of a user through multi-homing via the simultaneous use of several services. From the point of view of providers who differentiate their services in terms of data protection or on the basis of enhanced security features, this horizontal IOP is sometimes not advantageous, as unique selling points are not retained (also cf. Bundeskartellamt, 2021).

In principle, IOP makes it easier to switch to smaller providers, but at the same time lowers the incentive to actually do so (cf. Bourreau et al., 2022). If a contact with "bargaining power" decides to use only provider B, without IOP all his contacts who still want to reach him would also have to install provider B's service and use it for this particular communication. In the interoperable case, all contacts can easily remain exclusively with provider A and still be able to communicate with their contact or users from provider B. On the other hand, it is also made easier for those who switch to provider B to completely uninstall provider A, as they can continue to contact its users. Thus, (partial) IOP basically has both a pro-competitive effect (by reducing firm-specific network effects) and an anti-competitive effect (by reducing multi-homing) and it is unclear ex ante which of the effects ultimately dominates (cf. Bourreau et al., 2022).

### 4.4.2 Legal assessment

The regulations on IOP for messaging services provided for in the DMA are noticeably aimed at achieving a balance between different regulatory objectives. In particular, a high level of data protection is to be guaranteed and concerns regarding data security are to be taken into account. This is expressed, for example, in Art. 7(3) DMA, which emphasises that the level of security, including potentially existing end-to-end encryption, offered by the gatekeeper to its own users must be maintained in the interoperable services. If enforced consistently, this would imply, due to the discussed technical incompatibility of IOP and end-to-end encryption, that IOP cannot be established or does not have to be established by the gatekeeper for services or features that have already been using end-to-end encryption before, unless the connecting provider fully implements the gatekeeper's protocol or standard.

The regulation can be understood to mean that maintaining the level of security is a prerequisite for opening up the messaging service to other providers. This interpretation is supported by Art. 7(4) DMA. According to this, the gatekeeper must publish the technical details and general conditions for enabling IOP "including the necessary details on the level of security and end-to-end encryption" in the reference offer to be published by the gatekeeper. Thus, IOP can only be granted to providers who are able to meet these requirements. This caveat could be used by gatekeepers to make it more difficult to demand IOP, citing security concerns. However, recital 64 of the DMA makes clear that the content of the reference offer can be reviewed by the EU Commission (in consultation with BEREC, if necessary) to determine whether it meets the DMA's requirements for enabling IOP.

In this context, the question that needs to be clarified in particular is what requirements are to be placed on the "preservation" of the security level. Insofar as the gatekeeper provides end-to-end encryption for its users, it will be possible to demand as a minimum requirement that the other provider also guarantees corresponding encryption. However, it would probably be too far-reaching to demand identical security precautions in technical terms. In the sense of an effective IOP, equivalent measures to ensure data security should be sufficient.

Art. 7(5) DMA provides that the gatekeeper is obliged to comply with a "reasonable request" for IOP within a period of three months after publication of the reference offer. This raises the question of what requirements are to be placed on a "reasonable request". If interpreted narrowly, Art. 7(5) DMA could be understood as a “prohibition of chicanery”. Accordingly, only applications that are manifestly abusive could be disregarded as "unreasonable". However, it would also be conceivable to take economic aspects into account when assessing reasonableness, such as the question of whether the IOP in the specific case can only be established at disproportionate cost. In the interest of effective IOP, a narrow interpretation of Art. 7(5) seems preferable.

As already explained in more detail above, ensuring the required level of security, including end-to-end encryption, is likely to be a complex challenge from a technical point of view. It therefore seems appropriate that Art. 7(6) DMA allows the EU Commission to extend the deadlines for enabling IOP set out in Art. 7(2) to (5), provided that the gatekeeper concerned demonstrates that this is necessary to ensure the required level of security. Some of the experts on encryption technologies interviewed by WIK-Consult estimate the implementation or development effort for the use of a uniform standard to be up to 5 years.

Art. 7(7) DMA requires that the users of the gatekeeper and the other provider "remain free" to decide whether they make use of the IOP of the basic features. Accordingly, the IOP enabled between messaging services under Art. 7(5) DMA must not be imposed on the respective users. Art. 7(7) DMA does not contain any further specifications on how the users' freedom of choice is to be ensured. In particular, the question arises whether providers must provide an opt-in model or whether an opt-out model also satisfies the requirements of Art. 7(7) DMA.

Since the establishment of IOP is associated with the processing of personal data by the other provider, an opt-in model is likely to be necessary for data protection reasons alone, even if this also poses considerable challenges for practical implementation from the user's perspective, e.g. in the handling of group features or for consent requirements for messaging services that may be added gradually over time. However, the reference in Art. 7(8) DMA that the collection and exchange of data for the purposes of the IOP must fully comply with the requirements of the GDPR and the ePrivacy Directive also speaks in favour of a prioritised data protection view. The decision for or against the IOP must therefore meet the requirements for a "voluntary" decision within the meaning of Art. 7 GDPR. Insofar as the IOP covers several basic features, a differentiated selection and deselection of individual features would also have to be made possible. If the user decides to use the interoperable basic features, the collection and exchange of data must be strictly limited to what is necessary for the establishment of IOP (Art. 7(8) DMA). This is in line with the principle of data minimisation enshrined in Art. 5(1)(c) GDPR.

Art. 7(9) DMA supplements the above regulations with a general reservation clause. According to this, gatekeepers are not prevented from taking measures to ensure that third-party providers do not jeopardise the data protection, integrity and security of messaging services. The condition is that these measures are "strictly necessary and proportionate". This reservation clause should make it possible, for example, to later restrict the IOP initially granted if reasonable doubts arise about the third-party provider's guarantee of data protection and data security. Art. 7(9) does not regulate a procedure for such a suspension of IOP, but only requires that the measures be "duly justified". For reasons of proportionality, however, it is likely to be possible to require that the gatekeeper first demand a remedy from the third-party provider if security problems arise. A permanent termination of the IOP can only be considered as ultima ratio.

### 4.4.3 Recommendations

Due to the long list of risks of horizontal IOP obligations, it is generally to be welcomed that the DMA is taking a cautious approach in the area of messaging services. Not least given the IOP obligations now envisaged in the DMA's final decision, the aspect of end-to-end encryption is at the centre of discussions and often seems to represent a dividing point in the final assessment of corresponding obligations. The IOP obligation for messaging services has raised serious concerns in the industry about whether it would undermine the end-to-end encryption that some messaging services have put in place, as well as other security and anti-spam measures.

As described above, the final decision of the DMA for the time being only makes moderate requirements by, among other things, dispensing with symmetrical obligations and full standardisation for the time being and placing special priority on maintaining a high level of security and freedom of choice for users. It should first be noted that from a technical point of view, there is no clear or uniform definition of which aspects and attack models are actually understood by the term "level of security", e.g. in addition to content encryption, this can include user authentication, (lack of) trust in key-managing entities or the accumulation of metadata. Potential "attackers" vary from employers, ex-partners, corporations to own or foreign governments (Muffett, 2022).

This also applies to "end-to-end encryption" itself. Depending on the application and its value proposition, user (base) and infrastructure, in some cases very different "ends", attack and attacker models can be relevant, which also imply different trade-offs at the technical level (cf. Burgess, 2022; Muffett, 2022). Although uniform technical solutions are conceivable in principle at an abstract level, they reach their limits in detail and practical implementation, as experts interviewed by WIK-Consult also confirm. Corresponding compromises and an expansion of the parties and actors involved therefore ultimately also imply an expansion of possible points of attack and thus, in case of doubt, cause a drop in security levels.

Especially for the preservation of any end-to-end encryption in combination with a secure key exchange, the combination without a (de jure or de facto) agreement on an existing or new standard seems to be technically almost impossible in practical implementation. In the case of IOP regulations that do not explicitly provide for standardisation or are introduced without coordination on a uniform standard, preservation of end-to-end encryption would ultimately not be guaranteed, as also confirmed by the experts on encryption technologies interviewed by WIK-Consult. The implementation costs for such a uniform solution would be high. According to one of the experts, the effort in this case would be comparable to the development of a new joint interoperable messenger platform and would amount to about 5 years. According to another expert, standardisation including encryption at the basic level of bilateral messages could be achieved in 2-3 years in the best conceivable case. Even this, however, presupposes that the market players involved have the fundamental will to agree on a common standard.

Some aspects of the fundamental technical challenges of end-to-end encryption, especially for implementation in an interoperable environment, have already been discussed in Chapter 4.2.4. The Internet Society (2022) also expresses criticism regarding a potentially fundamental incompatibility of messenger IOP and end-to-end encryption. Alternatively, alternative providers or entrants would have to fully adopt the standards of gatekeepers and would thus be forced further into dependence on proprietary systems. Also from the white paper by WhatsApp (2021) discussed in Chapter 4.3.1.2, it is clear that end-to-end encryption via interfaces is at least not trivial, even within a corporate group. This impression is reinforced by media reports according to which Meta is only making limited progress with the announced integration of its services and the group-internal IOP due to the complexity of the technical expansion (Ahmed, 2021).

Active proponents of IOP regulations for messaging services also recognise the importance, but also the difficulty, of agreeing on messenger IOP and the best possible encryption, and concede that an adequate implementation, especially one that is encryption-compliant, could take "years" longer than currently envisaged in the DMA (cf. e.g. Stoltz et al., 2022). Alternatively, a proactive, informed renunciation of end-to-end encryption on the part of the user would be conceivable (Le Pape, 2022). However, in view of the problems already observed in the context of the GDPR and cookie banners with regard to consent given in inflationary amounts, a drop in the average security level for users would have to be feared (Utz et al., 2019).

Accordingly, the deadlines and the timeframe envisaged could be too tight, especially for group messages, whose encryption is already associated with additional hurdles in scaling in the non-interoperable case (cf. Chapter 4.2.4). Article 7(6) already partly takes this uncertainty into account and should initially be used generously. The focus on consumer aspects such as the preservation of encryption and data minimisation should also be maintained in practical implementation and enforcement. Here, however, there is the difficulty of distinguishing between valid technical defence arguments and possible circumvention strategies. In order to assess the extent to which an encryption- and data protection-compliant implementation of IOP is actually technically feasible and can be implemented within an appropriate framework, various central and independent organisations should therefore be involved. Likewise, the transparency and reporting obligations demanded elsewhere in the DMA should also be specified for this area.

In addition to the APIs offered by the messaging services themselves, there are also intermediaries such as Tyntec, which provide aggregated access to several APIs. Via these, any end customers can then be contacted via their respective preferred service (Tyntec, 2022). Here too, however, it must be taken into account that the messages only have transport encryption and the service provider can therefore also view the messages unencrypted.

The aspiration that users' freedom of choice should not be restricted by mandatory IOP measures should also be maintained in practice (cf. personal digital sovereignty). Users should be given clear and comprehensible control over who is allowed to contact them, when and how, and what data is used within and outside the service used. To ensure this, opt-in solutions should be required for consumers (also cf. Internet Society, 2022). In addition, control and transparency mechanisms may be necessary with regard to data outflows and the further use of data, unless this can be solved technically by design.

Although the DMA contains a proviso clause and requires "reasonable" applications from third-party providers (cf. Chapter 4.4.2), however, clarification or even regulatory review and selection procedures might be necessary to effectively prevent abuse (cf. inter alia Barczentewicz, 2022). In principle, providers of spam and mass messages would come to mind, who could use an IOP request as a loophole and possibly make renewed requests under changing names and company constructs. The identification of spam actors at the user level in decentralised systems can also be made more difficult, as the example of the email ecosystem shows.

Overall, the danger of the IOP obligations of the DMA is possibly rather that the regulations might not have the expected practical implications for the time being due to a lack of demand by competing services and the lack of adequate technical implementation possibilities. On the other hand, there is no reason to fear an excessive standardisation of services or a drop in the general level of security for the time being, as long as the prioritisation of end-to-end encryption, for example, is also maintained in practical implementation. These provisions for the simultaneous preservation of data protection and data security should indeed be given priority in practice over an IOP objective itself in case of doubt. Existing regulations such as the GDPR must also not be compromised in the process.

Another probably unintended effect could be that smaller competing providers do not take up the possibility of IOP (cf. the actively expressed lack of interest by the providers Signal and Threema, Chapter 4.1.4), but that it could also be activated by gatekeepers among themselves. Whether this possibility would be intended or possible remains unclear and the possible effects are complex. For example, Meta or Alphabet could demand access to Apple's iMessage, which would on the one hand weaken Apple's competitive position and exclusivity, but could also, among other things, increase data-related concerns against Meta and Alphabet.

Multi-messengers cannot be subsumed under an IOP approach in the narrower sense, but they can serve to further reduce the costs of multi-homing through an integrated user interface without limiting the data security of users by softening end-to-end encryption if decryption is implemented directly on the end-user devices. The fact that these applications will be enabled more broadly in the future through IOP regulations with corresponding documentation, as well as the exclusion of the prevention of corresponding access possibilities, appears to be a goal-oriented practical solution approach.

# 5 Conclusions and outlook

The study provides an overview of the complex issues raised by the concept of IOP and a possible obligation to establish it, with a focus on the context of today's internet and platform economy and online communication services. It presents the possible effects of IOP regulations on competition and innovation as well as on digital sovereignty and examines the potential need for such regulations. The focus is particularly on digital services from the field of communication services as well as the platform economy.

## 5.1 Interoperability concepts

Already in the understanding of the term and with regard to the different concepts of IOP from a technical, legal and economic perspective, a broad, partly inconsistent picture emerges. Especially in the economic and legal context, the term IOP and related concepts such as compatibility and portability are used in the same breath or even explicitly synonymously. Other definitions emphasise not only the exchangeability of data and information between systems, but also more concretely their usability and an associated intersection of functionality. The established subdivision into data IOP and protocol IOP is aimed at these different understandings. From partial IOP, where only some or a subset of all features are usable by users of other applications or systems, to "full protocol IOP" with a deeper level of integration and standardisation, IOP often presents itself as a continuum.

As a distinguishing working definition between compatibility and IOP, the following understanding was developed in the study. Compatibility is understood as the unimpeded operation and consistent interchangeability of components, applications and systems, especially within one environment. IOP is understood as the cooperation and combinability of components, applications and systems, which can also be located in different environments. In the context of digital markets, an environment can be understood as the technical sphere of influence or the ecosystem of a company.

Furthermore, IOP goes beyond selective, usually one-sided, (data) portability and distinguishes itself from this through a continuous, usually two-way, exchange of data. In addition to this two-way IOP, there are also one-way forms of IOP, such as so-called adversarial IOP through reverse engineering or the sharing of external media content on social media platforms.

In a technical context, the terms asymmetric and symmetric IOP are also used to distinguish between one-sided and two-sided IOP. The term asymmetric regulations is also used in a legal sense. For example, the IOP obligation for so-called "gatekeepers" provided for in the DMA is such an asymmetric obligation, whereas a symmetric regulation would directly apply to all market participants.

If a platform grants access to (complementary) third-party suppliers at upstream and downstream stages of the value chain, this is referred to as vertical IOP. It should be noted that symmetric IOP is not possible in the case of vertical competition, as the focus here is on access to an essential part of the value creation under the control of a company.  In the case of similar (substitutive) services that are in direct competition with each other, one speaks of horizontal IOP. In the case of horizontal competition, it must be clarified whether an IOP obligation should only apply to certain companies which have a strong market position (e.g. financial strength, number of users, etc.), or equally to all providers of a certain type of service (cf. also Table 3-3).

Depending on the competitive situation (horizontal or vertical), different economic effects must be taken into account or weighted accordingly in the assessment. However, it can also be stated that especially in the context of platforms and due to the development of multi-product ecosystems, the boundaries between horizontal and vertical company relationships are becoming increasingly blurred. Primarily horizontally competing services often also have various types of vertical relationships, which means that competition at other market levels can play an important role.

## 5.2 Interoperability and interoperability obligations in the platform economy

The basic desired effect of IOP from a welfare perspective is the dissolution of firm-specific network effects at the horizontal and also vertical level, so that resulting utility gains from the size of the network benefit consumers of all interoperable services. Consumers should be able to switch providers more easily, options to choose from should be created at the horizontal and vertical level through innovation, and price and quality competition should be intensified. In doing so, IOP can establish competition *in the* market and prevent the tipping of markets or mitigate existing market concentration. However, the possibility and actual level of multi-homing (the parallel use of different similar services by users) limits the relevance and necessity of IOP obligations, as users can also benefit from different features and access to different users in this way.

Digital sovereignty for consumers in the form of self-determined action can be strengthened by IOP if it reduces lock-in effects and strengthens freedom of choice. However, choice can be provided by horizontal competition and substitution possibilities, as well as by modular choices at the vertical level, which enable a mix-and-match approach, i.e. the combination of complementary products and services from different providers at different levels of the value chain.

The particular relevance of data is a special feature of platform services and ecosystems, that are characterised by data-driven learning effects. In this context, companies use user data for product improvements and/or increased marketing opportunities, both in continuous use within a service and especially in linking across different services, products, market levels and contexts. Therefore, the provision and use of one's own (personal) data is taking on an increasingly important role for users. For self-determined action, the greatest possible transparency and control are necessary here as to which data is collected, used or passed on, when and by whom. IOP and thus the interaction of more actors can fundamentally make this more difficult. Obtaining consent transparently and explicitly when data is shared with other services can achieve this, but it also increases complexity for consumers. In an interoperable network, providers may have access to metadata (details of sender and recipient of the information, time of interaction, location of users, etc.) with which users have no direct business relationship. Thus, in an interoperable environment, the extent of data processing by third parties may be beyond the direct control of users.

But also classic direct and indirect network effects continue to play a fundamental and growing role in the context of multi-sided platforms and also one-sided communication networks. These effects usually constitute the core argument for a possible introduction of IOP obligations. Even if network effects can foster the effect of market tipping and thus a monopolisation tendency in itself, and some firms even seem to strive for ever larger self-contained ecosystems ("walled gardens"), it is unclear whether this (causally) leads to market concentration and whether this is actually harmful for welfare and/or consumer surplus in each respective case. Thus, for an overall assessment of possible IOP obligations, a number of other, possibly moderating or counteracting, factors have to be taken into account.

Especially for digital services, the immediate costs of multi-homing can often be low (e.g. installing another app on the existing smartphone) and primarily non-monetary (e.g. registration, learning and other transaction costs). Since IOP can significantly weaken the incentive for multi-homing, caution is advised for respective IOP obligations from this perspective. However, if substantial costs of multi-homing can be avoided through IOP, this may well be welfare enhancing. For example, multi-homing between different mobile operating systems does not usually take place because it would require expensive hardware, in this case in the form of another smartphone.

If too much standardisation is required to achieve IOP, IOP can limit product variety and innovative differentiation opportunities in horizontal competition, also to the detriment of consumers and innovative companies. Too much homogenisation of features may even make customers less inclined to switch providers and ultimately reduce consumer benefits through reduced product variety. This results in a trade-off for the definition of core features to be made interoperable. If the innovation is steered into product dimensions that are not attractive for users, there is the aforementioned problem of homogenisation. If the innovation is steered into product dimensions that are relevant for users and induce demand effects, the goal of reducing company-specific network effects may be thwarted and the preceding definition of "relevant" core features may also be called into question.

At the vertical level, however, IOP can create planning security and demand potential on upstream and downstream markets and thus promote innovations by complementary providers. Here, however, especially with regard to the platform economy, there is the problem of the prevalence of vertically integrated services and products. IOP that is initially provided voluntarily can be used strategically and discriminatorily to damage competitors in downstream markets, e.g. by initially generating attractiveness in the early growth phases of platforms by opening them up to complementors and user groups of other services. Depending on market shares and the possible integration of own offers, interfaces are then sometimes closed again in the later course or only offered unilaterally, e.g. in order to achieve a strategic control of the flow of attention. It can also happen, especially under IOP, that (dominant) platforms or providers copy the interoperable products or features of external companies and integrate them into their own offerings ("sherlocking"), so that smaller companies may not be able to differentiate and maintain themselves in the market and the dominant position is ultimately even strengthened. In principle, however, a high level of available voluntary IOP tends to speak against an ex ante obligation, while a high level of adversarial IOP or even active attempts to prevent it can be an indication of a necessary intervention.

In addition, the costs incurred for the introduction of IOP, including adaptation, negotiation and maintenance costs, should be taken into account, which may even make market entry more difficult rather than easier for small companies. The process of standardisation can also disadvantage small and especially potential suppliers if it is shaped by existing, dominant companies and can even cause collusion risks and "patent hold-up" if companies can introduce their own technologies and patents into standard definitions in return for licence payments. In addition to the incumbents, other stakeholders such as potential competitors, consumer organisations and independent technological expertise should also be involved. Furthermore, access obligations also give rise to regulatory costs of monitoring and enforcing the obligations, as it must be assumed that the access obligation will be strategically undermined, e.g. by deliberate technical disruption of the IOP interfaces.

## 5.3 Interoperability for number-independent interpersonal telecommunications services

The study continued to deal in particular with the market segment of online communication services and an IOP obligation in this area. The focus is on online communication services which, according to the test criteria discussed, represent a relatively homogeneous product whose providers are primarily in horizontal competition. In the German and European market in particular, there is a strong market concentration on the Meta group, which encompasses the messaging services WhatsApp, Facebook Messenger and Instagram Messages and thus also exhibits varying degrees of vertical integration with the social networks Facebook and Instagram and the Meta group as a whole.

In the broader market segment, there is also a diverse field of different forms of organisational structure and monetisation. Telegram, for example, continues to test different approaches such as a freemium model. Some smaller services or the corresponding apps are offered against direct one-time or regular payments (Threema, Element). Not only with regard to legal definitions of NI-ICS, which aim at a service provision "*normally provided for renumeration*", the handling of other forms of financing often remains unclear. While the Meta group as a whole mainly generates its revenues from advertising, Signal is backed by a non-profit/donation-based approach. In the case of iMessage, no revenue is generated by the service itself either, but it serves to increase the attractiveness and exclusivity of the Apple ecosystem, which is characterised mostly by revenue in the hardware and service area. It is therefore necessary to include services with forms of indirect revenue and to assess the incentives and competitive effects associated with each of them. Especially for providers with direct monetisation, the possibility of differentiation is essential, while the exclusivity of iMessage through the generation of customer lock-in and company-specific network effects is relevant above all in the upstream competition between operating and hardware systems. Business models based on attention and/or data from users can even profit through IOP with other services and the metadata created in the process.

Even if a messaging service does not in itself fulfil the classic definition of a platform in the economic sense due to its restriction to direct network effects, in practice this market is nevertheless characterised by "real" platforms, as various forms of indirect network effects can also take on an essential role through embedment in platform ecosystems. The movement towards a prevalence of ecosystem messengers is taking place from two directions, especially internationally. On the one hand, originally single-purpose messengers are becoming platforms and/or ecosystems themselves through the addition of features, types of monetisation and company orientations. On the other hand, existing multi-sectoral ecosystems are expanding their portfolios to include messenger features.

With regard to the classification of individual services as NI-ICS (whether as obligated party or as claimant to IOP), legal clarity still needs to be created through administrative practice in some cases. For example, Telegram represents a borderline case between individual and mass communication, whose channel and open group features are to be classified as "public" under the DSA. Bilateral communication and private groups, on the other hand, represent classic messenger features.

The boundaries between open (mass communication, e.g. social media) and closed (individual communication) user groups are also often blurred. In both social networks and messaging services, features can be observed that enable closed user groups. Conversely, the exchange of direct messages is also possible between individual users in social networks. Even the criteria of an interactive exchange or a reply option and the restriction to a finite number of persons from the NI-ICS definition of the EECC do not always lead to a clear classification, as the example of Telegram shows. Also excluded from the legal definition, e.g. under the EECC, is communication that is only a "minor ancillary feature" and is intrinsically linked to another service. Apart from clear cases such as the chat feature of an online game, however, there may also be borderline cases or perspective circumvention possibilities here, e.g. in the case of Instagram Messages. As the usage patterns show, the feature is even used more frequently than many dedicated messengers in Germany, for example.

With regard to multi-homing, the market presents itself with a differentiated picture. Multi-homing is relatively easy due to services that can often be used free of charge or at low cost, and at the service level in Germany, for example, about 75% of users use at least two online communication services, while on average almost four services are used. At the enterprise level, these numbers are reduced to still 61% of users and just under three services on average. The dominance of the Meta group, which encompasses the services WhatsApp, Facebook Messenger and Instagram (Messages), is also reflected in the fact that 80% of users in Germany use at least one of these three services. Services from other companies are only used by up to 30% of respondents (Microsoft services) or far fewer (other services). Empirical results after the changes to WhatsApp's privacy policy also show that although alternative services were increasingly installed and initially used, only 0.5% of users actually left WhatsApp and uninstalled the app.

Nevertheless, it can be stated that multi-homing in the form of trying out and using several services in parallel is relatively easy to do in this market on the one hand and is thus also correspondingly widespread among a majority of users. Providers such as Signal were able to enter the market and increase their number of users to a relevant extent. In addition, a high installed base of multi-homing allows customers to switch even faster from one messenger to another and thus disciplines the market power of the dominant company. Since IOP can reduce the incentive for multi-homing, the worst that could happen here is an inhibition of exploration and diffusion of new services, as well as less discipline of market power. Even if WhatsApp or Meta's services remain by far the most widespread (not least due to their acquisition strategy), there is (potential) competitive pressure, which has presumably contributed, among other things, to WhatsApp's introduction of end-to-end encryption. Ultimately, the focus of all IOP regulations is a potential market failure in terms of functioning competition in the market, which could be overcome by establishing IOP. If, as in the case of messaging services, the level of multi-homing is comparatively high and the costs of multi-homing are low, a relatively low welfare loss for consumers can be assumed to begin with if an interoperable exchange across providers is not possible. Moreover, multi-homing preserves competition for the market.

Especially in the run-up to the DMA, there were various corresponding concerns about a proposed IOP obligation. In particular, market participants and observers were critical of a symmetrical obligation affecting all companies, as this would lead to the aforementioned excessive homogenisation. In particular, it was feared that alternative, data protection-conscious providers could lose their ability to differentiate and that a "lowest common denominator" would be reached with regard to the general level of security and data protection. The current decision of the DMA first addresses these concerns by imposing an asymmetrical obligation exclusively on dominant providers, so that all other providers remain free and independent in their decision to participate and thus in the design of their functionality. Signal and Threema, for example, already announced that they would not make use of the IOP connection to services such as WhatsApp and iMessage.

Since the decision of the DMA is initially limited to the basic feature of the simple exchange of messages and files, a greater possibility for differentiation via various additional features is also obtained here. However, this also leads to a conflict with the original goal of reducing company-specific network effects, as these are thereby retained within the framework of these additional features. On the other hand, the innovation incentive to stand out through exclusive features or not to fall behind in comparison to competing providers is preserved.

Although a more comprehensive standardisation would also require reliable planning and consideration of yet-to-be-included features over time, the costs of a piecewise and staggered implementation could possibly be higher in the long run due to inefficiencies in development when adaptations are then required at a later point in time.

On the user side, the freedom to decide whether or not to use interoperable features, depending on the provider, shall also be guaranteed. Users should be given clear and comprehensible control over who is allowed to contact them, when and how, and what data is used within and outside the service used. According to the legal assessment, an opt-in model is likely to be required for legal (data protection) reasons, but this has not been explicitly demanded so far. In the case of a resulting opt-in obligation, the achievement of the goals for IOP will be further diminished, since not all users will make use of the option and therefore company-specific network effects will once again remain. In addition, considerable challenges are foreseeable for the practical implementation and for the complexity from the user's perspective, e.g. for the handling of group features or for consent requirements for providers that may gradually be added over time.

It is true that the wording of the decision places great emphasis on the preservation of existing data protection and security levels and, if applicable, end-to-end encryption, which should also be preserved in the case of an interoperable connection and whose preservation should have priority. In the ongoing discussion, however, it is often questioned whether the technical requirements for an efficient exchange of features and data in the sense of an IOP for messaging services are achievable at all. The technical complexity of messengers and in particular of end-to-end encryption, which many sides are striving for, therefore seem to be developing into a neuralgic point. Despite comments to the contrary, the planned implementation in the DMA by means of APIs will probably not be sufficient to guarantee IOP, genuine end-to-end encryption and secure identity and key management at the same time. The complexity of all these undertakings increases from the core feature of 1:1 text messages alongside the range of features to be covered in addition (group chats, file attachments, audio/video calls, etc.). In addition, the term "security level" is very comprehensive and is not defined with sufficient precision, neither in theory nor in practice. Opening interfaces and establishing IOP with third parties generally implies a lowering of any security level, as this creates additional possibilities for attack vectors and third parties involved have to be trusted (e.g. with regard to user authentication and key exchange).

It is therefore questionable whether the approach pursued in the DMA to establish IOP without lowering the level of data protection and security compared to the status quo can be implemented at all. According to expert assessments, end-to-end encryption can only be achieved through complete (de jure or de facto) standardisation, which rules out the planned interface/API approach in particular. The establishment of such a standardised interoperable environment could again take about 5 years according to one of the experts interviewed by WIK-Consult. Another expert interviewed mentions 2-3 years as the best possible case for a standardised encryption agreement for simple bilateral text messages. The technical complexity and the requirements for standardisation, but also for computing capacities, also increase significantly if not only text messages but also real-time audio and video calls are to be encrypted.

A more short-term solution could in principle be the mandatory introduction of an existing standard (for gatekeepers), with a correspondingly high implementation effort for the gatekeepers concerned. Due to the aforementioned diversity of different standards, protocols, application areas, value propositions and attack models, however, market interest, at least from existing providers, would also be questionable here. A complete standardisation (with the participation of the gatekeepers and entrants) with the aim of also covering existing proprietary features (which are currently not covered by open standards) or future features of both parties is an extremely complex and lengthy procedure, to which the implementation costs would need to be added afterwards.

As an alternative to formal standardisation or voluntary use of a uniform standard, competing providers would have to directly adopt the existing protocols of the gatekeepers, which would thus be elevated to de facto industry standards. It is doubtful, however, that such an approach fosters competition and innovation or that such systems are at all attractive for small providers. Signal and Threema have already rejected such systems. There is thus a danger that such projects will lead to IOP systems that have to be developed at high costs in terms of financing and time required, but will ultimately not be accepted on the market. In addition, further developments of the standard, e.g. with regard to closing of future security gaps, are made more difficult or delayed if all companies that implement the standard are involved.

The hoped-for effect of the IOP would ultimately only affect such customers whose used providers would first want to take advantage of the IOP offer and then these customers would need to give their consent in each case again themselves. The factual positive effects are therefore to be assessed as considerably more limited and also generate new costs for consumers through increasing fragmentation and more complex usability.

Using the example of cross-provider groups, a possible impracticability becomes clear from both a legal consent and technical point of view, respectively in their combination. Assume that an alternative provider "C" implements reference offers from gatekeepers "A" and "B", but there is still no IOP between the latter two. If a user in a group chat of users of provider "C" now wants to invite a user of provider "A", all other group participants of provider "C" as well as the user of "A" to be invited would first have to individually agree that they may be addressed vis-à-vis the respective other provider and want to use the interoperable feature. Under these conditions, mixed groups of users from "A" and "C" as well as analogously groups of users from "A" and "B" could be formed.

However, the extent to which users from "A" and "B" can or should be brought together at the same time remains unclear. Could a user from "A" invite users from "B" within this group? Within a hypothetical group with users from "A", "B" and "C", de facto IOP would prevail between these users, which, however, does not exist de jure between providers "A" and "B" and therefore no corresponding consent can exist. A necessary relay function to enable group communication by provider "C" is not provided for and would violate end-to-end encryption if messages had to be translated between different protocols of "A" and "B". In addition to content encryption in the narrower sense, the problem of cross-provider user identification and authentication as well as contact discovery becomes particularly clear in the multilateral (group) context (cf. Chapters 4.2 and 4.3). Here, from the perspective (of the users) of individual providers, trust in the correct handling of other parties is fundamentally necessary and the respective consent situation is unclear, especially across more than two providers.

In the overall assessment, it therefore remains questionable how an IOP obligation for messaging services and the approach pursued in the DMA can be implemented in a targeted manner. The new IOP obligations of the DMA are also in conflict with the much more restrictive provisions of Section 21 (2) TKG (cf. Chapter 3.1.2.1). The greater caution in the TKG or EECC also seems to reflect our findings on horizontal IOP in comparison. In view of the risks described, close regulatory support is therefore necessary for the foreseen practical implementation.

The focus of the DMA on consumer aspects such as the preservation of encryption and data minimisation should in principle also be maintained in practical implementation and enforcement. Here, however, there is the difficulty of distinguishing between valid technical defence arguments and possible circumvention strategies. In order to assess the extent to which an encryption- and data protection-compliant implementation of IOP is actually technically possible and can be implemented within an appropriate framework, various central and independent organisations should therefore be involved. Likewise, the transparency and reporting obligations required elsewhere in the DMA should possibly also be concretised for this area.

In particular, the most common example of comprehensive IOP between directly competing services such as WhatsApp and Signal is unlikely to occur in the foreseeable future. More likely here, is the use by aggregation services such as Beeper, which could also be described as an intermediate stage between purely horizontal and purely vertical levels, as they act as a vertical complementary that enables horizontal IOP. The fact that Beeper has already expressed its interest in taking advantage of the IOP obligation shows that market acceptance also comes less from the direction of direct rivals on the purely horizontal level, but that models with vertical aspects could be more promising. Here it remains to be seen to what extent the market discovery process could produce novel popular solutions. Theoretically, an IOP between gatekeeper services could also be possible. Both WhatsApp and iMessage will have to publish reference offers, but it is questionable whether IOP would be implemented on this basis. If there were a concrete incentive to do so, the companies could have already implemented this without a legal obligation. However, Alphabet/Google has already expressed unilateral interest in a connection to iMessage in the past and could start a new attempt here to enable simple connectivity to iMessage users for Android customers. It is unclear to what extent the perception of an IOP obligation *between* gatekeepers is actually intended by the DMA, as this could even strengthen the dominance of some gatekeepers.

In general, two different approaches seem possible from the gatekeepers' side, especially with regard to WhatsApp and Facebook Messenger as the biggest potential targets for IOP requests. One possibility is (indirect) resistance, including only minimal and formal legal compliance or, for example, an overly complex and confusing design of the requested reference offers. Similar behaviour can currently be observed in the legal dispute between Apple and the Dutch market surveillance authority ACM (cf. ACM, 2019). It could also be possible that different gatekeepers collude (explicitly or tacitly) and design their respective reference offers as technically different as possible in order to increase the implementation effort for competitors and entrants.

In contrast to this, however, an "embrace strategy" is also conceivable, e.g. with the aim of being able to collect as much new (meta) data as possible. As an extreme form, in addition to the reference offer, even a ready-made implementation could be offered as "white label" solutions, in which the messaging service would technically build on the infrastructure of the gatekeeper and only the branding or the user interface and the marketing would be done by the alternative provider. Corresponding solutions are widespread, for example, in the area of mobile phone tariffs or cloud providers. Such a development should be counteracted, as there is no real infrastructure competition here and at most the dominance over data and the technologies used of some gatekeepers could be strengthened.

According to one of the experts interviewed, a central coordination office for reference offers could be conceivable as one pragmatic middle course. In this case, partial or full guidelines of how the reference offers are to be technically designed could reduce the implementation and coordination effort that would arise from a multitude of different reference offers, each only valid for one provider. Particularly if IOP is to be established with several providers at the same time, bilateral agreements scale poorly, since the combination possibilities of different offers and possibly different protocols used are exponentiated.

For requesting companies, the implementation effort would be lower if, for example, all reference offers had to be based at least on the same standard, such as the Signal or Matrix protocol or a new one to be developed. However, the current development in the area of the prevalent use of the Signal protocol shows that even implementations originating from the same basis can differ in essential details, such that potentially required agreement and adaptation efforts would not entirely disappear. A central agency could, for example, control and coordinate the reference offers or, in extreme cases, demand a uniform encryption or key exchange protocol that must be implemented as a fallback option in addition to the proprietary offers. However, this approach would also be associated with the underlying problems already mentioned, i.e. for agreeing on a uniform solution and in the practical implementation and operation. Here the question arises as to who should be the one to determine such a uniform procedure and to confirm the trustworthiness of the actors involved. This process could be supported, for example, by a public consultation.

## Bibliography

ACCC (2020). Digital Platform Services Inquiry - Online Messaging. Retrieved from: https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Service%20Inquiry%20-%20September%202020%20interim%20report.pdf.

ACM (2019). ACM launches investigation into abuse of dominance by Apple in its App Store. Retrieved from: https://www.acm.nl/en/publications/acm-launches-investigation-abuse-dominance-apple-its-app-store. 2022/03/31: 2022/03/31

Aghion, Philippe; Bloom, Nick; Blundell, Richard; Griffith, Rachel & Howitt, Peter (2005). Competition and innovation: An inverted-U relationship. In: *The quarterly journal of economics* 120, 2, p. 701-728

Aghion, Philippe; Blundell, Richard; Griffith, Rachel; Howitt, Peter & Prantl, Susanne (2009). The effects of entry on incumbent innovation and productivity. In: *The Review of Economics and Statistics* 91, 1, p. 20-32

Ahmed, Arooj (2021). The interoperability of WhatsApp and Messenger remains an uphill battle for Facebook; an executive argue for privacy-related issues. Retrieved from: https://www.digitalinformationworld.com/2021/07/the-interoperability-of-whatsapp-and.html. 2022/07/06: 2022/07/06

Amazon (2022). Amazon - Selling Partner API. Retrieved from: https://developer-docs.amazon.com/. 2022/03/31: 2022/03/31

Amnesty International (2018). Google’s new Chat service shows total contempt for Android users’ privacy. Retrieved from: https://www.amnesty.org/en/latest/news/2018/04/googles-new-chat-service-shows-total-contempt-for-android-users-privacy/. 2022/07/22: 2022/07/22

Anturix (2018). Sprachanrufe unter Signal. Retrieved from: https://forum.kuketz-blog.de/viewtopic.php?f=31&t=1467. 2022/07/06: 2022/07/06

Apple (2020). Privacy-Preserving Contact Tracing - Apple and Google. Retrieved from: https://www.apple.com/covid19/contacttracing. 2022/03/31/: 2022/03/31/

Apple (2021). Informationen zu iOS 14-Updates. Retrieved from: https://support.apple.com/de-de/HT211808. 2022/03/31: 2022/03/31

Apple (2022). Autoschlüssel auf dem iPhone oder der Apple Watch zu Apple Wallet hinzufügen. Retrieved from: https://support.apple.com/de-de/HT211234. 2022/03/31: 2022/03/31

Armstrong, Mark (2006). Competition in Two-Sided Markets. In: *The RAND Journal of Economics* 37, 3, p. 668-691

Arnold, René; Hildebrandt, Christian; Kroon, Peter & Taş, Serpil (2017). The Economic and Societal Value of Rich Interaction Applications in India. Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK). Retrieved from: https://www.wik.org/fileadmin/Studien/2017/WIK-BIF_Report_-_The_Economic_and_Societal_Impact_of_RIAs_in_India.pdf.

Arnold, René & Schneider, Anna (2017). An App for Every Step: A psychological perspective on interoperability of Mobile Messenger Apps. In: *28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age"*. Passau, Germany: p.

Arnold, René; Schneider, Anna & Lennartz, Jonathan (2020). Interoperability of interpersonal communications services – A consumer perspective. In: *Telecommunications Policy* 44, 3,

Arthur, W Brian (1989). Competing technologies, increasing returns, and lock-in by historical events. In: *The economic journal* 99, 394, p. 116-131

Autorité de la Concurrence & CMA (2014). The Economics of open and closed systems. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387718/The_economics_of_open_and_closed_systems.pdf.

Axelrod, Robert; Mitchell, Will; Thomas, Robert E; Bennett, D Scott & Bruderer, Erhard (1995). Coalition formation in standard-setting alliances. In: *Management science* 41, 9, p. 1493-1508

Baldwin, Carliss Young; Clark, Kim B & Clark, Kim B (2000). *Design rules: The power of modularity*. Bd. 1. MIT press, 0262024667

Barczentewicz, Mikołaj (2022). Privacy and Security Implications of Regulation of Digital Services in the EU and in the US. In: *TTLF Working Papers* 84,

Batchelor, Bill; Vandenborre, Ingrid; Luoma, Aurora; Frese, Michael J. & Kamp, Alexander (2021). CMA Proposes New UK Competition Regime for Large Tech Firms | Insights | Skadden, Arps, Slate, Meagher & Flom LLP. Retrieved from: https://www.skadden.com/insights/publications/2020/12/cma-proposes-new-uk-competition-regime. 2022/04/01/: 2022/04/01/

Baumol, William J; Panzar, John C & Willig, Robert D (1983). Contestable markets: An uprising in the theory of industry structure: Reply. In: *The American Economic Review* 73, 3, p. 491-496

Becker, Jörg; Holznagel, Bernd & Müller, Kilian (2021). Interoperability of messenger services: Possibilities for a consumer-friendly approach. In: *Perspectives on platform regulation: Concepts and models of social media governance across the globe* p. 119-143

Beeper (2022). Beeper - All Your Chats In One App. Retrieved from: https://www.beeper.com/. 2022/05/11: 2022/05/11

Belleflamme, Paul & Peitz, Martin (2019). Platform competition: Who benefits from multihoming? In: *International Journal of Industrial Organization* 64, p. 1-26

Belleflamme, Paul & Peitz, Martin (2021). *The Economics of Platforms*. Cambridge University Press, 9781108696913

Benlian, Alexander; Hilkert, Daniel & Hess, Thomas (2015). How open is this Platform? The meaning and measurement of platform openness from the complementers' perspective. In: *Journal of information Technology* 30, 3, p. 209-228

Bennaceur, Amel; Issarny, Valérie; Spalazzese, Romina & Tyagi, Shashank (2012). Achieving interoperability through semantics-based technologies: The instant messaging case. In: *International Semantic Web Conference*. Boston, MA: p. 17-33

BEREC (2016). Report on OTT services. Retrieved from: https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf.

Bhargavan, Karthikeyan; Barnes, Richard & Rescorla, Eric (2018). TreeKEM: Asynchronous Decentralized Key Management for Large Dynamic Groups A protocol proposal for Messaging Layer Security (MLS). Inria Paris. Retrieved from: https://hal.inria.fr/hal-02425247.

Bishop, DT & Cannings, Chris (1978). A generalized war of attrition. In: *Journal of theoretical biology* 70, 1, p. 85-124

Bloch, Joshua (2006). How to design a good API and why it matters. In: *Companion to the 21st ACM SIGPLAN symposium on Object-oriented programming systems, languages, and applications*. p. 506-507

Bluetooth (2022). Member Directory. Retrieved from: https://www.bluetooth.com/develop-with-bluetooth/join/member-directory/. 2022/04/01: 2022/04/01

Bohn, Dieter (2019). Google is finally taking charge of the RCS rollout. Retrieved from: https://www.theverge.com/2019/6/17/18681573/google-rcs-chat-android-texting-carriers-imessage-encryption. 2022/06/13: 2022/06/13

Bostoen, Friso (2018). Online platforms and vertical integration: the return of margin squeeze? In: *Journal of antitrust enforcement* 6, 3, p. 355-381

Boudreau, Kevin (2010). Open platform strategies and innovation: Granting access vs. devolving control. In: *Management science* 56, 10, p. 1849-1872

Boudreau, Kevin (2012). Let a thousand flowers bloom? An early look at large numbers of software app developers and patterns of innovation. In: *Organization Science* 23, 5, p. 1409-1427

Bourreau, Marc; Krämer, Jan & Buiten, Miriam (2022). Interoperability in Digital Markets. Retrieved from: https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf.

Breton, Thierry (2019). Questionnaire to the Commisioner-Designate for the Internal Market. Europäische Kommission,. Retrieved from: https://ec.europa.eu/commission/commissioners/sites/commcwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf. 2022/07/06: 2022/07/06

Briar (2021). Mailbox Architecture - Wiki. Retrieved from: https://code.briarproject.org/briar/briar/-/wikis/Mailbox-Architecture. 2022/07/06: 2022/07/06

Brown, Ian (2020). Interoperability as a tool for competition regulation. In: *OFA Research Paper* p. 2-2

Brynjolfsson, Erik; Hu, Yu & Smith, Michael D (2003). Consumer surplus in the digital economy: Estimating the value of increased product variety at online booksellers. In: *Management science* 49, 11, p. 1580-1596

BSI (2021). Moderne Messenger – heute verschlüsselt , morgen interoperabel ? Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.pdf?__blob=publicationFile&v=8.

Bundeskartellamt (2021). Sektoruntersuchung Messenger- und Video-Dienste, Zwischenbericht „Branchenüberblick und Stimmungsbild Interoperabilität". Retrieved from: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_MessengerVideoDienste_Zwischenbericht.pdf?__blob=publicationFile&v=8.

Bundesnetzagentur (2020). Nutzung von OTT-Kommunikationsdiensten in Deutschland Bericht 2020. Retrieved from: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile.

Bundesnetzagentur (2021). Interoperabilität zwischen Messengerdiensten Überblick der Potenziale und Herausforderungen. Retrieved from: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP.pdf?__blob=publicationFile&v=3.

Bundesnetzagentur (2022). Nutzung von Online-Kommunikationsdiensten in Deutschland Ergebnisse der Verbraucherbefragung 2021. Retrieved from: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_lang21.pdf?__blob=publicationFile&v=3.

Burgess, Matt (2022). Forcing WhatsApp and iMessage to Work Together Is Doomed to Fail. Retrieved from: https://www.wired.co.uk/article/dma-interoperability-messaging-imessage-whatsapp. 2022/07/06: 2022/07/06

Busch, Christoph (2022). Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation. In: *UCLA Journal of Law & Technology* 27, p. 15

BusinessWire (2021). The Connectivity Standards Alliance Unveils Matter, Formerly Known as Project CHIP. Retrieved from: https://www.businesswire.com/news/home/20210511005928/en/The-

Connectivity-Standards-Alliance-Unveils-Matter-Formerly-Known-as-Project-CHIP. 2022/05/31: 2022/05/31

Cadwalladr, Carole & Graham-Harrison, Emma (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. 2022/05/31: 2022/05/31

Chen, Jiawei; Doraszelski, Ulrich & Harrington, Jr, Joseph E (2009). Avoiding market dominance: Product compatibility in markets with network effects. In: *The RAND Journal of Economics* 40, 3, p. 455-485

Chiao, Benjamin; Lerner, Josh & Tirole, Jean (2007). The rules of standard-setting organizations: an empirical analysis. In: *The RAND Journal of Economics* 38, 4, p. 905-930

Choi, Jay Pil & Gerlach, Heiko (2013). Multi-Market Collusion with Demand Linkages and Antitrust Enforcement. In: *The Journal of Industrial Economics* 61, 4, p. 987-1022

Chou, Chien-fu & Shy, Oz (1993). Partial compatibility and supporting services. In: *Economics letters* 41, 2, p. 193-197

Claburn, Thomas (2020). Aggrieved ad tech types decry Google dominance in W3C standards – who writes the rules and for whom? Retrieved from: https://www.theregister.com/2020/07/17/aggrieved_ad_tech_types_decry. 2022/07/06: 2022/07/06

Clover, Juli (2022). Telegram Testing New Premium Subscription. Retrieved from: https://www.macrumors.com/2022/05/02/telegram-premium-subscription/. 2022/07/06: 2022/07/06

CMA (2020). A new pro-competition regime for digital markets - Appendix D : The SMS regime : pro-competitive interventions. Retrieved from.

CMA (2021). Mobile ecosystems market study. Retrieved from: https://www.gov.uk/cma-cases/mobile-ecosystems-market-study.

Cocorada, Sorin (2018). Signal Messanger Architecture – IT Security Operations. Retrieved from: https://sorincocorada.ro/signal-messanger-architecture/. 2022/07/06: 2022/07/06

Colangelo, Giuseppe & Maggiolino, Mariateresa (2018). Data accumulation and the privacy–antitrust interface: insights from the Facebook case. In: *International Data Privacy Law* 8, 3, p. 224-239

Crémer, Jacques; de Montjoye, Yves-Alexandre & Schweitzer, Heike (2019). Competition Policy for the digital era. European Commission. Retrieved from: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

Cressler, Cosette (2021). Understanding WhatsApp's Architecture & System Design. Retrieved from: https://www.cometchat.com/blog/whatsapps-architecture-and-system-design. 2022/05/18: 2022/05/18

CSA (2022). CSA Mitglieder. Retrieved from: https://csa-iot.org/members/. 2022/07/06: 2022/07/06

Cyphers, Bennett & Doctorow, Cory (2021). Privacy Without Monopoly: Data Protection and Interoperability. Retrieved from: https://www.eff.org/wp/interoperability-and-privacy. 2022/07/06: 2022/07/06

D'Incau, Paolo (2013). An interview with Eugene Fooksman #erlang. Retrieved from: https://pdincau.wordpress.com/2013/03/27/an-interview-with-eugene-fooksman-erlang/. 2022/07/06: 2022/07/06

Data Transfer Project (2021). Data Transfer Project - Portability Data Models. Retrieved from: https://github.com/google/data-transfer-project. 2022/03/31: 2022/03/31

David, Paul A. (1985). Clio and the Economics of QWERTY. In: *The American Economic Review* 75, 2, p. 332-337

David, Paul A. & Greenstein, Shane (1990). The Economics Of Compatibility Standards: An Introduction To Recent Research. In: *Economics of Innovation and New Technology* 1, 1-2, p. 3-41

De Palma, Andre; Leruth, Luc & Regibeau, Pierre (1999). Partial compatibility with network externalities and double purchase. In: *Information Economics and Policy* 11, 2, p. 209-227

De Reuver, Mark; Sørensen, Carsten & Basole, Rahul C (2018). The digital platform: a research agenda. In: *Journal of Information Technology* 33, 2, p. 124-135

Doctorow, Cory (2019). Interoperability: Fix the Internet, Not the Tech Companies. Retrieved from: https://www.eff.org/deeplinks/2019/07/interoperability-fix-internet-not-tech-companies. 2022/07/06: 2022/07/06

Doctorow, Cory (2022). I've been waiting 15 years for Facebook to die. I'm more hopeful than ever. Retrieved from: https://www.theguardian.com/commentisfree/2022/feb/24/ive-been-waiting-15-years-for-facebook-to-die-im-more-hopeful-than-ever. 2022/04/01: 2022/04/01

Doganoglu, Toker & Wright, Julian (2006). Multihoming and compatibility. In: *International Journal of Industrial Organization* 24, 1, p. 45-67

Dutta-Bergman, Mohan J. (2004). Interpersonal communication after 9/11 via telephone and internet: A theory of channel complementarity. In: *New Media & Society* 6, 5, p. 659-673

Economides, Nicholas & Skrzypacz, Andrzej (2003). Standards Coalitions Formation and Market Structure in Network Industries. In: *Available at SSRN 378340*

EDRi (2018). Answering guide for European Commission's "illegal" content "consultation". Retrieved from: https://edri.org/EDRiDSAAnsweringGuide.html. 2022/07/06: 2022/07/06

Eisenmann, Thomas; Parker, Geoffrey & Van Alstyne, Marshall (2009). Opening platforms: How, when and why. In: *Platforms, markets and innovation* 6, p. 131-162

Eisenmann, Thomas; Parker, Geoffrey & Van Alstyne, Marshall (2011). Platform envelopment. In: *Strategic management journal* 32, 12, p. 1270-1285

Element (2022a). Closed federation | Open federation. Retrieved from: https://element.io/enterprise/closed-federation-and-open-federation. 2022/05/18/: 2022/05/18/

Element (2022b). Hosted Matrix bridges | Element Matrix Services. Retrieved from: https://element.io/matrix-services/hosted-bridges. 2022/05/24: 2022/05/24

Ermoshina, Ksenia & Musiani, Francesca (2019). "Standardising by running code": the Signal protocol and *de facto* standardisation in end-to-end encrypted messaging. In: *Internet Histories* 3, 3-4, p. 343-363

ETSI (2022). ETSI ICT Standards. Retrieved from: https://www.etsi.org/standards. 2022/04/01: 2022/04/01

Europäische Kommission (2022a). Non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA. Retrieved from: https://www.lobbycontrol.de/wp-content/uploads/non_paper_interoperability_dma.pdf. 2022/07/06: 2022/07/06

Europäische Kommission (2022b). Remarks by Executive Vice-President Vestager on the Statement of Objections sent to Apple over practices regarding Apple Pay. Retrieved from: https://ec.europa.eu/commission/presscorner/home/en. 2022/05/02/: 2022/05/02/

Evans, David S. (2003). The antitrust economics of two-sided markets. In: *Yale Journal on Regulation* 20, 2, Art. 4,

Evans, David S. (2009). How catalysts ignite: the economics of platform-based start-ups. In: *Platforms, markets and innovation* 416, Evans, David S. & Schmalensee, Richard (2010). Failure to Launch: Critical Mass in Platform Businesses. In: *Review of Network Economics* 9, 4,

Facebook (2022). Nachrichten - WhatsApp Business On-Premises API - Dokumentation. Retrieved from: https://developers.facebook.com/docs/whatsapp/on-premises/reference/messages/. 2022/05/28: 2022/05/28

Faife, Corin (2022). Security experts say new EU rules will damage WhatsApp encryption. Retrieved from: https://www.theverge.com/2022/3/28/23000148/eu-dma-damage-whatsapp-encryption-privacy. 2022/05/18: 2022/05/18

Farrell, Joseph; Hayes, John; Shapiro, Carl & Sullivan, Theresa (2007). Standard setting, patents, and hold-up. In: *Antitrust LJ* 74, p. 603

Farrell, Joseph & Klemperer, Paul (2007). Coordination and lock-in: Competition with switching costs and network effects. In: *Handbook of industrial organization* 3, p. 1967-2072

Farrell, Joseph & Saloner, Garth (1985a). Economic issues in standardization. In:

Farrell, Joseph & Saloner, Garth (1985b). Standardization, compatibility, and innovation. In: *the RAND Journal of Economics* p. 70-83

Farrell, Joseph & Saloner, Garth (1986a). Competition, compatability and Standards: The economics of horses, penguins and lemmings. In:

Farrell, Joseph & Saloner, Garth (1986b). Installed base and compatibility: Innovation, product preannouncements, and predation. In: *The American economic review* p. 940-955

Farrell, Joseph & Saloner, Garth (1988). Coordination through committees and markets. In: *The RAND Journal of Economics* p. 235-252

Farrell, Joseph & Saloner, Garth (1992). Converters, compatibility, and the control of interfaces. In: *The journal of industrial economics* p. 9-35

Farrell, Joseph & Simcoe, Timothy (2012a). Choosing the rules for consensus standardization. In: *The RAND Journal of Economics* 43, 2, p. 235-252

Autho (2012b). Four paths to compatibility. In: *The Oxford Handbook of the Digital Economy*. Oxford University Press Oxford, UK, and New York, S. 34-58

Furman, Jason (2019). Unlocking digital competition: Report of the Digital Competition Expert Panel. In: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf*

Gallini, Nancy T (2002). The economics of patents: Lessons from recent US patent reform. In: *Journal of Economic Perspectives* 16, 2, p. 131-154

Gans, Joshua (2018). Enhancing competition with data and identity portability. In: *The Hamilton Project* p. 1-28

Gekeler, Martin (2022). Schnellübersicht Messengersysteme. Retrieved from: https://www.freie-messenger.de/systemvergleich/. 2022/05/18: 2022/05/18

Geradin, Damien & Rato, Miguel (2007). Can standard-setting lead to exploitative abuse? A dissonant view on patent hold-up, royalty stacking and the meaning of FRAND. In: *European Competition Journal* 3, 1, p. 101-161

Google (2020). Exposure Notifications implementation guide | Google API for Exposure Notifications. Retrieved from: https://developers.google.com/android/exposure-notifications/implementation-guide. 2022/03/31: 2022/03/31

Google (2022a). Messages End-to-End Encryption Overview - Version 1.2. Retrieved from: https://element.io/blog/the-digital-markets-act-explained-in-15-questions/. 2022/07/06/: 2022/07/06/

Google (2022b). Overview | Geocoding API. Retrieved from: https://developers.google.com/maps/documentation/geocoding/overview. 2022/03/31: 2022/03/31

Griggio, Carla F. ; Nouwens, Midas & Klokmose, Clemens Nylandsted (2022). Caught in the Network: The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems. In: *CHI Conference on Human Factors in Computing Systems*. New Orleans, LA, USA: Association for Computing Machinery, p. Article 104

Grüner, Sebastian (2019). Chat over IMAP - Gut gemeint ist leider nicht gut gemacht. Retrieved from: https://www.golem.de/news/chat-over-imap-gut-gemeint-ist-leider-nicht-gut-gemacht-1905-141009.html. 2022/05/18: 2022/05/18

Hagiu, Andrei & Wright, Julian (2020a). Data-enabled learning, network effects and competitive advantage. In: *Unpublished manuscript*

Hagiu, Andrei & Wright, Julian (2020b). When data creates competitive advantage. In: *Harvard business review* 98, 1, p. 94-101

Heim, Mathew & Nikolic, Igor (2019). A FRAND regime for dominant digital platforms. In: *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 10, p. 38

Higgins, Tim (2022). Why Apple's iMessage Is Winning: Teens Dread the Green Text Bubble. In: *The Wall Street Journal*. p.

HM Government (2022). Government response to the consultation on a new pro-competition regime for digital markets. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1073164/E02740688_CP_657_Gov_Resp_Consultation_on_pro-comp_digital_markets_Accessible.pdf.

Hodgson, Matthew (2019). Matthew Hodgson Presents Matrix 1.0: Decentralized Communication at Scale at Web3 Summit 2019. In: p.

IETF (2022). Working groups. In: *IETF*

Instagram (2022). Neue Funktionen für Direktnachrichten auf Instagram. Retrieved from: https://about.instagram.com/de-de/blog/announcements/introducing-new-dm-features/. 2022/03/31: 2022/03/31

Internet Society (2022). DMA and interoperability of encrypted messaging. Retrieved from: https://www.internetsociety.org/wp-content/uploads/2022/03/ISOC-EU-DMA-interoperability-encrypted-messaging-20220311.pdf. 2022/07/06: 2022/07/06

ISO (2017). iec/ieee international standard-systems and software engineering–vocabulary. In: *ISO/IEC/IEEE 24765: 2017 (E)*

Jacobides, Michael G & Lianos, Ioannis (2021a). Ecosystems and competition law in theory and practice. In: *Industrial and Corporate Change* 30, 5, p. 1199-1229

Jacobides, Michael G & Lianos, Ioannis (2021b). Regulating platforms and ecosystems: an introduction. In: 30, 5, p. 1131-1142

Jäschke, Marvin (2021). BfJ: Anwendung des NetzDG gegen Telegram. In: *Computer und Recht* 37, 7, p. r79-r80

Johannsen, Jan (2015). WhatsApp Plus: Immer noch Finger weg vom Messenger-Klon - CURVED.de. Retrieved from: https://curved.de/news/whatsapp-plus-faq-21036. 2022/05/18: 2022/05/18

Jullien, Bruno & Sand-Zantman, Wilfried (2021). The economics of platforms: A theory guide for competition policy. In: *Information Economics and Policy* 54, p. 100880

Kamien, Morton I (1992). Patent licensing. In: *Handbook of game theory with economic applications* 1, p. 331-354

Katz, Michael L & Shapiro, Carl (1985). Network externalities, competition, and compatibility. In: *The American economic review* 75, 3, p. 424-440

Katz, Michael L & Shapiro, Carl (1994). Systems competition and network effects. In: *Journal of economic perspectives* 8, 2, p. 93-115

Kerber, Wolfgang & Schweitzer, Heike (2017). Interoperability in the digital economy. In: *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 8, p. 39

Kokolakis, Spyros (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In: *Computers & security* 64, p. 122-134

Krämer, Jan & Schnurr, Daniel (2014). A unified framework for open access regulation of telecommunications infrastructure: Review of the economic literature and policy guidelines. In: *Telecommunications Policy* 38, 11, p. 1160-1179

Krämer, Jan & Schnurr, Daniel (2021). Big data and digital markets contestability: Theory of harm and data access remedies. In: *Available at SSRN 3789510*

Krämer, Jan; Sellenart, Pierre & de Streel, Alexandre (2020). Making data portability more effective for the digital economy. CERRE. Retrieved from: https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/.

Kröner, Peter & Divya, Manian (2013). SpecGraph. Retrieved from: https://github.com/SirPepe/SpecGraph. 2022/03/31: 2022/03/31

Kroon, Peter & Arnold, René (2018). Die Bedeutung von Interoperabilität in der digitalen Welt: Neue Herausforderungen in der interpersonellen Kommunikation - WIK-Diskussionsbeitrag Nr. 437. Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK). Retrieved from: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_437.pdf.

Kroon, Peter; Baischew, Dajan; Lucidi, Stefano; Märkel, Christian & Sörries, Bernd (2020). Digital Sovereignty in Europe – a first benchmark. WIK. Retrieved from: https://www.wik.org/en/veroeffentlichungen/studien/weitere-seiten/digital-sovereignty?msclkid=a0794a20b3ea11ec910c887fdf5c32cc.

Kuketz, Mike (2020). Messenger-Brücken sind datenschutzrechtlich bedenklich. Retrieved from: https://www.kuketz-blog.de/messenger-bruecken-sind-datenschutzrechtlich-bedenklich/. 2022/05/18: 2022/05/18

Laffont, Jean-Jacques; Rey, Patrick & Tirole, Jean (1998). Network competition: II. Price discrimination. In: *The RAND Journal of Economics* p. 38-56

Lancieri, Filippo & Sakowski, Patricia Morita (2021). Competition in digital markets: a review of expert reports. In: *Stan. JL Bus. & Fin.* 26, p. 65

Le Pape, Amandine (2022). The Digital Markets Act explained in 15 questions. Retrieved from: https://element.io/blog/the-digital-markets-act-explained-in-15-questions/. 2022/07/06/: 2022/07/06/

Lee, Robin S (2013). Vertical integration and exclusivity in platform and two-sided markets. In: *American Economic Review* 103, 7, p. 2960-3000

Lemley, Mark A & Samuelson, Pamela (2021). Interfaces and Interoperability After Google v. Oracle. In: *Tex. L. Rev.* 100, p. 1

Lerner, Josh & Tirole, Jean (2006). A model of forum shopping. In: *American economic review* 96, 4, p. 1091-1113

Lewis, Grace (2013). Standards in Cloud Computing Interoperability. In: *SEI Blog*

Lomas, Natasha (2022). Europe says yes to messaging interoperability as it agrees on major new regime for Big Tech. Retrieved from: https://techcrunch.com/2022/03/24/dma-political-agreement/?guccounter=1. 2022/07/06: 2022/07/06

Lyles, Taylor (2020). A year later, Amazon’s voice assistant alliance still hasn’t attracted any of its rivals. Retrieved from: https://www.theverge.com/2020/9/9/21429893/amazon-voice-interoperability-initiative-alexa-apple-google-samsung. 2022/03/31: 2022/03/31

Majority Staff Report and Recommendations & Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary (2020). Investigation of Competition in Digital Markets. In:

Manenti, Fabio M & Somma, Ernesto (2008). One-way compatibility, two-way compatibility and entry in network industries. In: *International Journal of the Economics of Business* 15, 3, p. 301-322

Manyika, James; Chui, Michael; Bisson, Peter; Woetzel, Jonathan; Dobbs, Richard; Bughin, Jacques & Aharon, Dan (2015). *The Internet of Things: Mapping the value beyond the hype*. Bd. 24. McKinsey Global Institute New York, NY, USA,

March, Salvatore; Hevner, Alan & Ram, Sudha (2000). Research commentary: An agenda for information technology research in heterogeneous and distributed environments. In: *Information Systems Research* 11, 4, p. 327-341

Marlinspike, Moxie (2016a). Reflections: The ecosystem is moving. Retrieved from: https://signal.org/blog/the-ecosystem-is-moving/. 2022/07/06: 2022/07/06

Marlinspike, Moxie (2016b). WhatsApp's Signal Protocol integration is now complete. Retrieved from: https://signal.org/blog/whatsapp-complete/. 2022/05/18: 2022/05/18

Marlinspike, Moxie (2017). Technology preview: Private contact discovery for Signal. Retrieved from: https://signal.org/blog/private-contact-discovery/. 2022/05/18: 2022/05/18

Marlinspike, Moxie & Perrin, Trevor (2016). The X3DH Key Agreement Protocol. Signal. Retrieved from: https://signal.org/docs/specifications/x3dh/x3dh.pdf.

Marsden, Chris; Meyer, Trisha & Brown, Ian (2020). Platform values and democratic elections: How can the law regulate digital disinformation? In: *Computer Law & Security Review* 36, p. 105373

Matos, Tarcila & Torres-Sarmiento, Carolina (2022). FRAND for Dominant Digital Platforms: Enhancing the Way Essential Inputs are Accessed, Transferred and Shared. In: *GRUR International* 71, 6, p. 516-527

Matrix (2022). Bridges. Retrieved from: https://matrix.org. 2022/05/24/: 2022/05/24/

Matutes, Carmen & Regibeau, Pierre (1988). " Mix and match": product compatibility without network externalities. In: *The RAND Journal of Economics* p. 221-234

Meaker, Morgan (2022). Europe's Digital Markets Act Takes a Hammer to Big Tech. Retrieved from: https://www.wired.com/story/digital-markets-act-messaging/. 2022/07/06: 2022/07/06

Meta (2020). Say "Hello" to Messenger: Introducing New Messaging Features for Instagram. Retrieved from: https://about.fb.com/news/2020/09/new-messaging-features-for-instagram/. 2022/07/06: 2022/07/06

Monopolkommission (2021). Telekommunikation 2021: Wettbewerb im Umbruch, 12. Sektorgutachten. Retrieved from: https://www.monopolkommission.de/images/PDF/SG/12sg_telekommunikation_volltext.pdf.

Muffett, Alec (2022). A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022. Retrieved from: https://alecmuffett.com/alecm/e2e-primer/e2e-primer-web.html. 2022/07/27: 2022/07/27

Nominet (2019). Cyber security and the cloud - Enterprise security leaders have their say. Retrieved from: https://media.nominetcyber.com/wp-content/uploads/2019/08/Cloud-security-report_2019.pdf.

Norman, George & Thisse, Jacques-Francois (1996). Product variety and welfare under tough and soft pricing regimes. In: *The Economic Journal* 106, 434, p. 76-91

Noura, Mahda; Atiquzzaman, Mohammed & Gaedke, Martin (2019). Interoperability in internet of things: Taxonomies and open challenges. In: *Mobile networks and applications* 24, 3, p. 796-809

Nouwens, Midas; Griggio, Carla F & Mackay, Wendy E (2017). WhatsApp is for family; Messenger is for friends: Communication Places in App Ecosystems. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, p. 727-735

OECD (2018). Rethinking Antitrust Tools for Multi-Sided Platforms. OECD. Retrieved from: https://www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf.

OECD (2021). Data portability, interoperability and digital platform competition. In:

Oestreich, Nicolas (2018). Weitgehend unbemerkt: Vodafone und o2 stellen ihre Messenger ein. Retrieved from: https://www.iphone-ticker.de/weitgehend-unbemerkt-vodafone-und-o2-stellen-ihre-messenger-ein-125269/. 2022/06/13: 2022/06/13

Open Banking (2022a). About the Open Banking Implementation Entitiy. Retrieved from: https://www.openbanking.org.uk/about-us/. 2022/07/06: 2022/07/06

Open Banking (2022b). Fintechs. Retrieved from: https://www.openbanking.org.uk/fintechs/. 2022/07/06: 2022/07/06

Oracle (2010). Fusion Middleware Interoperability and Compatibility Guide. Retrieved from: https://docs.oracle.com/cd/E17904_01/doc.1111/e17836/overview.htm#INTOP109. 2022/04/01: 2022/04/01

Padilla, Jorge; Perkins, Joe & Piccolo, Salvatore (2020). Self-preferencing in markets with vertically-integrated gatekeeper platforms. In: *Available at SSRN 3701250*

Panzarino, Matthew (2020). Apple and Google are launching a joint COVID-19 tracing tool for iOS and Android. Retrieved from: https://social.techcrunch.com/2020/04/10/apple-and-google-are-launching-a-joint-covid-19-tracing-tool/. 2022/03/31: 2022/03/31

Parker, Geoffrey; Petropoulos, Georgios & Van Alstyne, Marshall W (2020). Digital platforms and antitrust. In: *Available at SSRN 3608397*

Polites, Greta L & Karahanna, Elena (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. In: *MIS quarterly* p. 21-42

Porell, Jim (2020). Rocket and Open Source: A Brief History on the Open Mainframe Movement. Retrieved from: https://blog.rocketsoftware.com/2020/09/rocket-and-open-source-a-brief-history-on-the-open-mainframe-movement/#.YN9p9RNue3. 2022/07/06: 2022/07/06

Prüfer, Jens & Schottmüller, Christoph (2021). Competing with big data. In: *The Journal of Industrial Economics* 69, 4, p. 967-1008

Pujol, Alexandre; Magoni, Damien; Murphy, Liam & Thorpe, Christina (2019). Spying on Instant Messaging Servers: Potential Privacy Leaks through Metadata. In: *Transactions on Data Privacy* 12(2), p. 175-206

Quan-Haase, Anabel & Collins, Jessica L. (2008). 'I'm there, but I might not want to talk to you'. In: *Information, Communication & Society* 11, 4, p. 526-543

Autho (2020). Corona-Warn-App: Tracing the start of the official COVID-19 Exposure Notification App for germany. In: *Proceedings of the SIGCOMM'20 Poster and Demo Sessions.* S. 24-26

Reuter, Markus (2022). Sichere Messenger Threema und Signal sind gegen Interoperabilität. Retrieved from: https://netzpolitik.org/2022/digital-markets-act-sichere-messenger-threema-und-signal-sind-gegen-interoperabilitaet/. 2022/07/08/: 2022/07/08/

Riley, Chris (2020). Unpacking interoperability in competition. In: *Journal of Cyber Policy* 5, 1, p. 94-106

Rochet, Jean-Charles & Tirole, Jean (2003). Platform competition in two-sided markets. In: *Journal of the european economic association* 1, 4, p. 990-1029

Roettgers, Janko (2021). OK Google, meet Alexa: Interoperability emerges as key antitrust issue. Retrieved from: https://www.protocol.com/google-alexa-sonos-antitrust. 2022/05/03/: 2022/05/03/

Rohlfs, Jeffrey (1974). A theory of interdependent demand for a communications service. In: *The Bell journal of economics and management science* p. 16-37

Rösler, Paul; Mainka, Christian & Schwenk, Jörg (2018). More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. In: *2018 IEEE European Symposium on Security and Privacy (EuroS P)*. p. 415-429

RTR (2020). Monitoring von digitalen Kommunikations Plattformen und Gatekeepern des offenen Internetzugangs. Retrieved from: https://www.bwb.gv.at/fileadmin/user_upload/PDFs/Monitoring_von_digitalen_Plattformen__RTR_Methodenpapier_.pdf.

Ruppel, Erin K.; Burke, Tricia J. & Cherney, Maura R. (2017). Channel compplementarity and multiplexity in long-distance friends' patterns of communication technology use. In: *New Media & Society* 20, 4, p. 1564-1579

Salinas, Sonia Ordonez & Nieto Lemus, Alba Consuelo (2017). Data Warehouse and Big Data Integration. In: *International Journal of Computer Science and Information Technology* 9, 2, p. 01-17

Samuelson, William & Zeckhauser, Richard (1988). Status quo bias in decision making. In: *Journal of risk and uncertainty* 1, 1, p. 7-59

Sanchez-Cartas, Juan Manuel & León, Gonzalo (2021). Multisided platforms and markets: A survey of the theoretical literature. In: *Journal of Economic Surveys* 35, 2, p. 452-487

Sanders, James (2019). Multicloud deployments are twice as likely to fall victim to security breaches. Retrieved from: https://www.techrepublic.com/article/multicloud-deployments-are-twice-as-likely-to-fall-victim-to-security-breaches/. 2022/07/06: 2022/07/06

Scherer, François M (1979). The welfare economics of product variety: an application to the ready-to-eat cereals industry. In: *The Journal of Industrial Economics* p. 113-134

Scott Morton, Fiona M.; Crawford, Gregory S.; Crémer, Jacques; Dinielli, David; Fletcher, Amelia; Heidhues, Paul; Schnitzer, Monika & Seim, Katja (2021). Equitable Interoperability: The 'Super Tool' of Digital Platform Governance. In: *SSRN Electronic Journal*

Scott Morton, Fiona M. & Kades, Michael (2021). Interoperability As a Competition Remedy for Digital Networks. In: *SSRN Electronic Journal* February,

Shampanier, Kristina; Mazar, Nina & Ariely, Dan (2007). Zero as a special price: The true value of free products. In: *Marketing science* 26, 6, p. 742-757

Shapiro, Carl (2001). Setting compatibility standards: cooperation or collusion. In: *Expanding the Boundaries of Intellectual Property* 81, p. 97-101

Shapiro, Carl & Varian, Hal R (1998a). *Information rules: A strategic guide to the network economy*. Harvard Business Press, 087584863X

Shapiro, Carl & Varian, Hal R (1998b). Versioning: the smart way to. In: *Harvard business review* 107, 6, p. 107

Sidak, J Gregory (2009). Patent holdup and oligopsonistic collusion in standard-setting organizations. In: *Journal of Competition Law & Economics* 5, 1, p. 123-188

Signal, Foundation (2021). Signal Server Source Code. Retrieved from: https://github.com/signalapp/Signal-Server. 2022/05/18: 2022/05/18

Simcoe, Timothy & Watson, Jeremy (2019). Forking, Fragmentation, and Splintering. In: *Strategy Science* 4, 4, p. 283-297

Sirbu, Marvin & Hughes, Kent (1986). Standardization of local area networks. In: *14th Annual Telecommunications Policy Research Conference, Virginia*. p.

Stack Overflow (2022). Newest Questions. In: *Stack Overflow*

Stamm, Barbara (2022). Marktmachtabhängige und -unabhängige Zugangsregulierung im neuen TKG – TKG-Novelle I: Erweiterung der Zugangsverpflichtungen statt

Deregulierung. In: *Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR)* p. 357-363

Statista (2021). Nutzung von Cloud Computing in deutschen Unternehmen bis 2020. Retrieved from: https://de.statista.com/statistik/daten/studie/177484/umfrage/einsatz-von-cloud-computing-in-deutschen-unternehmen-2011/. 2022/04/04: 2022/04/04

Statista (2022). Public Cloud - Europe | Statista Market Forecast. Retrieved from: https://www.statista.com/outlook/tmo/public-cloud/europe. 2022/07/06: 2022/07/06

Stoltz, Mitch; Crocker, Andrew & Schmon, Christoph (2022). The EU Digital Markets Act's Interoperability Rule Addresses An Important Need, But Raises Difficult Security Problems for Encrypted Messaging. Retrieved from: https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises. 2022/07/06: 2022/07/06

Stylos, Jeffrey (2009). Making APIs more usable with improved API designs, documentation and tools. In: Carnegie Mellon University, p.

Stylos, Jeffrey & Myers, Brad A (2006). Mica: A web-search tool for finding api components and examples. In: *Visual Languages and Human-Centric Computing (VL/HCC'06)*. IEEE, p. 195-202

Syrmoudis, Emmanuel; Mager, Stefan; Kuebler-Wachendorff, Sophie; Pizzinini, Paul; Grossklags, Jens & Kranz, Johann (2021). Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. In: *Proc. Priv. Enhancing Technol.* 2021, 3, p. 351-372

Tandoc, Edson C., Jr.; Lou, Chen & Min, Velyn Lee Hui (2019). Platform-swinging in a poly-social-media context: How and why users navigate multiple social media platforms. In: *Journal of Computer-Mediated Communication* 24, 1, p. 21-35

Taş, Serpil & Arnold, René (2019). Auswirkungen von OTT-1-Diensten auf das Kommunikationsverhalten – Eine nachfrageseitige Betrachtung. WIK. Retrieved from: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_440.pdf.

Taş, Serpil; Wiewiorra, Lukas & Schneider, Anna (2021). Let‘s stay home! Kommunikationsverhalten und Mediennutzung in Deutschland. Retrieved from: https://www.wik.org/fileadmin/Studien/2021/Kommunikationsverhalten.pdf.

Telegram (2022). Telegram Ad Platform Explained. Retrieved from: https://promote.telegram.org/getting-started. 2022/07/06: 2022/07/06

TestingStandards.co.uk (o.J.). Discussion & Review. Retrieved from: http://www.testingstandards.co.uk/interop_et_al.htm. 2022/04/01: 2022/04/01

Thanos, Costantino (2014). Mediation: the technological foundation of modern science. In: *Data Science Journal* 13, p. 88-105

Tiwana, Amrit & Konsynski, Benn (2010). Complementarities between organizational IT architecture and governance structure. In: *Information Systems Research* 21, 2, p. 288-304

Tiwana, Amrit; Konsynski, Benn & Bush, Ashley A (2010). Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. In: *Information systems research* 21, 4, p. 675-687

Twitter (2022). Twitter API Documentation. Retrieved from: https://developer.twitter.com/en/docs/twitter-api. 2022/07/06: 2022/07/06

Tyntec (2022). tyntec | APIs for Messaging, Chat Apps, Number Data, and Authentication | tyntec. Retrieved from: https://www.tyntec.com/. 2022/07/06: 2022/07/06

Unger, Nik; Dechand, Sergej; Bonneau, Joseph; Fahl, Sascha; Perl, Henning; Goldberg, Ian & Smith, Matthew (2015). SoK: Secure Messaging. In: *2015 IEEE Symposium on Security and Privacy*. p. 232-249

US Kongress (2018). H.R.4943 - CLOUD Act: Clarifying Lawful Overseas Use of Data Act or the CLOUD Act. In: p.

Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian & Holz, Thorsten (2019). (Un) informed consent: Studying GDPR consent notices in the field. In: *Proceedings of the 2019 acm sigsac conference on computer and communications security*. p. 973-990

van Wegberg, Marc (2004). Compatibility choice by multi-market firms. In: *Information Economics and Policy* 16, 2, p. 235-254

VZBV (2021). INTEROPERABILITÄT BEI MESSENGERDIENSTEN. Retrieved from.

Wegner, Peter (1996). Interoperability. In: *ACM Computing Surveys (CSUR)* 28, 1, p. 285-287

WhatsApp (2021). WhatsApp Security Whitepaper. Retrieved from: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf. 2022/05/18: 2022/05/18

WhatsApp (2022). Für Unternehmen wird der Start mit WhatsApp jetzt noch einfacher – ganz egal, wie groß sie sind. Retrieved from: https://blog.whatsapp.com/making-it-easier-for-businesses-of-all-sizes-to-get-started-on-whatsapp. 2022/05/19: 2022/05/19

Wheeler, Brian (2018). Brexit: UK government's battle with Apple over EU citizens app. In: *BBC News*. p.

Wolfangel, Eva (2021). Datenschutz: Wie sicher sind Telegram und andere Messenger? Retrieved from: https://www.spektrum.de/news/sicherheitsluecken-beim-messenger-telegram-gefunden/1936957. 2022/05/18: 2022/05/18

Wooden, Andrew (2022). EU messaging interoperability demands raise concerns. Retrieved from: https://telecoms.com/514443/eu-messaging-interoperability-demands-raise-concerns/. 2022/03/29/: 2022/03/29/

Wright, Julian (2004). One-Sided Logic in Two-Sided Markets. In: *Review of Network Economics* 3, 1, p. 44-64

Yurieff, Kaya (2020). Facebook takes a big step in linking Instagram, Messenger and WhatsApp. Retrieved from: https://www.cnn.com/2020/09/30/tech/instagram-messenger-messaging/index.html. 2022/04/01: 2022/04/01

Zingales, Luigi & Rolnik, Guy (2017). A Way to Own Your Social-Media Data (Opinion). In: *The New York Times*. p.