Wiewiorra, Lukas et al.

Research Report

Interoperabilitätsvorschriften für digitale Dienste: Bedeutung für Wettbewerb, Innovation und digitale Souveränität insbesondere für Plattform- und Kommunikationsdienste

WIK-Consult Bericht

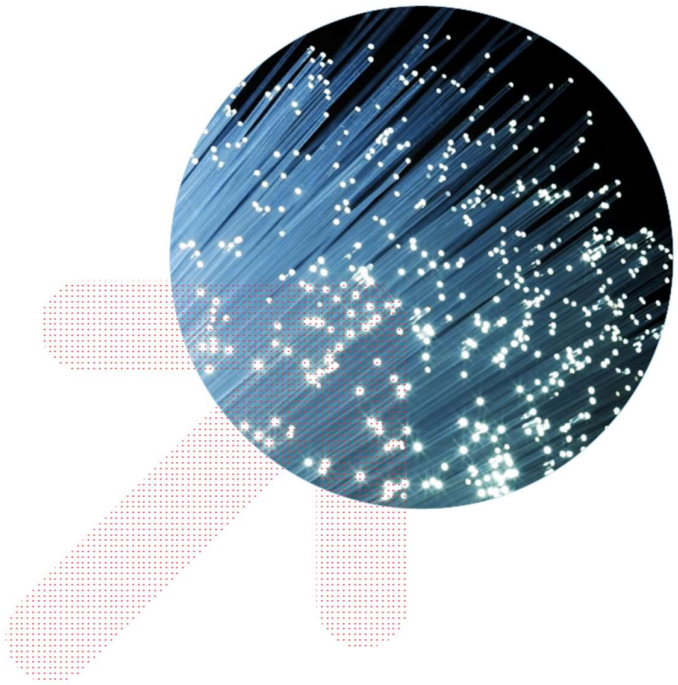
Provided in Cooperation with:
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef

Suggested Citation: Wiewiorra, Lukas et al. (2022) : Interoperabilitätsvorschriften für digitale Dienste: Bedeutung für Wettbewerb, Innovation und digitale Souveränität insbesondere für Plattform- und Kommunikationsdienste, WIK-Consult Bericht, WIK-Consult GmbH, Bad Honnef

This Version is available at:
https://hdl.handle.net/10419/265393

WIK-Consult • Bericht

Studie für die Bundesnetzagentur



Interoperabilitätsvorschriften für digitale Dienste

Bedeutung für Wettbewerb, Innovation und digitale Souveränität insbesondere für Plattform- und Kommunikationsdienste

Autoren:

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

Danksagung

Die Autoren bedanken sich bei Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum), Prof. Dr. Rainer Böhme (Universität Innsbruck) und Prof. Dr. Joachim Posegga (Universität Passau) für ihre Kommentare und Einschätzungen zur Ende-zu-Ende-Verschlüsselung.

Impressum

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

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin	Dr. Cara Schwarz-Schilling
Direktor	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzender des Aufsichtsrates	Dr. Thomas Solbach
Handelsregister	Amtsgericht Siegburg, HRB 7043
Steuer-Nr.	222/5751/0926
Umsatzsteueridentifikations-Nr.	DE 329 763 261

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kurzfassung

Im Rahmen dieser Studie wird mangelnde ***Interoperabilität (IOP)*** als potenzielle Ursache bzw. Treiber für Konzentrationstendenzen, aber auch als mögliche Abhilfemaßnahme in bereits konzentrierten digitalen Märkten beleuchtet. Basierend auf den gewonnenen Erkenntnissen werden anschließend die Notwendigkeit und die möglichen Auswirkungen von IOP-Vorschriften für digitale Dienste in den Bereichen Plattformökonomie und Online-Kommunikationsdienste bzw. im Besonderen für nummernunabhängige interpersonelle Kommunikationsdienste, engl. Number-independent Interpersonal Communications Services (NI-ICS), untersucht.

Grundlagen

Der in der Implementierung befindliche ***Beschluss des DMA (Digital Markets Act)*** sieht neben Regelungen im Bereich von Hard- und Softwarefunktionalitäten eine IOP-Verpflichtung für Basisfunktionalitäten für Anbieter von NI-ICS vor. Auf eine Verpflichtung im Bereich Social Media wurde hingegen vorerst verzichtet. Ähnliche Bestrebungen befinden sich unter anderem in den Vereinigten Staaten (ACCESS Act), dem Vereinigten Königreich und Australien in der Ausarbeitung.

IOP wird dabei als Austausch von Informationen und insbesondere auch als deren gegenseitige Nutzbarmachung zur Herstellung von Funktionalitäten verstanden. Allgemein ergibt sich beim Begriffsverständnis und den verschiedenen Konzepten von IOP aus technischer, rechtlicher und ökonomischer Perspektive ein breites, teils uneinheitliches Bild. IOP geht insbesondere über die punktuelle, meist einseitige, Datenportabilität hinaus und grenzt sich von dieser durch einen kontinuierlichen, meist wechselseitigen, Datenaustausch ab. Diese Form wird auch als Daten-IOP bezeichnet, während die Protokoll-IOP stärker auf eine grundlegende Zusammenschaltung und den Funktionalitätsaustausch abzielt. Neben dieser wechsel- bzw. zweiseitigen IOP finden sich aber auch einseitige Formen von IOP, wie z. B. das Teilen von externen Medieninhalten auf Social Media Plattformen oder die sogenannte adversariale (feindliche) IOP durch Reverse Engineering.

Während in der Plattformökonomie neben dem Angebot gleichartiger Dienste insbesondere viele Up- und Downstreamverflechtungen zwischen unterschiedlichen Wertschöpfungsstufen vorzufinden sind, handelt es sich z. B. bei Online-Kommunikationsdiensten um eine primär horizontale Beziehung der unterschiedlichen Anbieter. Horizontale IOP betrifft damit Firmen bzw. Dienste im direkten Wettbewerb und kann damit ggf. für eine Teilung direkter Netzwerkeffekte sorgen. Bei vertikaler IOP sind im Gegensatz dazu Firmen bzw. Dienste in vor- und nachgelagerten Wertschöpfungsstufen betroffen, welche durch IOP Zugriff auf eine Wertschöpfungsstufe erlangen können, womit die Teilung indirekter Netzwerkeffekte erreicht werden kann.

Interoperabilitätsverpflichtungen

Das grundsätzliche Argument für ***horizontale IOP-Verpflichtungen*** besteht darin, dass es Nutzern ermöglicht werden soll, alternative Anbieter zu nutzen, ohne dabei den Zugang zu Interaktionspartnern zu verlieren, die ausschließlich bzw. hauptsächlich den Dienst eines (dominanten) Anbieters nutzen. Eine pro-kompetitive Wirkung besteht durch die Auflösung der Firmenbezogenheit von Netzwerkeffekten bzw. von netzwerkbedingten Lock-in-Effekten sowie einer Reduktion des Market-tipping-Risikos. Horizontale IOP kann aber auch anti-kompetitiv wirken, da eine Homogenisierung Differenzierungs- und Innovationsmöglichkeiten einschränkt und sie ggf. bestehende Anreize zum Multi-Homing reduziert. Es ist ex ante unklar welche der Effekte schlussendlich dominieren.

Im Hinblick auf IOP-Verpflichtungen im horizontalen Wettbewerb zwischen relativ homogenen Diensten und Gütern ist daher Vorsicht geboten. Je nach Marktstruktur und -umfeld kann insbesondere durch die Möglichkeit und kundenseitige Ausübung von Multi-Homing wettbewerblicher Druck auch ohne IOP bzw. IOP-Verpflichtungen entstehen. Wenn Multi-Homing ohne nennenswerte Kosten möglich ist, sind die möglichen Wohlfahrtsgewinne von IOP begrenzt. Horizontale IOP birgt hingegen Risken für die Innovationsanreize der beteiligten Unternehmen, da Wettbewerb *um* den Markt durch Wettbewerb *im* Markt abgelöst wird und der derzeitige technische Entwicklungsstand festgeschrieben wird. Weiterentwicklungen sind insbesondere bei festgelegten technischen Standards weniger dynamisch und durch marktweit geteilte Netzwerkeffekte weniger attraktiv. Zusätzlich können mögliche IOP-Verpflichtungen auf horizontaler Ebene entstehende Wettbewerbsvorteile abschwächen und so wichtige Innovationsrenten reduzieren. IOP führt zu einer geringeren Produktvielfalt zwischen horizontal konkurrierenden Produkten und impliziert damit eine schlechtere Übereinstimmung von Produkteigenschaften und Konsumentenpräferenzen. Der resultierende negative Wohlfahrtseffekt ist besonders bedeutend, wenn Konsumentenpräferenzen stark ausgeprägt sind.

Durch ***vertikale IOP-Verpflichtungen*** können modulare Kombinationsmöglichkeiten über vor- und nachgelagerte Wertschöpfungsstufen hinweg erleichtert und entsprechende Innovationsanreize geschaffen werden. Dies betrifft insbesondere den Fall von etablierten vertikal integrierten Firmen. Allerdings kann ein „zu offener“ Zugang die Anreize für (radikale) Innovationen bei Drittanbietern und Plattformen selbst hemmen.

IOP-Verpflichtungen in vertikalen Strukturen sind aber tendenziell positiv zu bewerten. Vertikale IOP schafft Planungssicherheit über zur Verfügung stehende technische (Programmier-)Schnittstellen (APIs) und fördert Innovationen komplementärer Anbieter. Ebenso sichern verpflichtende vertikale IOP-Standards die Erreichbarkeit der gesamten Nutzerbasis eines Marktes und vergrößern so das Nachfragepotenzial auf vor- und nachgelagerten Märkten.

Neben den Umsetzungskosten von IOP, die für kleinere Anbieter eine Markteintrittshürde darstellen können, bestehen bei der Standardisierung allgemein außerdem Gefahren

durch Kollusion und eine Einflussnahme von dominanten Akteuren, z. B. durch die strategische Platzierung von Patenten. In puncto digitaler Souveränität kann IOP durch die Reduktion von Lock-in-Effekten einerseits Wahlfreiheit und Selbstbestimmung von Verbrauchern ermöglichen, andererseits die Kontrolle über die Datenverarbeitung erschweren, insbesondere falls in einem interoperablen Netzwerk auch Anbieter Zugriff auf (Meta-)Daten haben, zu denen der Nutzer in keiner direkten Geschäftsbeziehung steht. Auch die Wirkungen auf die Souveränitätsdimensionen der Cybersicherheit und strategischer Aspekte sind ambivalent.

Interoperabilität bei NI-ICS

Die ***Einordnung und Definition von NI-ICS***, die unter anderem als Grundlage für die IOP-Verpflichtung von Messaging-Diensten im Rahmen des DMA dient, weist im Rahmen moderner Online-Kommunikationsdienste noch juristische Unklarheiten auf. Eine Einschätzung, ob z. B die Privatnachrichtenfunktion des Dienstes Instagram als untergeordnete Nebenfunktion von Instagram als sozialem Netzwerk anzusehen ist, lässt sich nicht immer basierend auf technischen Kriterien bestimmen und hängt unter Umständen von den dynamischen Nutzungsgepflogenheiten der Nutzer ab. Die Abgrenzung wird außerdem durch die Verbreitung von Diensten, die zu vertikal integrierten Ökosystemen gehören, sowie durch ein breites Angebot an Funktionalitäten erschwert. So bietet der Dienst Telegram zwar Funktionen, die, vergleichbar mit sozialen Medien, Informationen einer unbestimmten Anzahl von Personen in offenen Kanälen zugänglich machen, wird aber in großen Teilen auch analog zu WhatsApp oder Signal für die bilaterale oder private Kommunikation in Gruppen genutzt.

WhatsApp und die ebenfalls zum Meta-Konzern gehörigen Dienste Facebook Messenger und Instagram Messages stellen insbesondere in Europa die beliebtesten Online-Kommunikationsdienste dar. Eine Sonderauswertung der jährlichen Umfrage des WIK zur Nutzung von Online-Kommunikationsdiensten im Rahmen dieser Studie zeigt, dass 80% der Nutzer in Deutschland mindestens einen dieser drei Dienste verwenden. Dienste anderer Unternehmen nutzen jeweils nur bis zu 30% der Befragten (Microsoft-Dienste), oder weit weniger (sonstige Dienste).

Der hohe Anteil von ***Multi-Homing*** auf der Diensteebene (75% der Anwender nutzen mindestens zwei Dienste, im Durchschnitt werden 3,7 Dienste verwendet) wird durch die Aggregation auf die bereitstellenden Unternehmen teilweise relativiert. Noch 61% der Nutzer verwenden Dienste unterschiedlicher Unternehmen und im Durchschnitt werden immerhin noch 2,8 Dienste von unterschiedlichen Unternehmen genutzt. Eine internationale empirische Studie zeigt, dass trotz der gestiegenen Installationszahlen alternativer Dienste nur etwa 0,5% der Nutzer tatsächlich WhatsApp deinstallierten. Dennoch kann ein hoher Anteil an Multi-Homing zu einer Disziplinierung der Marktmacht eines dominanten Anbieters beitragen, da so ein schnellerer und unkomplizierter Wechsel zwischen Kommunikationskanälen ermöglicht wird.

Alle Regelungen des DMA sind asymmetrisch gegenüber dominanten sogenannten „Gatekeepern“ auferlegt, so dass es alternativen Anbietern freigestellt bleibt, ob sie IOP gegenüber Gatekeepern oder auch untereinander anstreben möchten. Insbesondere einer branchenweiten, symmetrischen Regelung standen Marktteilnehmer und -beobachter im Vorfeld kritisch gegenüber, da fehlende Differenzierungsmöglichkeiten und ausbleibendes Innovationspotenzial durch eine zu starke Homogenisierung befürchtet wurden. Auch in Bezug auf die Funktionalität beschränkt sich die Verpflichtung auf die Basisfunktionalität des Austauschs von Nachrichten und Dateien zwischen Einzelnutzern, die zeitlich gestaffelt noch um Gruppenchats und Anrufe erweitert wird. Eine gestaffelte Entwicklung birgt aber die Gefahr, dass die Planung für den Entwicklungspfand unvollständig vorgenommen bzw. von der dynamischen Marktentwicklung überholt wird und später nötige Anpassungen umso aufwendiger werden. Für Anbieter besteht zwar weiterhin die Möglichkeit, sich mit unabhängigen Angeboten oder Zusatzfunktionalitäten abzuheben, was allerdings auch das ursprüngliche Ziel von horizontaler IOP, der Auflösung firmenspezifischer Netzwerkeffekte, beeinträchtigt.

Neben der freiwilligen Entscheidung für alternative Anbieter wird auch der Erhalt der Wahlfreiheit für Nutzer hervorgehoben, welche jedoch den praktischen Nutzen der IOP ggf. weiter einschränkt. Endnutzer sowohl des Gatekeepers als auch eines IOP anfragenden Anbieters sollen dabei frei in ihrer Entscheidung bleiben, die Funktionen interoperabel zu nutzen oder nicht. Die Nutzer können damit z.B. entscheiden, ob sie für Nutzer des jeweilig anderen Anbieters tatsächlich erreichbar (und auffindbar) sein möchten. Aus Datenschutzsicht erfordert dies voraussichtlich ein granulares Opt-in-Modell, dessen Ausgestaltung allerdings in der praktischen Umsetzung große Herausforderungen im Hinblick auf Komplexität und Usability aufwirft.

Der Gesetzestext legt insgesamt einen hohen Wert auf den Erhalt von Datensicherheit und Datenschutz, während hier im Vorfeld vor einem Absinken auf einen „kleinsten-gemeinsamen-Nenner“ gewarnt wurde. Dazu gehört ein Datensparsamkeitsgebot, in dem die Sammlung und der Austausch von Daten ausschließlich auf das nötige Niveau zur Gewährleistung einer effektiven IOP zu beschränken ist. Das gleiche Schutzniveau, welches für eigene Nutzer angeboten wird, muss auch für die IOP mit externen Anbietern gelten. Dazu gehört explizit auch der Erhalt einer ggf. bestehenden Ende-zu-Ende-Verschlüsselung. Diese Regelung lässt sich dahingehend verstehen, dass die Beibehaltung des Sicherheitsniveaus eine Voraussetzung für die Öffnung eines Gatekeeper-Dienstes gegenüber anderen Anbietern ist. Inwiefern diese Konsequenz in der praktischen Umsetzung beibehalten werden kann, ist aufgrund der technischen Komplexität bei der Vereinbarung von IOP und Ende-zu-Ende-Verschlüsselung aber höchst fraglich.

Bestehende Entwickler von eigenen Messaging-Standards und Aggregationsdiensten anhand von sogenannten Bridges („Übersetzer“ zwischen verschiedenen Protokollen) wie Matrix und Beeper haben bereits ihr Interesse an einer Inanspruchnahme der IOP-Verpflichtung bekundet, während sich alternative Messenger wie Signal und Threema

kritisch positionierten und eine Zusammenarbeit mit anderen Diensten weiterhin mit Verweis auf die Datenschutz- und Sicherheitsrisiken ablehnen.

Wie das Beispiel des Meta-Konzerns zeigt, der die 2019 angekündigte Ende-zu-Ende-verschlüsselte IOP zwischen seinen eigenen Diensten bis heute nicht vollständig implementieren konnte, ist bereits die Verschlüsselung zwischen Diensten eines Konzerns eine Herausforderung. Auch laut von im Rahmen dieser Studie befragten Experten für Verschlüsselungstechnologien kann es hier ohne vollständige Standardisierung bzw. Nutzung eines gemeinsamen Standards letztendlich keine echte Ende-zu-Ende-Verschlüsselung unter IOP geben.

Allgemein wird der Aufwand einer Einigung auf eine vollständige Standardisierung als extrem hoch eingeschätzt, da dieser einer Entwicklung einer vollständig neuen Messenger-Plattform gleichgesetzt werden kann. Die Implementierung von IOP bei Ende-zu-Ende verschlüsselten Diensten bzw. Funktionen könnte daher noch mehrere Jahre entfernt sein. Für eine vollständige Standardisierung wird der zeitliche Aufwand von einigen befragten Experten auf mehrere Jahre (bis zu 5) beziffert. Der Implementierungs- und Standardisierungsaufwand steigt dabei jeweils deutlich von bilateralen Textnachrichten zu Gruppenchats und Audio- und Videochats an.

Zudem besteht nicht zuletzt für den Gesetzestext des DMA die Problematik, dass die Begriffe eines „Sicherheitsniveaus“ und auch der „Ende-zu-Ende-Verschlüsselung“ keiner einheitlichen oder objektiven Definition unterliegen. Je nach Anwendung und deren Nutzenversprechen, Nutzer(basis) und Infrastruktur können teils stark unterschiedliche „Enden“, Angriffs- und Angreifermodelle relevant sein, die auch unterschiedliche Abwägungen auf technischer Ebene implizieren. So sind einheitliche technische Lösungen zwar auf einer abstrakten Ebene grundsätzlich denkbar, stoßen aber im Detail und der praktischen Implementierung an ihre Grenzen. Entsprechende Kompromisse und eine Erweiterung der beteiligten Parteien und Akteure implizieren daher letztendlich auch eine Erweiterung möglicher Angriffspunkte und bedingen damit im Zweifel ein Absinken von Sicherheitsniveaus.

In der Beschlussversion des DMA ist die Erfüllung der IOP-Vorschriften via Schnittstellen/APIs vorgesehen, allerdings wird sich eine umfassendere Standardisierungsvorgabe für die Zukunft vorbehalten. In Anbetracht der Komplexität könnte ein abgestimmter vollständiger Entwicklungsansatz langfristig günstiger zu besseren Ergebnissen führen als die teilweise und gestaffelte Implementierung. Gegen eine Standardisierung wiederum sprechen aber unter anderem ein ebenfalls hoher Aufwand, die mögliche Verhinderung von Innovationen und aus dem Findungsprozess resultierende Risiken wie eine strategische Einflussnahme von dominanten Akteuren.

Folglich müsste insbesondere im Fall der Implementierung von IOP mit Hilfe von Schnittstellen/APIs das bestehende Sicherheitsniveau letztendlich aufgeweicht werden, oder

eine Einigung auf einen (evtl. bereits bestehenden proprietären) Verschlüsselungsstandard erfolgen. Die letzte Variante wäre für die betreffenden Unternehmen allerdings mit hohen Wechselkosten verbunden, was die Attraktivität von IOP für alternative Anbieter drastisch verringert. Dabei ist zu berücksichtigen, dass bei einer Ablehnung von IOP durch alternative Anbieter deren Nutzer nicht von den potenziellen Vorteilen einer solchen Lösung profitieren können. Daher ist eine attraktive Lösung mit breiter Akzeptanz als zielführend anzusehen. Sollte im Gegensatz dazu eine einfacher zu implementierende Lösung unter Aufweichung des ursprünglich bestehenden Sicherheitsniveaus gewählt werden, ist es allerdings ebenso unklar, ob Unternehmen mit einem derzeit hohen Sicherheitsniveau eine solche Lösung implementieren würden und ob Nutzer (falls eine Implementierung vorgenommen wird) dann von dieser Möglichkeit Gebrauch machen würden.

Es bleibt daher in der Gesamtabwägung fraglich, wie der im DMA verfolgte Ansatz und allgemein eine IOP-Verpflichtung für Messaging-Dienste zielführend umgesetzt werden kann. In Anbetracht der möglichen Risiken scheint eine enge regulatorische Begleitung geboten, um unerwünschte Nebeneffekte für Verbraucher, Wettbewerb und Innovation möglichst gering zu halten. Letztlich steht im Fokus aller IOP-Vorschriften ein potenzielles Marktversagen, welches durch die Herstellung von IOP überwunden werden könnte. Sollten wie im Fall von Messaging-Diensten das Niveau von Multi-Homing vergleichsweise hoch und die Kosten von Multi-Homing gering sein, ist grundsätzlich von einem eher geringen Wohlfahrtsverlust für Verbraucher auszugehen, wenn ein anbieterübergreifender, interoperabler Austausch nicht möglich ist. Demgegenüber stehen für eine Implementierung von IOP-Verpflichtungen sowohl durch Schnittstellen oder Standards eine Reihe von Kosten und Risiken wie eine Reduktion von Multi-Homing, Innovationsanreizen, Sicherheitsniveaus inklusive der Ende-zu-Ende-Verschlüsselung und Usability. Damit besteht die Gefahr, dass solche Vorhaben in interoperablen Systemen münden, welche unter hohem zeitlichen und finanziellen Aufwand entwickelt werden müssen, aber letztlich am Markt nicht angenommen werden. Darüber hinaus entstehen (regulatorische) Kosten für die kontinuierliche Überwachung und Einhaltung der IOP-Vorgaben und die Aufrechterhaltung und Pflege der entsprechenden Schnittstellen mit hoher Qualität und Verfügbarkeit.

Vor dem Hintergrund der endgültigen Verabschiedung des DMA sollte in jedem Fall darauf geachtet werden, dass die beschriebenen Risiken bei der nun anstehenden praktischen Umsetzung der Verpflichtung bestmöglich regulatorisch minimiert werden und nicht zuletzt der Fokus auf Verbraucheraspekte wie den Erhalt der Verschlüsselung und Datensparsamkeit aufrechterhalten wird.

1 Einleitung

Digitale Dienste wie Handelsplattformen, soziale Netzwerke, Suchmaschinen, Messaging-Dienste, Betriebssysteme oder App Stores haben in den letzten Jahren Einzug in verschiedenste Bereiche des täglichen Lebens gehalten und dabei zahlreiche positive Veränderungen hervorgebracht, indem sie Zugang zu Informationen, Produkten und Dienstleistungen erleichtern oder neue Möglichkeiten bieten, mit Familie und Freunden in Kontakt zu treten. Mit der Entwicklung von großen Internetkonzernen wird das Internet aber zunehmend zentralistischer und bildet immer stärker verzahnte, sich verschließende Ökosysteme und Konzentrationstendenzen heraus (vgl. Lancieri und Sakowski, 2021).

Dabei können Anbieter von geschlossenen und proprietären Diensten durch Netzwerkeffekte und nach Erreichen der kritischen Masse Lock-In-Effekte ausnutzen und dadurch ihre Marktmacht weiter steigern. Auch über vertikale Wertschöpfungsstufen hinweg kann mangelnder Zugang die Entstehung komplementärer Dienste und Konkurrenz auf vor- und nachgelagerten Märkten verhindern. Dies kann sowohl die unmittelbaren Funktionen von Diensten wie NI-ICS (nummernunabhängiger interpersoneller Kommunikationsdienst, engl. Number-independent Interpersonal Communications Service) betreffen, als auch die Einbindung dieser Dienste in das weitreichendere digitale Ökosystem der Plattformbetreiber (z. B. Smart-Home, Streaming-Angebote, soziale Netzwerke etc.). Dies könnte wiederum dazu führen, dass negative Wohlfahrtseffekte entstehen, da Kunden keine alternativen Angebote nutzen, verschlechterte Nutzungsbedingungen hinnehmen, oder Anbieter geringere Investitions- und Innovationsanreize haben.

Im Rahmen dieser Studie soll daher mangelnde Interoperabilität (IOP) als potenzielle Ursache bzw. Treiber für Konzentrationstendenzen und damit verbundene negative Wohlfahrtseffekte, aber auch als mögliche Abhilfemaßnahme in bereits konzentrierten digitalen Märkten beleuchtet werden. Basierend auf den gewonnenen Erkenntnissen sollen in dieser wissenschaftlichen Studie anschließend die potenzielle Notwendigkeit und die möglichen Auswirkungen von IOP-Vorschriften für digitale Dienste in den Bereichen Plattformökonomie und Online-Kommunikationsdienste bzw. im Besonderen NI-ICS untersucht werden. Ein Schwerpunkt liegt hierbei insbesondere auf den Auswirkungen von IOP-Vorschriften für den Wettbewerb, die Innovationstätigkeit und die Verwirklichung von Aspekten der digitalen Souveränität in Form eines selbstbestimmten Handelns der Marktteilnehmer.

Die Studie ist wie folgt aufgebaut. Kapitel 2 bietet einen grundlegenden Überblick über IOP. Dabei wird der Begriff in Bezug auf verwandte Konzepte eingeordnet und abgegrenzt und das Verständnis im Rahmen dieser Studie definiert. Anschließend werden verschiedene Arten, Ausprägungen und Implementierungsformen von IOP dargelegt. Außerdem diskutiert das Kapitel grundlegende Zusammenhänge und Auswirkungen von IOP auf Wettbewerbsprozesse, Innovationsanreize und Verbraucheraspekte.

Kapitel 3 befasst sich mit IOP im allgemeinen Kontext digitaler Plattformen und Dienste und analysiert dabei die mögliche Rolle von IOP in der Plattformökonomie. Diskutiert wird hier sowohl der Status quo von IOP in der Plattformökonomie, ein potenziell bestehender Mangel an IOP, sowie mögliche IOP-Verpflichtungen als Abhilfemaßnahme. Den erwünschten positiven Wirkungen von IOP werden dabei die identifizierten Risiken gegenübergestellt und verschiedene Marktkonstellationen erörtert, die eine entsprechende Abwägung beeinflussen können. Darauf aufbauend wird ein Prüfschema zur Bewertung von möglichen IOP-Vorschriften im Kontext digitaler Dienste aufgestellt. Außerdem werden technische und prozedurale Aspekte und Hürden für (die Einführung von) IOP dargelegt.

In Kapitel 4 liegt der Fokus auf Online-Kommunikationsdiensten und insbesondere auf NI-ICS, für die im Rahmen des Digital Markets Act (DMA) eine teilweise Verpflichtung zur IOP vorgesehen ist. Zunächst werden Online-Kommunikationsdienste und NI-ICS voneinander abgegrenzt und die aktuelle Marktsituation beschrieben. Bezugnehmend auf das Prüfschema aus Kapitel 3 werden spezifische Marktcharakteristika und ökonomische Besonderheiten herausgearbeitet. Insbesondere werden technische Aspekte erörtert, die für verschiedene Implementierungsansätze von IOP in diesem Marktsegment nötig wären. Dabei liegt der Fokus auf der Frage, ob und wie diese Ansätze von IOP mit der Ende-zu-Ende-Verschlüsselung vereinbar sind. Für die verschiedenen Ansätze zur Umsetzung von IOP wird eine Bewertung anhand ökonomischer, technischer und juristischer Aspekte vorgenommen und der aktuelle Ansatz des DMA eingeordnet.

Kapitel 5 fasst die Schlussfolgerungen der Studie zusammen und bietet einen Ausblick auf zukünftige Entwicklungen.

2 Wirkungsweise verschiedener Interoperabilitätskonzepte

2.1 Interoperabilitätskonzepte

2.1.1 Kompatibilität und Interoperabilität

In technischen Zusammenhängen bezeichnet *Kompatibilität* allgemein das Miteinanderfunktionieren von Teilen. Entsprechend definieren Farrell und Saloner (1986a) in einem frühen Überblicksartikel zu Kompatibilität und Standardisierung Kompatibilität als das Resultat eines koordinierten Produktdesigns. Dabei unterscheiden die Autoren zwischen drei Klassen von Kompatibilität:

- *Physische Kompatibilität* (z. B. Kameras und Linsen, Autos und Zapfsäulen, Fernseher und Sendesysteme etc.)
- *Kommunikationskompatibilität* (z. B. Telefonsysteme, Straßenschilder, Landessprachen etc.)
- *Kompatibilität durch Konvention* (z. B. Währungen, Zeitzonen, Bankkarten etc.)

Allerdings merken die Autoren dazu an, dass diese Kategorien weder erschöpfend noch trennscharf voneinander sind. Beispielsweise basieren auch Telefonsysteme und Straßenschilder auf Kompatibilität durch Konventionen. Darüber hinaus hängt nach der Auffassung der Autoren Kompatibilität auch davon ab, ob Produkte desselben Herstellers betrachtet werden, oder Produkte von unterschiedlichen Herstellern. Insbesondere bei der Verwendung von Produkten unterschiedlicher Hersteller kann auch nur partielle Kompatibilität bestehen. Damit haben die Autoren bereits viele Aspekte dieser Thematik tangiert, welche in späteren Forschungsarbeiten weiter konkretisiert und geschärft wurden.

Im Kontext digitaler Produkte und Dienste kann IOP allgemein als die Fähigkeit von zwei oder mehr Softwarekomponenten definiert werden, trotz Unterschieden in Sprache, Schnittstelle und Ausführungsplattform zusammenzuarbeiten (Wegner, 1996, S. 1). Die Konzepte Kompatibilität und IOP werden dabei häufig synonym oder zumindest nicht trennscharf verwendet. Im Folgenden sollen daher unterschiedliche Definitionen von IOP vorgestellt werden, um daraus eine Arbeitsdefinition für diese Studie herauszuarbeiten.

Im Verzeichnis der Fachbegriffe für den Bereich System- und Softwareentwicklung der ISO/IEC/IEEE (ISO, 2017, S. 79) wird ***Kompatibilität*** unter anderem definiert als „Grad, in dem ein Produkt, System oder eine Komponente Informationen mit anderen Produkten, Systemen oder Komponenten austauschen oder seine erforderlichen Funktionen ausführen kann, während es *dieselbe Hardware- oder Softwareumgebung* nutzt“, sowie „die Fähigkeit von *zwei oder mehr Systemen* oder Komponenten, Informationen *auszutauschen“*. Andere Definitionen beziehen sich explizit auf den Aspekt das technische

Komponenten dann miteinander kompatibel sind, solange sich beide in derselben Umgebung (z. B. Betriebssystem) befinden, *ohne das Verhalten der jeweils anderen Komponente zu beeinträchtigen*. (TestingStandards.co.uk, o.J.) Dies impliziert beispielsweise, dass zueinander kompatible Software auf demselben Endgerät ohne Konflikte funktionieren kann, jedoch noch nicht notwendigerweise die Funktionalität zwischen den beiden Softwarekomponenten oder über verschiedene Endgeräte hinweg sichergestellt sein muss. Allerdings kann Kompatibilität auch eine übergreifende Funktionalität zwischen z. B. unterschiedlichen Software- und Betriebssystemversionen oder sogar Endgeräten beinhalten. Der Datenbankanbieter Oracle bezeichnet Kompatibilität beispielsweise als die Fähigkeit von Systemen mit unterschiedlichen Versionen (oder Releases) zu interoperieren (Vorwärts- und Rückwärtskompatibilität) (Oracle, 2010).

IOP wird im Verzeichnis der Fachbegriffe für den Bereich System- und Softwareentwicklung der ISO/IEC/IEEE (ISO, 2017, S. 237) definiert als „Grad, in dem zwei oder mehr Systeme, Produkte oder Komponenten Informationen *austauschen und die ausgetauschten Informationen nutzen können",* sowie „die Fähigkeit von Objekten *zur Zusammenarbeit* d. h. die Fähigkeit, gegenseitig Informationen zu kommunizieren, um Ereignisse, Vorschläge, Anfragen, Ergebnisse, Verpflichtungen und Flüsse auszutauschen." IOP fokussiert sich nach dieser Definition nicht spezifisch auf die Funktionalität innerhalb einer Hardware- oder Softwareumgebung und greift darüber hinaus explizit den Aspekt der Nutzbarkeit der zwischen Systemen, Produkten oder Komponenten ausgetauschten Informationen und damit der *Zusammenarbeit von Systemen* auf. Der Datenbankanbieter Oracle bezeichnet IOP als die Fähigkeit von Systemen derselben Version (oder Releases) zusammenzuarbeiten (Oracle, 2010).

In diesem technischen Kontext bezieht sich Kompatibilität daher häufig nur auf die Austauschbarkeit unterschiedlicher abhängiger Komponenten (z. B. neuer/älter, Variante A/B) in einer Umgebung zur Erreichung einer spezifischen Funktionalität, sowie dem störungsfreien Nebeneinander von Komponenten innerhalb derselben technischen Umgebung, welche funktional auch voneinander unabhängig sein können. Im Fall von Vorwärts- oder Rückwärtskompatibilität werden häufig zusätzliche Technologien notwendig, sogenannte Adapter oder Konverter (siehe Kapitel 2.1.2), welche zwischen den divergierenden Versionen oder Ausführungen von Technologien vermitteln.

Obwohl IOP häufig synonym mit Kompatibilität verwendet wird, stellt dieses Konzept gezielter auf die Zusammenarbeit von Systemen in unterschiedlichen Umgebungen und die Nutzbarkeit der übertragenen Informationen über Systemgrenzen hinweg ab. Dem Konzept von IOP liegt daher je nach Definition bereits die Voraussetzung eines gemeinsamen Standards zugrunde.

In einer allgemeinen Analyse von IOP im Kontext datenzentrierter Forschungsaktivitäten identifiziert Thanos (2014) zur Erreichung von IOP zwischen zwei Entitäten[1] unterschiedliche Konzepte die IOP bedingen können:

- Austauschfähigkeit (Exchangeability): Die beiden Entitäten müssen in der Lage sein, *sinnvolle Informationen* auszutauschen.
- Kompatibilität (Compatibility): Die beiden Entitäten müssen in der Lage sein, *logisch konsistente Informationen* auszutauschen (wenn die ausgetauschten Informationen eine Beschreibung von Funktionalitäten, Richtlinien oder Verhalten sind).
- Usability: Die Benutzerinstanz muss in der Lage sein, die *ausgetauschten Informationen zu nutzen*, um eine Reihe von Aufgaben auszuführen, die von der Nutzung dieser Informationen abhängen (Thanos, 2014, S. 89).

Um einen sinnvollen Informationsaustausch zwischen zwei Entitäten im Sinne einer Austauschfähigkeit zu gewährleisten, müssen drei Arten von Heterogenität überwunden werden. Erstens, die Heterogenität zwischen Datenformaten und den Sprachen, welche zur Abfrage der Daten genutzt werden (syntaktische Austauschfähigkeit); zweitens, Heterogenität zwischen den Datenmodellen (strukturelle Austauschfähigkeit); drittens, Heterogenität in der Semantik, welche beispielsweise Dimensionen wie Granularität, Umfang, Zeit, Synonyme, Homonyme etc. beschreibt (semantische Austauschfähigkeit). Wenn die alleinige Austauschfähigkeit ausreicht, um die Nutzereinheit in die Lage zu versetzen eine Reihe von Aufgaben auf der Grundlage der ausgetauschten Informationen zu erfüllen, wird von „grundlegender IOP“ gesprochen.

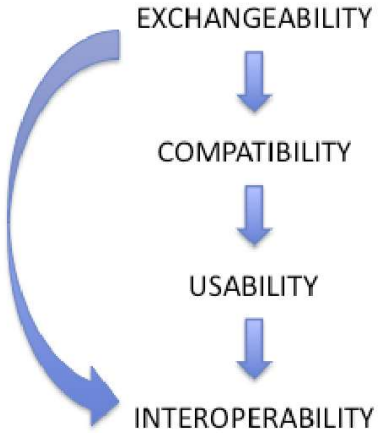
Kompatibilität stellt zusätzlich sicher, dass keine Diskrepanzen z. B. auf der funktionalen Ebene, im Verhalten und der Geschäftslogik auftreten. Kompatibilität bedeutet also, dass die erste Bedingung (Austauschfähigkeit) erfüllt ist, sowie logische Konsistenz in allen für die Zusammenarbeit relevanten Dimensionen vorliegt. Eine Prüfung auf Kompatibilität erfordert daher zunächst eine Beschreibung der statischen Merkmale eines Dienstes. Damit werden allerdings nur die abstrakten Fähigkeiten eines Dienstes beschrieben, nicht aber unter welchen Voraussetzungen und Umständen der Dienst tatsächlich erbracht werden kann. Daher muss ebenfalls eine Beschreibung der dynamischen Eigenschaften eines Dienstes vorliegen. Diese beschreiben welche Informationen bzw. konkreten Bedingungen für die Erbringung eines Dienstes erforderlich sind. Damit impliziert Kompatibilität jedoch nicht notwendigerweise das zwei kompatible Dienste (Komponenten) auch miteinander kombiniert werden können, um z. B. daraus einen neuen Dienst bereitzustellen, wie dies in der Plattformökonomie regelmäßig der Fall ist (Servicekomposition). Kompatibilität ist also keine Garantie für IOP (Thanos, 2014, S. 91).

1 Als Entität wird ein Informationsobjekt in der Datenmodellierung bezeichnet. Damit ist ein eindeutig identifizierbares Objekt gemeint, über das Informationen gespeichert oder verarbeitet werden sollen. Ein solches Objekt kann beispielsweise ein Nutzerkonto, ein Zustand oder sogar ein physischer Gegenstand sein.

„Usability ist gegeben, wenn die wahrgenommene Nützlichkeit und die wahrgenommene Benutzerfreundlichkeit von Daten/Werkzeugen/Diensten eng miteinander verbunden sind“ (Thanos, 2014, S. 92). Das bedeutet, dass die Daten, die von dem Dienst eines Anbieters bereitgestellt werden, auch mit Zusatzinformationen versehen sein müssen, um für andere Anwender nutzbar zu sein. Mit dieser Bedingung sind neben der Genauigkeit, Vollständigkeit, Konsistenz und Aktualität der bereitgestellten Daten selbst auch die Verfügbarkeit und Konsistenz von Metadateninformationen gemeint. Soll ein Dienst beispielsweise von verschiedenen Nutzergruppen oder für verschiedene Anwendungsszenarien verwendet werden, müssen unterschiedliche (bzw. reichhaltigere) Metadateninformationen zur Verfügung gestellt werden um in all diesen Fällen IOP herstellen zu können.

Insgesamt bauen die vorgestellten Bedingungen aufeinander auf. Dies bedeutet, dass Austauschfähigkeit eine notwendige, aber nicht hinreichende Bedingung für Kompatibilität ist. Wenn die alleinige Austauschfähigkeit bereits ausreicht, um eine Entität in die Lage zu versetzen eine Reihe von Aufgaben auf der Grundlage der ausgetauschten Informationen zu erfüllen, kann von *grundlegender IOP* gesprochen werden.[2] Darüber hinaus sind sowohl Austauschbarkeit als auch Kompatibilität notwendige, aber nicht hinreichende Bedingungen für Usability. Nur wenn Austauschbarkeit, Kompatibilität und Usability gewährleistet sind, ist *volle IOP* erreicht. *Damit ist Kompatibilität ein schwächeres Konzept als IOP* (Thanos, 2014, S. 93).

Abbildung 2-1: Hierarchie der Bedingungen für IOP.



Quelle: Thanos (2014, S. 93)

2 Der direkte Pfeil in Abbildung 2-1 verdeutlicht „grundlegende Interoperabilität“ falls Austauschfähigkeit als alleinige Bedingung hinreichend ist.

Während andere Autoren die Begriffe aus ökonomisch-rechtlicher Perspektive auch explizit austauschbar verwenden (Lemley und Samuelson, 2021), übertragen Kerber und Schweitzer (2017) die technische Sichtweise von IOP auf digitale Märkte und definieren IOP im Hinblick auf die *Funktionalität und Zusammenarbeit von Produkten verschiedener Firmen,* während Kompatibilität aus ihrer Sicht typischerweise die Fähigkeit von Produkten ein und desselben Unternehmens bezeichnet miteinander zu funktionieren. Diese Definition kann damit nicht als vollständig konsistent mit der Definition von Thanos (2014) angesehen werden, unterstreicht aber trefflich, dass Usability als Voraussetzung für IOP (nach reiner Kompatibilität), über die Grenzen von Unternehmen hinweg eine größere Herausforderung darstellt als innerhalb eines Unternehmens, da hier bereits relevante Metadaten und das Wissen darüber wie diese korrekt zu interpretieren sind vorliegt. Riley (2020, S. 101) schlussfolgert, dass effektive IOP im Kontext digitaler Märkte damit nicht nur gemeinsame Standards voraussetzt, sondern auch Kompatibilität. Standards betreffen daher insbesondere auch die Herstellung von Usability über die Grenzen einzelner Umgebungen wie z. B. dem Ökosystem einzelner Unternehmen hinweg.

Arbeitsdefinitionen von Kompatibilität und Interoperabilität

Im Kontext dieser Studie wird **Kompatibilität** als die *störungsfreie Arbeit und konsistente Austauschfähigkeit* von Komponenten, Anwendungen und Systemen insbesondere *innerhalb einer Umgebung* verstanden.

Unter **Interoperabilität (IOP)** wird die *Zusammenarbeit und Kombinierbarkeit* von Komponenten, Anwendungen und Systemen verstanden, welche sich *in unterschiedlichen Umgebungen* befinden können.

Unter einer Umgebung kann im Kontext digitaler Märkte der technische Einflussbereich oder das Ökosystem eines Unternehmens verstanden werden.

Im Folgenden soll der Begriff der IOP weiter beleuchtet werden. Dazu werden verschiedene Dimensionen und Aspekte von IOP weiter ausgeführt.

2.1.1.1 Interoperabilität als Kontinuum

IOP zwischen verschiedenen Anwendungen kann je nach Umfang des abgebildeten Funktionsumfangs variieren. Beispielsweise kann eine Teilmenge aller Funktionalitäten, die eine spezifische Anwendung bereitstellt mit anderen Anwendungen interoperabel sein, während die verbleibenden Funktionen nur den Nutzern der entsprechenden Anwendung selbst zur Verfügung stehen. Zwischen den Extremen „volle IOP“ und „keine IOP“ findet sich in der Literatur auch Analysen zu ***partieller IOP***, welche dieses Spektrum andeuten (Chou und Shy, 1993).

Darüber hinaus kann IOP auch in einem zeitlichen Kontinuum verortet werden. Während ***Datenportabilität*** einen punktuellen Export von Daten aus einer Anwendung oder einem Dienst bezeichnet, welche bei einem Wechsel zu einem anderen Dienst zum Import zur Verfügung stehen, kann vollständige IOP als der automatisierte wechselseitige Austausch (Export und Import) von Daten zwischen Diensten in Echtzeit angesehen werden. Datenportabilität ist also auch bei im Betrieb nicht interoperablen Diensten möglich, setzt aber zumindest eine Austauschfähigkeit voraus.

Crémer et al. (2019) unterscheiden in diesen beiden Dimensionen zwischen Verschiedenen Typen von IOP. **„Protokoll-IOP“** sorgt dafür, dass zwei Systeme grundlegend zusammengeschaltet werden und miteinander funktionieren können. Damit wird die Herstellung und das Angebot komplementärer Dienste ermöglicht. Zur Herstellung von Protokoll-IOP können damit Standards notwendig sein. Unter vollständiger Protokoll-IOP können auch Substitute von Diensten miteinander interoperabel gemacht werden. Dies kann beispielsweise die IOP von Messaging-Diensten oder Internet-of-Things-Produkten betreffen. Diese Definition von Protokoll-IOP entspricht damit der klassischen Sichtweise aus dem Wettbewerbsrecht und umfasst beispielsweise Betriebssysteme, sowie Telefone und Ladegeräte.

„Daten-IOP“ bezeichnet nach Crémer et al. (2019) den Datenaustausch in Echtzeit und kann damit als die kontinuierliche Form von Datenportabilität angesehen werden für die üblicherweise sogenannte APIs (Programmierschnittstellen) notwendig sind. Damit kann beispielsweise die Entwicklung und Einbindung von Add-Ons von Drittanbietern für prominente Anwendungen und Diensten ermöglicht werden. In einer solchen Situation können die Nutzer zu einem neuen Anbieter wechseln, ohne den Zugang zu Netzwerkeffekten zu verlieren, die von den Nutzern ausgehen, die beim alten Anbieter verbleiben. Dies lässt sich am Beispiel eines sozialen Netzwerks verdeutlichen. Selbst wenn ein Nutzer in der Lage wäre seine Daten zu einem neuen sozialen Netzwerk mitzunehmen, wäre er immer noch nicht in der Lage, mit den Nutzern zu interagieren, die bei dem alten Netzwerk verbleiben. In diesem Zusammenhang wurde argumentiert, dass "Identitätsportabilität" (Gans, 2018) oder "Portabilität von sozialen Graphen" (Zingales und Rolnik, 2017) - beides eigentlich eine Form von Protokoll-IOP - wünschenswert wären, um nutzerseitige Netzwerkeffekte zu überwinden. Übertragbarkeit von Identitäten bedeutet in diesem Fall sogar, dass eine Person zu einem neuen Netzwerk wechseln und ihre Identität mitnehmen kann, so dass alle Nachrichten, die sich auf diese Person beziehen, an das neue Netz weitergeleitet werden, und umgekehrt. Die Idee der Identitätsübertragbarkeit ist somit vergleichbar mit der Zusammenschaltung in Verbindung mit der Nummernübertragbarkeit in Telekommunikationsnetzen.

2.1.1.2 Horizontale und vertikale Interoperabilität

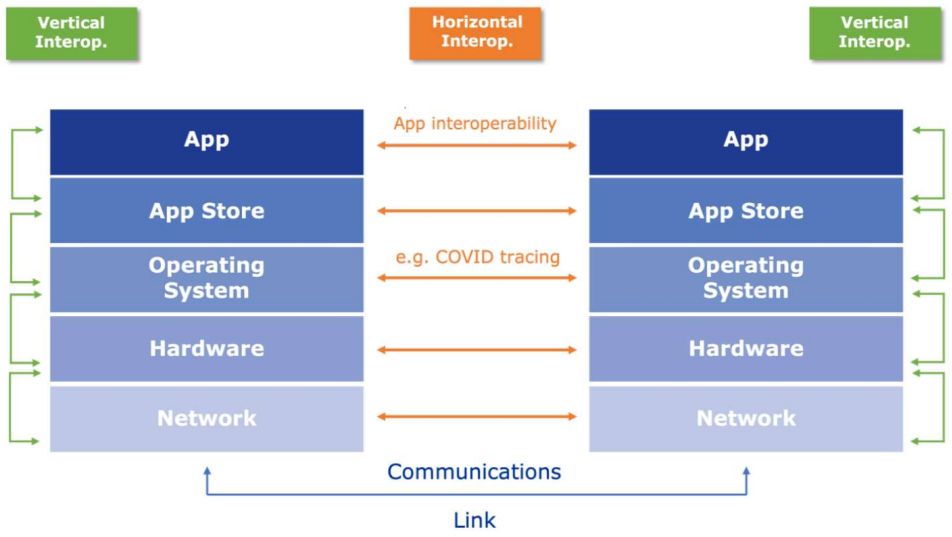
Eine weitere Unterscheidung lässt sich zwischen **horizontaler IOP (gleichartigen Diensten)** und **vertikaler IOP (vor- und nachgelagerten Wertschöpfungsstufen)** treffen (Riley, 2020). In diesem Kontext ist es entscheidend, ob sich diese Dienste in direktem Wettbewerb zueinander befinden, oder ob ein Dienst insbesondere den Wettbewerb von Diensten auf vor- oder nachgelagerten Stufen der Wertschöpfung beeinflusst.

Der Fall horizontaler IOP beschreibt dabei beispielsweise die Situation von Messaging-Diensten welche von Verbrauchern als Substitute wahrgenommen werden können und damit auf derselben Wertschöpfungsstufe in direktem Wettbewerb zueinander stehen. In diesem Fall betrifft IOP insbesondere den Zugang bzw. das Teilen von direkten Netzwerkeffekten zwischen Diensten. Bei einer Reihe von Produkten und Dienstleistungen ist der durch den Konsum gewonnene Nutzen für einen Verbraucher nicht immer gleich, sondern hängt stark davon ab, wie viele andere Konsumenten das Produkt oder den Dienst ebenfalls nachfragen. Diese Eigenschaft ist beispielsweise typisch für Kommunikationsdienste aller Art oder Hardware- und Software-Systeme. Ein Messenger wird somit attraktiver, je größer dessen Nutzerbasis zur Kommunikation ist. Diese positiven Nachfrageexternalitäten werden gemeinhin auch als Netzwerkeffekte bezeichnet, die sich hinsichtlich eines direkten als auch indirekten Wirkungskanals unterscheiden lassen (Farrell und Klemperer, 2007; Katz und Shapiro, 1994). Direkte Netzwerkeffekte bestehen dann, wenn der Nutzen für Verbraucher positiv von der Anzahl anderer Verbraucher des gleichen Dienstes oder Dienste-Systems abhängt (s. Messenger). Indirekte Netzwerkeffekte hingegen wirken über die Anzahl an Akteuren auf einer anderen Marktseite oder einer anderen Wertschöpfungsstufe. So wirkt beispielsweise eine große Nutzerbasis eines Hardware-Systems fördernd auf das Angebot von entsprechend passender Software, welches wiederum einen positiven Nutzen stiftet für die Nutzer des Hardware-Systems.

Der Fall vertikaler IOP ist insbesondere im Kontext digitaler Plattformen und Ökosysteme relevant, in denen Dienste über die Wertschöpfungskette hinweg vertikal miteinander kombiniert und orchestriert werden können (Jacobides und Lianos, 2021b). Als Plattform wird nach Evans (2003) eine Bereitstellung der Interaktions- und Koordinierungsmöglichkeit mindestens zweier Marktseiten in Funktion eines Intermediärs verstanden. Als Bedingungen für die Entstehung von Plattformen nennt Evans mindestens zwei unterscheidbare Marktseiten, (potenziell) realisierbare Externalitäten bei der Koordinierung und den Intermediär als Internalisierungsinstanz der Externalitäten. In diesem Fall beschränken sich die Netzwerkeffekte nicht nur auf eine spezifische Nutzergruppe, sondern beeinflussen ebenfalls eine oder mehrere weitere Nutzergruppe(n) ist von gruppenübergreifenden („cross-group“) Netzwerkeffekten die Rede. Lassen sich gruppenübergreifende Netzwerkeffekte zwischen zwei Nutzergruppen (z. B. A und B) *in beide Richtungen* beobachten spricht man von indirekten Netzwerkeffekten, da in diesem Fall der Nutzen für einen Teilnehmer in Gruppe A von der Anzahl der Teilnehmer in Gruppe B abhängt, deren Nutzen wiederum von der Anzahl der Teilnehmer in Gruppe A abhängt. Damit hängt der Nutzen eines Teilnehmers in Gruppe A indirekt von der Anzahl der Teilnehmer in Gruppe A ab.

Diese gruppenübergreifenden Netzwerkexternalitäten werden in Plattformmärkten durch Intermediäre wie beispielsweise Matching-Plattformen internalisiert. Parker et al. (2020) definieren daher eine Plattform als digitale Ressource zur Verwirklichung von effizienten Interaktionen von Marktseiten, so dass eine Wertschöpfung ermöglicht werden kann. Hierfür unterscheiden sie in Plattformen, die aggregieren, wie Suchmaschinen, oder digitale Marktplätze, die Matching zwischen zwei Marktseiten ermöglichen. In diesem Fall betrifft IOP insbesondere den Zugang zu einer Wertschöpfungsstufe durch vor- und nachgelagerte Anbieter und damit den Zugang bzw. das Teilen von indirekten Netzwerkeffekten. Diese Unterscheidung in horizontale und vertikale IOP wurde anschließend von verschiedenen Autoren aufgegriffen (Bourreau, Krämer, & Buiten, 2022; Mancini, 2021; Steffen, Wiewiorra, & Kroon, 2021).

Abbildung 2-2: Horizontale und vertikale IOP in mobilen Ökosystemen.



Quelle: Bourreau et al. (2022, S. 15)

Abbildung 2-2 verdeutlicht die Beziehung dieser beiden Konzepte im Kontext von mobilen Ökosystemen. Aufbauend auf der physischen Kommunikationsschicht (Funkwellen) befindet sich die Netzwerkschicht. Auf dieser Ebene herrscht bereits durch Standardisierung (z. B. 5G, LTE, GSM) eine IOP, da beliebige Endgeräte, die entsprechende Standards implementiert haben, in allen Mobilfunknetzen eingesetzt werden können und untereinander kommunizieren können. Allerdings ist die Zusammenschaltung und damit IOP dieser Netze regulatorisch verpflichtend. Die darauf aufbauenden Wertschöpfungsstufen unterliegen bisher allerdings keinen verpflichtenden IOP-Vorschriften. Auf der Hardwareebene bestehen ebenfalls standardisierte Schnittstellen (z. B. Bluetooth, NFC), welche eine IOP auf dieser Ebene ermöglichen (z. B. den Einsatz beliebiger Bluetooth

Headsets oder Kopfhörer mit beliebigen Endgeräten). Auf der darauf aufbauenden Betriebssystemebene bestehen ebenfalls Beispiele für IOP. Das während der Pandemie ausgerollte Betriebssystem-Feature des COVID-19-Trackings, welches die Basis für die Corona-Warn-App darstellt, ist ebenfalls interoperabel zwischen den beiden dominanten mobilen Betriebssystemen (iOS, Android). Die nachfolgende Wertschöpfungsstufe stellen Softwaremarktplätze dar, welche derzeit nicht auf freiwilliger Basis interoperabel zwischen Anbietern unterschiedlicher mobiler Betriebssysteme sind. Auf der Ebene mobiler Applikationen finden sich allerdings Beispiele für freiwillige IOP. Serviceprovider wie z. B. Dropbox ermöglichen das Teilen von Daten über die Grenzen unterschiedlicher mobiler Ökosysteme hinweg. Ebenso erlauben unterschiedliche Anbieter mobiler Videospiele „Cross-play"-Funktionen, die es den Spielern erlauben plattformübergreifend zwischen unterschiedlichen Betriebssystemen zusammen zu spielen.

Vertikale IOP bezeichnet in diesem Zusammenhang die Kombination von Funktionalitäten über die Grenzen einzelner Wertschöpfungsstufen hinaus. In diesem Kontext ist beispielsweise für die Corona-Warn-App der Zugriff auf die COVID-Tracking-Funktionalität des Betriebssystems notwendig, um entsprechende Warnhinweise an einzelne Nutzer ausgeben zu können. Die Betreiber der beiden großen Ökosysteme (Apple, Google) gewähren derzeit pro Land nur einem staatlich verifizierten Anbieter Zugriff auf diese Schnittstelle und schränken damit die IOP gezielt ein. Darüber hinaus geben die Anbieter die Spezifikation der Schnittstelle einseitig an die Betreiber der Applikationen vor. Vergleichbar ist für eine Banking-App die Zahlungen für ihre Kunden über ein mobiles Endgerät abwickeln will, ein Zugriff auf die jeweilige NFC-Schnittstelle notwendig. Dieser Zugriff auf die NFC-Schnittstelle und damit vertikale IOP wird von Apple und Google unterschiedlich gehandhabt. Während Google App-Entwicklern relativ freien Zugriff gewährt, handhabt Apple den Zugriff auf die NFC-Schnittstelle seiner Endgeräte sehr restriktiv.

Die Unterscheidung in horizontale und vertikale IOP erscheint daher im Rahmen dieser Studie als besonderes zielführende Unterscheidung, da sie deutlich zu einer Abgrenzung zwischen relevanten Diensten der Plattformökonomie und Online-Kommunikationsdiensten beitragen kann. Während in der Plattformökonomie neben dem Angebot gleichartiger Dienste insbesondere viele Up- und Downstreamverflechtungen zwischen unterschiedlichen Wertschöpfungsstufen vorzufinden sind, handelt es sich bei Online-Kommunikationsdiensten um eine primär horizontale Beziehung der unterschiedlichen Anbieter.

2.1.1.3 Einseitige (asymmetrische) und zweiseitige (symmetrische) Interoperabilität

Bei **einseitiger (asymmetrischer) IOP** ist es möglich Informationen gerichtet zu oder von einer Anwendung zu übertragen, aber kein wechselseitiger Austausch zwischen zwei Anwendungen. Bei **zweiseitiger (symmetrischer) IOP** ist im Gegensatz dazu ein Austausch zwischen Nutzern unterschiedlicher Anwendungen und Dienste in beide Richtungen möglich (Manenti und Somma, 2008).

Im Fall von asymmetrischer IOP können Anbieter von Diensten beispielsweise Funktionalitäten anbieten, welche die Zuwanderung zu oder Reichweite von ihrer Plattform erhöhen, während sie Funktionalitäten einschränken, welche die Abwanderung zu oder Reichweite von konkurrierenden Diensten erhöhen könnten. Ein konkretes Beispiel findet sich in Import- und Exportfunktionen bei Smartphones. Apple und Google bieten jeweils Apps für Betriebssystemwechsler auf den jeweils konkurrierenden Betriebssystemen an, um den Wechsel zu ihrer eigenen Plattform zu erleichtern, unterstützen aber nicht aktiv die Abwanderung zu anderen Betriebssystemen durch eine eigens bereitgestellte Exportfunktion. Dieses Beispiel wird in Kapitel 2.1.2 im Kontext von Adaptern und Konvertern erneut aufgegriffen. Die Competition and Markets Authority des Vereinigten Königreichs (CMA, 2020) stellte darüber hinaus fest, dass soziale Medienplattformen APIs selten wechselseitig anbieten. Facebook ermöglicht konkurrierenden Plattformen in diesem Zusammenhang durch Schnittstellen Inhalte einfach auf seiner Plattform zu teilen. Im Gegensatz dazu stehen Facebook-Nutzern vergleichbare Funktionen, um Inhalte auch in anderen sozialen Medien zu teilen, nur in sehr begrenztem Umfang zur Verfügung.

Sollte IOP auch gegen den Willen eines Unternehmens hergestellt werden, spricht man von **adversarialer (feindlicher) IOP**. Ein Bespiel dafür sind beispielsweise Druckerpatronen von Drittherstellern, welche die Authentifizierung der Erkennung des Druckers als Originalzubehör umgehen, oder auch modifizierte Versionen des WhatsApp-Messengers, die beispielsweise in Afrika stark verbreitet sind. Dies kann beispielsweise durch sogenanntes „Reverse Engineering“, also dem Nachvollziehen einer eigentlich proprietären Implementierung einer Schnittstelle oder Softwarekomponente, erreicht werden. In diesem Fall kann sich das betreffende Unternehmen z. B. durch schnelle und häufige Technologieänderungen gegen die ungewollte IOP wehren, was für Verbraucher häufige Unterbrechungen der IOP zur Folge hat. Darüber hinaus stehen betreffenden Unternehmen auch juristische Schritte offen, falls diese Patente an der für die IOP notwendigen Technologie halten, welche von Konkurrenten (oder Herstellern von Komplementen) ohne Zustimmung verwendet werden.

Diese Beispiele verdeutlichen, dass horizontale IOP symmetrisch oder asymmetrisch sein kann. Im Gegensatz dazu ist vertikale IOP immer asymmetrisch, da eine Plattform nur einseitig Zugang auf eine Wertschöpfungsstufe für Drittanbieter gewährt, aber nicht umgekehrt (Bourreau et al., 2022).

Grundsätzlich kann ein Unternehmen IOP daher sowohl kooperativ („Einladung“ von Komplementen, Zubehör, Add-ons etc.), adversarial (z. B. Reverse Engineering) oder indifferent (ökonomisch durch IOP nicht positiv oder negativ beeinflusst) gegenüberstehen.

2.1.2 Umgehung von Inkompatibilität: Adapter/Konverter und Multi-Homing

In der ökonomischen Literatur finden sich allerdings auch Diskussionen und Analysen zum Einsatz von sogenannten **Adaptern bzw. Konvertern** zur Herstellung von IOP (Farrell und Saloner, 1992). In diesem Fall muss kein einheitlicher Standard und teilweise auch kein kooperatives Verhalten bestehen, sondern ein (technisches) Bindeglied sorgt für die Übersetzung zwischen zwei eigentlich nicht kompatiblen Systemen. Adapter bzw. Konverter sind damit als Übersetzer zwischen nicht-standardisierten Systemen oder zwei Systemen, die unterschiedliche Standards verfolgen, anzusehen. Über diese Technologien kann IOP teilweise auch ohne die direkte Zustimmung einer der beiden Seiten und nur asymmetrisch hergestellt werden. Ein Zwei-Wege-Konverter entspricht der von vielen Programmen gebotenen Möglichkeit das Format des Rivalen zu lesen und zu speichern (Farrell & Saloner, 1992; Manenti & Somma, 2008).

Letztlich ist das Ziel von IOP der Austausch von Information zwischen Nutzern über die Grenzen spezifischer Dienste bzw. Betreiber hinweg zur Erbringung und Nutzung eines Dienstes. Selbst für den Fall, dass kein einheitlicher Standard für eine spezifische Dienstkategorie besteht und keine Adapter oder Konverter verfügbar sind, können Verbraucher Inkompatibilitäten durch **Multi-Homing** selbst überwinden (De Palma et al., 1999; Doganoglu und Wright, 2006). Die Mehrfachnutzung bzw. gleichzeitige Nutzung unterschiedlicher Dienste ist damit eine weitere Möglichkeit für Verbraucher, um von den Netzwerkeffekten verschiedener Dienste gleichzeitig profitieren zu können. Natürlich kann Multi-Homing für Verbraucher mit zusätzlichen Kosten verbunden sein (z. B. Aufwand, Zeit, Kosten) und ist damit nur eine attraktive Option zur Überwindung von Inkompatibilität, falls diese Kosten vergleichsweise gering bzw. vernachlässigbar ausfallen (Belleflamme und Peitz, 2019). Aus Sicht der Unternehmen hängt die Beziehung zwischen Kompatibilität und Gewinnen von zwei gegenläufigen Effekten ab. Einerseits erhöht geringe Kompatibilität unter Multi-Homing die Nachfrage und damit die Gewinne, andererseits führt geringe Kompatibilität zu stärkerem Wettbewerb auf der Outputebene und senkt so die Gewinne. Unter Multi-Homing kann es daher zu asymmetrischen Gleichgewichten kommen, in denen große Unternehmen einen möglichst niedrigeren Grad an Kompatibilität bevorzugen, während kleinere Unternehmen vollständige Kompatibilität vorziehen würden (De Palma et al., 1999).

2.1.3 Kompatibilität durch Konvention: Standards

Unter einem **Standard** ist eine Reihe von technischen Spezifikationen zu verstehen, die von einem Hersteller entweder stillschweigend oder aufgrund einer förmlichen Vereinbarung eingehalten werden (David und Greenstein, 1990, S. 4). Meistens ist für IOP ein Standard zu definieren, also eine Konvention (z. B. Datenformate, Schnittstellen und Funktionen) wie Daten zwischen unterschiedlichen Diensten zur Bereitstellung von spezifizierten Funktionalitäten regelmäßig im Betrieb ausgetauscht und interpretiert werden können. Das Herstellen von IOP setzt in diesem Fall die Verfügbarkeit oder die Einigung auf einen gemeinsamen Standard voraus. Standards können sowohl **de-facto** (ex-post

am Markt) als auch **de-jure** (ex-ante festgelegt) entstehen. Bekannte de-jure Standards sind beispielsweise die durch öffentliche Standardisierungsorganisationen geprägten ISO- oder DIN-Normen. Aber auch private Standardisierungsorganisationen können de-jure Standards hervorbringen, wie beispielsweise den Nahfunkstandard Bluetooth (Headsets, Kopfhörer, Peripheriegeräte etc.), welcher durch die „Bluetooth Special Interest Group“[3] besetzt durch namhafte Technologieunternehmen geprägt wird.

In der ökonomischen Literatur wird Standardisierung dabei aus verschiedenen Perspektiven analysiert, die im Folgenden kurz vorgestellt werden.

2.1.3.1 Standard-Kriege

Standard-Kriege beschreiben die Dynamiken am Markt, in einer Situation in welcher sich die beteiligten Parteien ex-ante nicht auf einen Standard geeinigt haben. Daher existieren verschiedene (technische) Ansätze bzw. Formate für einen bestimmten Zweck zwischen denen die Kunden wählen können. Durch die Entscheidungen der Konsumenten können sich proprietäre Technologien durch Marktpenetration als allgemein verwendeter Standard (de-facto) etablieren, falls die Kunden mit der Zeit eine der verfügbaren Alternativen präferieren. In diesem Prozess spielen üblicherweise direkte und indirekte Netzwerkeffekte, beispielsweise durch die Verfügbarkeit komplementärer Produkte, eine entscheidende Rolle. Die ökonomische Literatur zu marktbasierter ex-post Standardisierung und den dabei relevanten Dynamiken ist sehr umfänglich (Besen & Farrell, 1994; Clements, 2004; Economides, 1996; Farrell & Saloner, 1985a, 1985b, 1986b; Katz & Shapiro, 1985, 1994; Regibeau & Rockett, 1996). Aus der jüngeren Vergangenheit gibt es viele Beispiele für Standard-Kriege und de-facto Standardisierung. Dazu zählen unter anderem die gängigen Microsoft-Office Formate, das Portable Document Format (PDF) von Adobe oder das BluRay-Format, welches sich am Markt für physische Video-Datenträger gegen die HD-DVD als Nachfolger der klassischen DVD durchgesetzt hat.

2.1.3.2 Koordinations- und Koalitionsspiele

Farrell und Saloner (1988) untersuchten erstmals die Effizienz eines hybriden Standardisierungsmechanismus. Dabei wird neben der marktbasierten Lösung auch eine Koordination über ein Komitee berücksichtigt, in dem sich die beteiligten Parteien treffen und koordinieren können. Die Autoren finden heraus, dass hybride Standardisierung den beiden reinen Formen der Standardisierung überlegen sein kann, da die Unternehmen damit vor dem Markteintritt mehr Möglichkeiten zur Koordination haben und damit die negativen Auswirkungen von Standard-Kriegen bzw. Inkompatibilität vermieden werden können.

Vergleichbare Analysen gibt es im Kontext von Koalitionen für die Festlegung von Standards. Häufig lässt sich ein Markt nicht durch einen einzelnen Akteur und sein Produkt von der Annahme eines Standards überzeugen. Daher scheint die Bildung von Koalitio-

3 Bluetooth (2022)

nen (z. B. Computerhersteller, Softwareanbieter, Anbieter von Peripheriegeräten) zielführend. In der Praxis stehen hinter vielen, der in Kapitel 2.1.3.1 diskutierten Formate Allianzen, welche gemeinsam einen Standard am Markt etablieren wollen. Allianzen sind dann stabiler falls die Größe der Allianz zunimmt und instabiler bei dem Vorhandensein von (engen) Rivalen in der Allianz (Axelrod et al., 1995). Aus einer theoretisch ökonomischen Perspektive entscheiden sich die Firmen dabei zunächst für den Beitritt zu einer Standard-Allianz und finden sich anschließend am Markt in einem Oligopolspiel wieder. Dabei profitiert ein Unternehmen durch den Beitritt zu einer Allianz von den Netzwerkeffekten, die durch alle Mitglieder hervorgerufen werden, sieht sich anschließend aber einem verstärkten Wettbewerb auf dem Produktionsmarkt gegenüber. Daher kann das Ausmaß der Netzwerkeffekte einen maßgeblichen Einfluss auf die gebildeten Allianzen haben. Wenn die Netzwerkeffekte sehr stark sind, schließen sich alle Unternehmen in einer Allianz zusammen und es herrscht vollständige Kompatibilität. Bei schwächeren Netzwerkeffekten, wird ein Unternehmen bereits abweichen und einen Standard im Alleingang anbieten, während alle verbleibenden Unternehmen in einer gemeinsamen Allianz verbleiben. Im anderen Extremfall, bei sehr schwachen Netzwerkeffekten, herrscht völlige Inkompatibilität, da sich keine der Unternehmen zusammenschließen wollen (Economides und Skrzypacz, 2003).

2.1.3.2.1 Wartespiele (Zermürbungskriege)

Bei formalen ex-ante Standardisierungsprozessen wird die Konsensfindung im Rahmen von Komitees und Gremien angestrebt. Dabei muss üblicherweise unterstellt werden, dass im Rahmen dieses Prozesses Kosten entstehen, welche für alle Beteiligten mit der Dauer der Konsensfindung ansteigen. Diese Situation kann als Zermürbungskrieg bezeichnet werden, da die Beteiligten in jeder Runde des Koordinationsspiels Kosten aufwenden müssen, um weiter an dem Prozess teilzunehmen. Ziel in einem Zermürbungskrieg ist es, als letzter Teilnehmer im Prozess die Oberhand zu behalten und damit die Standardisierung maßgeblich beeinflussen zu können. Spieler, die bereits früher nicht mehr bereit sind, die Kosten der Konsensfindung weiter zu tragen, steigen aus dem Prozess aus und überlassen damit den/dem verbleibenden Spieler(n) die Entscheidungsgewalt. Der Wert die Festlegung eines Standards maßgeblich beeinflussen zu können bestimmt sich durch den dadurch beeinflussten Geschäftserfolg und eine mögliche Reduktion der eigenen Kosten, falls eigene technische Lösungen weiterverwendet werden können und damit z. B. Skalen- oder Verbundeffekte erzielt werden können. Diese Prozesse bergen daher die Gefahr, dass die aggregierten Kosten, die alle Teilnehmer investieren, um erfolgreich aus der Standardisierung hervorzugehen den Wert des Standards übersteigen. Daher kann in manchen Fällen eine direkte Zufallsauswahl das Ergebnis eines Zermürbungskriegs übertreffen. Darüber hinaus wird das Ergebnis einer solchen Situation durch die Zusammensetzung der Spieler bestimmt. Teilnehmer ohne starke Eigeninteressen, bzw. eine Reduktion der Eigeninteressen aller Spieler können so Verzögerungen bei der Standardisierung verringern und den ex-ante-Anreiz zur Verbesserung der eingebrachten Vorschläge in den Standardisierungsprozess erhöhen (Bishop und Cannings, 1978; Farrell und Simcoe, 2012a).

2.1.3.2.2 Signalisierungsspiele

Standardisierung kann auch als Signalisierungsspiel aufgefasst werden. In diesem Fall sehen Verbraucher einen Standard vergleichbar mit einem Gütesiegel oder einer Zertifizierung an. Standardisierungsorganisationen werden von den Inhabern von Technologien angerufen und entscheiden über die eingebrachten Vorschläge mit unterschiedlichem Anspruch an die Qualität der Vorschläge. Anspruchsvolle Standardisierungsorganisationen sind dabei schwerer von einem Vorschlag zu überzeugen als weniger anspruchsvolle Standardisierungsorganisationen, da sie die Interessen der Verbraucher gegenüber den Interessen der Unternehmen stärker in ihre Entscheidung einfließen lassen. Die Verbraucher nehmen diese Unterschiede in der Standardisierung wahr und schätzen eine anspruchsvollere und verbraucherfreundlichere Standardisierung. Daher wird z. B. eine DIN-Norm von Verbrauchern als verbindlicher und weitreichender empfunden als ein reiner Industriestandard wie z. B. Bluetooth. Damit wird die Entscheidung eines Unternehmens über die passende Standardisierungsorganisation für einen technischen Vorschlag zu einer entscheidenden strategischen Variablen. Im Hinblick auf das Optimierungsproblem der Konsumenten beeinflusst eine Standardisierung dadurch den bedingten Erwartungswert der wahren (für sie unbeobachtbaren) Qualität einer Technologie und schafft damit (je nach Qualitätsanspruch der Standardisierungsorganisation) mehr oder weniger Sicherheit bei der Kaufentscheidung (Chiao et al., 2007; Lerner und Tirole, 2006).

2.2 Auswirkungen auf Wettbewerbsprozesse

Die in dieser Studie verwendete Arbeitsdefinition von IOP gemäß Kapitel 2.1 wird in der ökonomischen Literatur hauptsächlich unter dem Oberbegriff der Kompatibilität untersucht. Interoperable Dienste teilen demnach gemeinsame Funktionen und entsprechende Wettbewerbswirkungen betreffen die Nutzerbasis interoperabler Dienste gleichermaßen. Von wettbewerblichen Hauptinteresse sind in diesem Zusammenhang insbesondere die unterschiedlichen Wirkungen von IOP zwischen horizontal konkurrierenden Diensten und IOP zu vor- und nachgelagerten Wirtschaftsstufen (Farrell und Saloner, 1985b; Katz und Shapiro, 1985).

Die Hauptmotivation zur Einführung von IOP aus ökonomischer Perspektive ist das Auflösen firmenspezifischer Netzwerkeffekte, sodass resultierende Nutzengewinne aus der Größe des Netzwerks den Konsumenten aller interoperablen Dienste zugute kommen. Diese grundlegende Wirkungsweise von IOP impliziert eine Reihe von wettbewerblichen als auch innovationsökonomischen Effekten, die in diesem Kapitel allgemein erläutert werden.

2.2.1 Interoperabilität und Wettbewerb

2.2.1.1 Die Rolle von Netzwerkeffekten

In einem horizontalen Wettbewerbsumfeld, in dem keine IOP zwischen den Diensten besteht, entsteht der Nutzen durch etwaige Netzwerkeffekte für Konsumenten eines Dienstes nur auf Basis der Nutzerbasis des jeweiligen Anbieters. Durch eine (symmetrische und vollständige) horizontale IOP wird diese Situation aufgelöst und die relevante Netzwerkgröße auf dessen Basis Netzwerkeffekte anfallen beinhaltet in einem solchen Szenario die Konsumenten aller interoperablen Dienste. Durch das Zusammenlegen der Marktanteile der horizontal interoperablen Anbieter werden dadurch entstehende Netzwerkeffekte maximiert und so, ceteris paribus, Wohlfahrtsgewinne im statischen Wettbewerb realisiert (Katz und Shapiro, 1985). Hieraus resultierende Effekte zweiter Ordnung, wie z. B. Änderungen von Preisen und die letztendliche Verteilung dieser zusätzlichen Netzwerk-Renten zwischen Produzenten und Verbrauchern, hängen jedoch von anderen Marktbegebenheiten ab wie beispielsweise der Marktstruktur oder der Nachfrageelastizität. Implikationen für die dynamische Wettbewerbsperspektive sind Gegenstand von Kapitel 2.2.2.

2.2.1.2 Interoperabilität als Unternehmensstrategie

Neben einer extern postulierten IOP von Produkten, bestehen auch für aktive Unternehmen Anreize IOP ihrer Produkte und Dienste selbst herzustellen. Ist die technische Umsetzung dessen grundsätzlich möglich, entweder unilateral durch Konverter oder multilateral durch marktgetriebene Standards (s. Kapitel 2.1.2), wird IOP ökonomisch zu einer strategischen Entscheidungsvariable, ähnlich zu Marktpreisen oder angebotenen Mengen. Infolgedessen können die privaten und gesamtgesellschaftlichen (wohlfahrtsmaximierenden) Anreize IOP herzustellen deutlich variieren.

Dies trifft insbesondere auf Unternehmen zu, die bereits über eine große Nutzerbasis bzw. Marktanteil verfügen und dessen Nutzer vergleichsweise nur wenig von horizontaler IOP zu anderen Produkten und resultierenden zusätzlichen Netzwerkeffekten profitieren würden. Katz und Shapiro (1985) weisen darauf hin, dass große Unternehmen deutlich stärkere Anreize haben, „Nicht-Interoperabilität“ beizubehalten, auch wenn eine IOP gesamtwirtschaftlich wünschenswert und effizient ist. Im Umkehrschluss profitieren kleinere Unternehmen mit einer geringen Nutzerbasis besonders stark von einer IOP zwischen Produkten. Folglich präferieren sie eine Einführung von IOP auch dann, wenn es gesamtwirtschaftlich ineffizient ist.

Unterschiedliche Anreize zur Einführung von insbesondere vertikaler IOP können auch hinsichtlich der zeitlichen Sequenz der Öffnung bestehen. Bei einer sog. „Open early – close late“ Strategie profitiert eine Plattform im frühen Produktzyklus von innovativen Komplementärprodukten und kann so ihre Attraktivität steigern (Eisenmann et al., 2009).

Je etablierter ein solcher Plattformdienst wird, desto stärker werden die Anreize, erfolgreiche Komplemente und Funktionen in die Plattform zu integrieren und selbst bereitzustellen (sog. „Sherlocking“). Eine Reduzierung von vertikaler IOP wird in diesem fortgeschrittenen Stadium aus Sicht der Plattform dann attraktiver.

2.2.1.3 Auflösen von Marktkonzentration und Market tipping

Mögliche Asymmetrien in Marktanteilen („Installed Bases“) sind insbesondere auf Märkten der Plattformökonomie und für Kommunikationsdienste relevant, da hier besonders starke positive Netzwerkexternalitäten bestehen. Auf solchen Märkten ist es für Anbieter essenziell möglichst schnell eine „kritische Masse“ an Nachfragern für das eigene Produkt zu gewinnen, um so entstehende firmenspezifische Netzwerkeffekte optimal nutzen zu können und einen Wettbewerbsvorteil zu realisieren. In einer solchen „Competition for the Market“ Umgebung im Sinne von Rochet und Tirole (2003) kann es daher zum gänzlichen „Kippen“ von Märkten und einer letztendlich starken Marktkonzentration auf einen oder wenige Anbieter kommen („Market tipping“). Dominante Firmen haben in einer solchen Marktsituation keinen Anreiz zu horizontaler IOP, während Unternehmen, die ein neues Produkt veröffentlichen oder gänzlich neu in den Markt eintreten wollen hiervon profitieren würden.

Chen et al. (2009) zeigen, dass IOP von Produkten und das Auflösen der Exklusivität von Netzwerkeffekten beim dominanten Anbieter helfen kann, Marktkonzentrationen entgegenzuwirken. In einem bereits konzentrierten Markt ist diese ex-post Einführung von horizontaler IOP jedoch für die dominante Firma nicht anreizkompatibel und wird sich in symmetrischer Form daher nicht marktgetrieben einstellen. In Märkten mit einer vergleichsweise geringen Differenz in Marktanteilen, d. h. die noch nicht „gekippt“ sind, bestehen ggf. Anreize zur Einführung von horizontaler IOP für alle konkurrierenden Unternehmen. In einem solch symmetrischen Szenario fallen Nutzengewinne durch realisierte Netzwerkeffekte in vergleichbarem Maß bei allen Marktteilnehmern an und IOP wirkt wie eine Vergrößerung der Marktgröße. Eine marktgetriebene Einführung von IOP ist strategisch somit vorteilhaft für die Unternehmen. Kapitel 3.2.1 präzisiert die Möglichkeiten mit einer horizontalen IOP-Regelung Marktkonzentrationen auf digitalen Plattformmärkten entgegenzuwirken.

2.2.1.4 Die Rolle von Multi-Homing

Grundsätzlich ist horizontale IOP zwischen Produkten nicht die einzige Möglichkeit, um firmenspezifische Netzwerkeffekte auf einem Markt voll zu nutzen. Wenn es Konsumenten möglich ist, mehrere konkurrierende Produkte und Dienste nebeneinander zu nutzen, dann liegt sog. Multi-Homing vor und entsprechende Netzwerkeffekte fallen in vollem Maße an. Beispielsweise besteht für Konsumenten die Möglichkeit so mehrere Messaging-Dienste gleichzeitig zu nutzen, um gleichermaßen die Nutzerbasis des einen als

auch des anderen Anbieters erreichen zu können. Ist Multi-Homing also ohne nennenswerte Zusatzkosten möglich, d. h. nicht monetäre Transaktionskosten als auch monetäre Produktpreise sind gering, dann ist der mögliche Zugewinn durch horizontale IOP begrenzt. Ist Multi-Homing jedoch nur eingeschränkt möglich und mit deutlichen Zusatzkosten verbunden, zeigen Doganoglu und Wright (2006), dass Multi-Homing nur ein imperfektes Substitut für eine tatsächliche IOP ist. Entstehende Kosten durch Multi-Homing werden von den Unternehmen nicht internalisiert und könnten durch eine horizontale IOP-Regelung wohlfahrtsfördernd vermieden werden. In dem Modell von Doganoglu und Wright (2006) wird allerdings davon ausgegangen, dass der Netzwerknutzen nicht sehr ausgeprägt ist, so dass Märkte nicht kippen und mehrere (horizontal differenzierte) Anbieter sich auch ohne IOP am Markt etablieren können. Das Modell hat daher nur begrenzte Aussagekraft in Märkten mit sehr starken Netzwerkeffekten, die Kippen können. Da in gekippten Märkten nur noch ein dominanter Anbieter existiert, ist Multi-Homing zunächst nicht relevant. Der Vergleich der Wirkung von Multi-Homing und IOP hinsichtlich der Frage, welches Instrument den Markteintritt eines innovativen Marktneulings eher begünstigt ist in diesem Szenario ex-ante nicht klar zu beantworten und wird in Doganoglu und Wright (2006) nicht untersucht. Kapitel 3.3.1 spezifiziert die substitutive Wechselwirkung von Multi-Homing und IOP im Kontext der Plattformökonomie daher näher und stellt insbesondere auf die dynamische Wettbewerbsperspektive beider Konzepte ab.

2.2.1.5 Homogenität von Produkten

Durch eine IOP von horizontal konkurrierenden Diensten werden diese maßgeblich ähnlicher aus Konsumentensicht. Digitale Plattformen bieten einen Kern an vergleichbaren oder sogar identischen Funktionen, verschiedene Netzwerke und Kommunikationsdienste erlauben die Kommunikation zur identischen und gemeinsamen Nutzerbasis oder genügen auf Grund technischer Standards den gleichen Sicherheits- und Privatsphäre-Anforderungen. Durch horizontale IOP werden Produkte und Dienste somit homogener und die Möglichkeiten von Anbietern sich von der Konkurrenz zu differenzieren schrumpfen (Farrell und Saloner, 1985b). Abstrahiert man von anderen begleitenden Faktoren wie z. B. Netzwerkeffekten, impliziert eine geringere horizontale Differenzierung von Produkten im statischen Wettbewerb einen intensivieren Preiswettbewerb.

Einerseits ist ein intensiverer Wettbewerb, in monetären Preisen oder noch differenzierbaren Produktdimensionen, gut für Verbraucher, birgt jedoch Renteneinbußen auf der Anbieterseite. Je nach Kostenstrukturen derzeit operierender Anbieter, könnte somit eine ex-post IOP-Vorgabe den Preissetzungsspielraum beschränken, Gewinne reduzieren und ultimativ den Marktaustritt einzelner Unternehmen bedeuten. Für eine weiterführende Diskussion von Produktdifferenzierungsmöglichkeiten im Kontext von Plattformdiensten verweisen wir auf Kapitel 3.3.4.

Wettbewerbswirkungen von Interoperabilität

- IOP von Diensten ermöglicht das Nutzen von anbieterspezifischen **Netzwerkeffekten** allen Nutzern von interoperablen Anbietern.
- **Anreize** für eine nachträgliche Einführung von **horizontaler IOP variieren stark hinsichtlich Marktanteilen** und der bereits gewonnenen Nutzerbasis. Große Anbieter verlieren durch IOP möglicherweise einen Wettbewerbsvorteil, wohingegen Dienste kleinerer Anbieter attraktiver werden.
- IOP kann **Marktkonzentrationen abschwächen** oder dem **Kippen von Märkten vorbeugen**, indem Netzwerkeffekte nicht mehr anbieterspezifisch auftreten und ein Anbieterwechsel ohne einen Verlust von Netzwerkeffekten erfolgen kann.
- Wenn **Multi-Homing** ohne nennenswerte Kosten möglich ist, sind die gesamtwirtschaftlichen **Zugewinne von IOP begrenzt**.
- Durch IOP **steigt die Homogenität von Produkten** und schränkt die Möglichkeit zur Produktdifferenzierung ein. Dies impliziert einen **stärkeren Wettbewerbsfokus** in anderen Produktdimensionen wie z. B. **Preise oder Qualitätsmerkmale**, die von einer IOP-Regelung nicht betroffen sind.

2.2.1.6 Kostenwirkungen von Interoperabilität

Während bisher maßgeblich auf mögliche Nutzengewinne durch IOP von Produkten abgestellt wurde, geht dieser Abschnitt auf verschiedene Kostendimensionen ein, die mit der Einführung oder dem Unterhalt von IOP einhergehen. In dieser Hinsicht ist eine Unterscheidung in firmenspezifische und gesamtwirtschaftliche Kostenkomponenten sinnvoll.

2.2.1.6.1 Unternehmensspezifische Fixkosten durch Interoperabilität

Bestimmte Kostenkomponenten entstehen Firmen erwartungsgemäß nur einmalig bei der Einführung bzw. Umsetzung von IOP-Auflagen. Solche Aufwendungen können beispielweise durch Ausgaben für Forschung und Entwicklung sein, um bestehende Produkte anzupassen, Verhandlungskosten zur Ausgestaltung eines notwendigen technischen Standards oder die Kosten durch die Einführung eines gänzlich neuen, interoperablen Produkts.

Solche einmaligen Kosten stellen ökonomisch versunkene Kosten dar und Katz und Shapiro (1985) stellen heraus, dass in einem solchen Fall die Grenzkosten von interoperablen als auch nicht operablen Produkten und Diensten identisch sind. Versunkene Fix-

kosten durch IOP sind somit nicht relevant für nachgelagerte strategische Entscheidungen, wie die Wahl von Preisen, Mengen oder Produktqualitäten und kosteninduzierte Wettbewerbswirkungen sind nicht zu erwarten.

Ebenfalls sind in einem solchen Szenario die privatwirtschaftlichen Anreize IOP herzustellen oft geringer als im Vergleich zur gesamtgesellschaftlichen Betrachtungsweise. Dies liegt daran, dass hohe Fixkosten für Unternehmen ein Hemmnis darstellen können, Produkte und Dienste interoperabel zu gestalten. Dies ist insbesondere der Fall wenn potenzielle Zugewinne durch IOP stark asymmetrisch ausfallen und nicht alle Marktteilnehmer von IOP profitieren, sodass Fixkosten der Einführung nicht amortisiert werden können. In dieser Hinsicht können hohe Fixkosten durch IOP, z. B. komplexe technische Anforderungen durch eingeführte Standards, auch Markteintritte junger Unternehmen erschweren und somit zukünftigen Wettbewerb abschwächen. Die Gefahr, dass hohe Kosten durch IOP-Standards als Marktzutrittsschranke zu Plattformmärkten fungieren können, konkretisieren wir in Kapitel 3.3.6. Ebenfalls bestehen Anreize für etablierte Anbieter die Qualität eingeführter IOP-Schnittstellen ex-post zu verschlechtern, um bei zugangssuchenden Unternehmen kontinuierliche Kosten zum Erhalt der IOP zu verursachen. Durch solche Sabotage-Anreize (siehe auch Kapitel 3.3.3) ist daher wahrscheinlich mit fortlaufenden Kosten zum Erhalt und „Pflege“ der IOP-Schnittstellen zu rechnen.

2.2.1.6.2 Unternehmensspezifische variable Kosten von Interoperabilität

Im Gegensatz zu Fixkosten sind ebenfalls Situationen denkbar, in denen durch IOP entstehende Kosten variabel sind und in Abhängigkeit der Produktnachfrage oder der Nutzerbasis anfallen. In nicht-digitalen Märkten sind dies oft Inputkosten je produzierter Einheit, aber auch im digitalen Kontext lassen sich Beispiele finden. Die Umsetzung von IOP kann möglicherweise Lizenzzahlungen im Rahmen eines Standards beinhalten, die in Abhängigkeit der nachträglich realisierten Nachfrage und Nutzerbasis anfallen. Die Höhe der hierfür anfallenden Gesamtkosten ist somit von den Unternehmen nachträglich beeinflussbar und spielt eine strategische Rolle bei der Wahl von Preisen und avisierten Verkaufsmengen.

Katz und Shapiro (1985) weisen darauf hin, dass solche variablen Kostenkomponenten durch die Kompatibilität von Diensten, ceteris paribus, kontraktiv auf die angebotene Menge wirkt. Dieser Anreiz für Unternehmen zur strategischen Mengenreduktion wirkt der eigentlichen Motivation zur Einführung von IOP, nämlich dem Nutzen von Netzwerkeffekten durch eine größere verbundene Nutzerbasis, entgegen. Gehen variable Kostenkomponenten inhärent mit einer IOP einher, sollte berücksichtigt werden, dass der obige kontraktive Mengeneffekt mögliche positive Wirkungen abschwächt. Sollten variable Kostenkomponenten durch IOP nicht entstehen, ist dennoch darauf zu achten, dass diese z. B. bei Verhandlungen über Standards in Form von mengenabhängigen Lizenzgebühren nicht artifiziell geschaffen werden. Neben einem Kanal zur wohlfahrtsreduzierenden Mengenreduktion bergen diese zudem Kollusionsgefahren (s. Kapitel 3.3.2). Im

Kontext vertikaler IOP und entstehender variabler Kosten wird diese kontraktive Mengenwirkung durch das Marginalprinzip im Profitmaximierungskalkül der Unternehmen zudem auf einen vor- bzw. nachgelagerten Markt verstärkt. Klassische Ineffizienzen entlang der Wertschöpfungskette, wie die doppelte Marginalisierung, werden hierdurch verstärkt (Bourreau et al., 2022).

2.2.1.6.3 Konsumenten- und gesamtwirtschaftliche Kosten von Interoperabilität

Neben Kostenkomponenten, die bei Firmen direkt anfallen, kann IOP auch mittelbare Kosten verursachen, die Konsumenten direkt tragen oder sich gesamtgesellschaftlich mit etwaiger Zeitverzögerung materialisieren. Kapitel 2.2.1.5 hat bereits dargelegt, dass horizontale IOP zu einer Homogenisierung horizontal konkurrierender Produkte führt. Eine geringere Möglichkeit zur Produktdifferenzierung ist gleichbedeutend mit einer reduzierten Produktvielfalt aus Konsumentensicht. Verbraucher können nur noch aus einer eingeschränkteren Produktpalette wählen und finden Produkte, die durchschnittlich schlechter zu ihren inhärenten Bedürfnissen und Präferenzen passen. Durch die schlechtere Übereinstimmung von Produkteneigenschaften und Präferenzen wirkt eine geringere Produktvielfalt schädlich auf den aus dem Konsum gewonnenen Nutzen und letztendlich die Gesamtwohlfahrt (Brynjolfsson et al., 2003; Scherer, 1979). Dieser Wirkungskanal zwischen der Produktvielfalt und einem Wohlfahrtseffekt ist dann besonders bedeutend, wenn Konsumentenpräferenzen besonders stark ausgeprägt sind, d.h. Vorlieben oder Abneigung zu bestimmten Produkteigenschaften eine große Bedeutung für den Konsumentennutzen haben (Norman und Thisse, 1996).

Insbesondere im Kontext der Plattformökonomie oder auch Messaging-Diensten können angebotene Produkte als zunehmend komplex angenommen werden und diese weisen eine Vielzahl an Eigenschaften auf, zu denen konsumentenseitig entsprechende Präferenzen vorherrschen. Insbesondere Präferenzen über Privatsphäre- und Datenschutz-Einstellungen oder Funktionsumfang der Dienste sind maßgeblich heterogen zwischen Konsumenten, sodass es bei einer Einschränkung der Produktvielfalt zu signifikanten Nutzeneinbußen kommen kann.

Kosteneffekte von Interoperabilität

- Unternehmensspezifische **Fixkosten** durch die Einführung von IOP stellen versunkene Kosten dar und **sind nicht wettbewerbsrelevant**, sofern sie einmal gezahlt sind. Nichtsdestotrotz können solche Kostenkomponenten die **Einführung von IOP erschweren** und als **Markteintrittsbarriere** für kleine Unternehmen fungieren. Es ist zudem mit fortlaufenden Kostenaufwendungen zum Erhalt und **Pflege** von IOP-Schnittstellen zu rechnen.
- Mengenabhängige **(variable) Kosten** durch IOP sind **wettbewerbsrelevant** und haben eine **kontraktive Wirkung auf die angebotene Menge** bzw. setzten Anreize die eigene Nutzerbasis zu reduzieren. Dies wirkt **konträr zur eigentlichen Motivation von IOP**, der Nutzung von Netzwerkeffekten durch eine möglichst große verbundene Nutzerbasis.
- IOP führt zu einer **geringeren Produktvielfalt** zwischen horizontal konkurrierenden Produkten und impliziert eine **schlechtere Übereinstimmung von Produkteigenschaften und Konsumentenpräferenzen**. Der resultierende negative Wohlfahrtseffekt ist besonders bedeutend, wenn Konsumentenpräferenzen stark ausgeprägt sind.

2.2.2 Interoperabilität und Innovationsanreize

Entscheidungen zu Innovation und Investition in Forschung und Entwicklung werden immer in einem aktuellen Wettbewerbsumfeld getroffen und berücksichtigen zukünftige und noch unsichere Marktsituationen. Mechanismen, die den Innovationswillen von Unternehmen fördern sollen, nehmen daher strategischen Einfluss entweder auf die derzeitige oder zukünftige Marktsituation nach einer Innovation. Die Beurteilung von Innovationswirkungen durch IOP als natürlich auftretenden Aspekt als auch exogenes Instrument, folgt dieser Logik. Unter Anwendung, der aus dem Kapitel 2.2.1 bekannten statischen Wettbewerbseffekte von IOP auf einen längerfristigen Zeithorizont, lassen sich so dynamische Auswirkungen abschätzen. Ähnlich zum vorangegangenen Kapitel werden an dieser Stelle Implikationen für Innovationen allgemein erläutert. Für einen konkreten Bezug, insbesondere zu Innovationswirkungen auf Märkten der Plattformökonomie bzw. zu Messaging-Diensten, verweisen wir auf Kapitel 3.2.2 und 3.3.5 und separat zu Messengern auf Kapitel 4.

Bei der Bewertung von Innovationsanreizen im Kontext von IOP ist es sinnvoll zwischen Auswirkungen von IOP auf einerseits horizontaler Ebene und andererseits vertikaler Ebene, also zu vor- bzw. nachgelagerten Märkten, zu unterscheiden. Die Vorteilhaftigkeit von IOP und zu erwartende Innovationseffekte unterscheiden sich in dieser Hinsicht teilweise deutlich.

2.2.2.1 Innovationswirkungen durch vertikale Interoperabilität

Investitionen in innovative Vorhaben stellen grundsätzlich Entscheidungen unter Unsicherheit dar. Dies trifft insbesondere auf Märkte der Plattformökonomie zu, die durch eine komplexe Gemengelage aus Wettbewerbsdynamik, technischem Fortschritt und potenziellen regulatorischen Eingriffen geprägt sind. Eine exogen vorgegebene IOP von Diensten, möglicherweise über einen Standard, schafft in diesem Marktkontext Planungssicherheit über in Zukunft angebotene Produkteigenschaften oder technisch verfügbare Schnittstellen. Diese Sicherheit fördert nicht nur die Planbarkeit von Innovationsvorhaben auf horizontaler Ebene, sondern insbesondere auch die Entwicklung neuer komplementärer vertikaler Produkte und Dienste (Baldwin et al., 2000; Farrell und Simcoe, 2012b). Insbesondere die garantierte Verfügbarkeit von technischen Schnittstellen ist bei der Entwicklung von komplementären Diensten auf digitalen Märkten ein kritischer Unsicherheitsfaktor.

Im Falle von vertikaler IOP, die symmetrisch von allen Diensten der vorgelagerten Wirtschaftsstufe gewahrt werden muss, entsteht ein weiterer positiver Innovationsaspekt. Durch eine größere relevante Nutzerbasis aller nun interoperablen Dienste, vergrößert sich der potenzielle Absatzmarkt für komplementäre Diensteanbieter. Ohne vertikale IOP-Regelung stellen möglicherweise nur einzelne Anbieter entsprechende API-Schnittstellen zur Verfügung, wohingegen ein entsprechender symmetrischer IOP-Standard Nutzer aller Anbieter technisch erreichbar macht. Der adressierbare Markt für komplementäre Anbieter vergrößert sich somit und es wird attraktiver auf vor- und nachgelagerten Märkten neue komplementäre Produkte und Dienste für die vergrößerte Nutzerbasis zu entwickeln (Katz und Shapiro, 1985).

Im Extremfall eröffnet IOP möglicherweise sogar erst das Entstehen gänzlich neuer komplementärer Geschäftsmodelle und befähigt Konsumenten zum sog. „Mix and Match“ und dem Erstellen eigener innovativer Dienste Kompositionen. Matutes und Regibeau (1988) zeigen, dass die Kombinationsmöglichkeit verschiedener modularer Dienste einerseits Nutzengewinne durch eine erhöhte Produktvielfalt generiert und Unternehmen in der Lage sind durch höhere Preise an diesen zu partizipieren. Private und gesamtwirtschaftliche Anreize zu vertikaler IOP können somit gleichgerichtet sein und entsprechende IOP-Schnittstellen stellen sich möglicherweise marktgetrieben ein.

2.2.2.2 Innovationswirkungen durch horizontale Interoperabilität

Während zu erwartende Innovationseffekte von vertikaler IOP überwiegend positiv sind, birgt IOP auf horizontaler Ebene jedoch einige Innovationshemmnisse. Zunächst werden durch das Festsetzen eines IOP-Standards bestimmte Produkteigenschaften und technische Schnittstellen zwar garantiert, Standards können jedoch auch einen bestimmten Technologiestand oder einen Umsetzungsprozess festschreiben. Die technische Umset-

zung solcher IOP-Vorgaben mit heutigen Mitteln, kann zukünftig möglicherweise effizienter erfolgen. Innovationen in dieser Hinsicht können daher erschwert werden, wenn Standards nicht ausreichend flexibel und zukunftssicher formuliert sind. Die Gefahr eines zu rigiden technischen Standards ist vor allem dann gegeben, wenn er exogen festgesetzt wird und sich nicht marktgetrieben als de-facto herausstellt (Arthur, 1989).

Eine weitere Innovationsproblematik kann mit dem Vergrößern von Netzwerkeffekten durch horizontale IOP und den damit verbundenen konkurrierenden Produkten einhergehen. Die Ausweitung von anbieterspezifischen Netzwerkeffekten auf den gesamten Markt bewirkt zwar, dass Märkte nicht zu einem einzelnen Anbieter „kippen“, impliziert aber gleichzeitig, dass der derzeitige Technologiestand möglicherweise über einen Standard manifestiert wird. Produktinnovationen, die eine Abweichung von diesem Standard bedeuten würden, sind möglicherweise nicht mehr interoperabel zu bereits bestehenden Konkurrenzprodukten und dessen Nachfrager profitieren nicht mehr von marktweiten Netzwerkeffekten. Die geringere Attraktivität aus Verbrauchersicht von innovativen, aber nicht-interoperablen Produkten hemmt entsprechende Nachfrageverschiebungen, reduziert mögliche Innovationsrenten der Anbieter und verwässert die unilateralen Anreize überhaupt erst zu innovieren. Obwohl die Innovation gesamtwirtschaftlich wünschenswert ist, unterbleibt sie, da unilaterale private Anreize durch den Verlust von marktweiten Netzwerkeffekten zu gering sind und frühe Innovatoren überproportional hohe Kosten von dann fehlender IOP tragen (Farrell und Saloner, 1985a; Farrell und Saloner, 1986b). In der ökonomischen Literatur wird dieses Phänomen als „Excess Inertia“ beschrieben, also einem ineffizienten Verharren im Status quo. Das marktgetriebene Ausbrechen aus einer solchen Innovationsfalle ist dabei sehr schwer oder gänzlich nicht zu erwarten (Arthur, 1989; David, 1985). Diese Gefahr ist insbesondere dann gegeben, wenn zu erwartende Netzwerkeffekte besonders stark sind und Verluste durch fehlende IOP für den First-Mover der Innovation dementsprechend hoch ausfallen.

Während horizontale IOP in statischer Perspektive hilfreich sein kann Wettbewerb innerhalb eines Marktes herzustellen und durch Netzwerkeffekte gekippte Marktkonzentrationen aufzulösen (s. Kapitel 3.2.1), ergeben sich auf langfristiger, dynamischer Sicht jedoch zusätzliche Innovationsgefahren. Digitale Plattformmärkte sind generell dynamisch und weisen grundsätzlich hohe Anreize für Innovationen auf. Wettbewerbsvorteile durch innovative Produkte werden durch bestehende Netzwerkeffekte schnell potenziert und können so zu substanziellen Nachfragegewinnen führen (s. Kapitel 3.3.1 zu Wettbewerb um den Markt). Diese positiven Nachfrageelastizitäten für das marktsuperiore Produkt eines Anbieters sind ökonomisch effizient und sichern notwendige Innovationsrenten und rechtfertigen Investitionsausgaben ähnlich zur Wirkungsweise von Patenten (Gallini, 2002; Kamien, 1992). Ein Markteingriff zur Etablierung von horizontaler IOP schmälert daher möglicherweise Renten bereits erfolgter Innovationen oder aber signalisiert die Möglichkeit weiterer IOP-Eingriffe in der Zukunft. Insbesondere letzteres stellt einen möglichen Risikofaktor für zukünftige Innovationsvorhaben dar. In einem Umfeld starker firmenspezifischer Netzwerkeffekte könnten Unternehmen so Opfer ihres eigenen Erfolges werden,

indem natürliche Marktdynamiken zwar innovative Produkte überproportional belohnen, aber diese Renten durch einen ex-post IOP-Eingriff auch Wettbewerbern zugänglich gemacht werden. Vor diesem Hintergrund betonen unter anderem Geradin und Rato (2007) die Wichtigkeit von angemessenen (FRAND – „Fair reasonable and non discriminatory") Lizenzzahlungen zur Wahrung von Innovationsanreizen bei der Einführung von möglichen IOP-Standards.

Interoperabilität und Innovation

- **Vertikale IOP** schafft **Planungssicherheit** über zur Verfügung stehende technische Schnittstellen (APIs) und **fördert Innovationen komplementärer Anbieter**. Ebenso sichern verpflichtende vertikale IOP-Standards die **Erreichbarkeit der gesamten Nutzerbasis** eines Marktes und vergrößert so das **Nachfragepotenzial auf vor- und nachgelagerten Märkten**.
- **Horizontale IOP** birgt **Innovationsgefahren,** indem der derzeitige technische Innovationsstand zementiert wird. **Technische Weiterentwicklungen** sind entweder durch Einhaltung eines nicht zukunftssicheren Standards **nicht möglich** oder werden **unterlassen**, da **marktweite Netzwerkeffekte** für ein **innovatives, aber nicht-interoperables Produkt** zunächst **nicht anfallen** („Excess Inertia"). Zusätzlich können mögliche IOP-Auflagen auf horizontaler Ebene entstehende **Wettbewerbsvorteile abschwächen** und so wichtige **Innovationsrenten reduzieren**.

2.2.3 Interoperabilität und Verbraucherschutz

In der digitalen Gesellschaft spielen IOP und Kompatibilität von Waren und Dienstleistungen auch aus der Perspektive des Verbraucherschutzes eine immer wichtigere Rolle. Dem trägt das deutsche und europäische Verbraucherrecht durch eine Reihe von neueren Regelungen Rechnung. Als Beispiel kann die vorvertragliche Informationspflicht aus § 312d Abs. 1 BGB i.V.m. Art. 246a § 1 Abs. 1 S. 1 Nr. 18 EGBGB genannt werden.[4] Danach sind Unternehmer bei außerhalb von Geschäftsräumen geschlossenen Verträgen und Fernabsatzverträgen verpflichtet, dem Verbraucher vor Vertragsschluss Informationen über die Kompatibilität und die IOP von Waren mit digitalen Elementen (§ 327a Abs. 3 S. 1 BGB) oder digitalen Produkten (§ 327 Abs. 1 S. 1 BGB) zur Verfügung zu

4 Die Vorschrift geht in ihrer ursprünglichen Form auf Art. 5 Abs. 1 lit. h) Verbraucherrechte-RL 2011/83/EU zurück (vgl. auch Erwgr. 19 Verbraucherrechte-RL: „Der Begriff der wesentlichen Interoperabilität beschreibt die Information in Bezug auf die standardmäßige Umgebung an Hard- und Software, mit der die digitalen Inhalte kompatibel sind, etwa das Betriebssystem, die notwendige Version und bestimmte Eigenschaften der Hardware."). Die aktuelle Fassung der Vorschrift, die ab dem 28.5.2022 anwendbar ist, geht auf Art. 4 Abs. 3 lit. b) der Modernisierungs-RL (EU) 2019/2161 zurück.

stellen.[5] Der Begriff der IOP bezieht sich nach der Gesetzesbegründung etwa auf Hard- und Software, mit denen digitale Inhalte verwendet werden können (BT-Drs. 17/12637, 74). Der Gesetzestext schränkt den Umfang der Informationspflicht allerdings in zweifacher Weise ein. Zum einen sind die Angaben über Kompatibilität und IOP nur erforderlich, soweit diese „wesentlich" sind. Zum anderen besteht die Aufklärungspflicht nur, „soweit diese Informationen dem Unternehmer bekannt sind oder bekannt sein müssen." Der Unternehmer muss daher nur über die IOP und Kompatibilität mit einigermaßen marktgängiger und aktueller Hard- und Software informieren; ein Hinweis auf die fehlende Verwendbarkeit mit ganz veralteten und kaum noch gebräuchlichen Systemen ist nicht erforderlich (BT-Drs. 17/12637, 74).

Durch das Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 25.6.2021 (BGBl. 2021 I 2123) wurden die Begriffe „Kompatibilität" und „Interoperabilität" an noch prominenterer Stelle im deutschen Verbrauchervertragsrecht verankert. Nach § 327e Abs. 2 S. 1 Nr. 1 lit. a) BGB n.F. entspricht ein digitales Produkt den subjektiven Anforderungen an die Produktqualität, wenn es „die vereinbarte Beschaffenheit hat, einschließlich der Anforderungen an seine Menge, seine Funktionalität, seine Kompatibilität und seine Interoperabilität".[6] Gemäß der Legaldefinition in § 327e Abs. 2 S. 3 BGB n.F. und der zugrunde liegenden Definition in Art. 2 Nr. 10 Digitale-Inhalte-Richtlinie (EU) 2019/770 bezeichnet der Begriff der Kompatibilität „die Fähigkeit eines digitalen Produkts, mit Hardware oder Software zu funktionieren, mit der digitale Produkte derselben Art in der Regel genutzt werden ohne dass sie konvertiert werden müssen". IOP wird demgegenüber in § 327e Abs. 2 S. 4 BGB n.F. im Anschluss an Art. 2 Nr. 12 Digitale-Inhalte-Richtlinie (EU) 2019/770 definiert als „die Fähigkeit eines digitalen Produkts, mit anderer Hardware oder Software als derjenigen, mit der digitale Produkte derselben Art in der Regel genutzt werden, zu funktionieren". Diese Begriffsbestimmungen weichen von den gängigen technischen Definitionen ab, die etwa in der Informatik gebräuchlich sind (Metzger, in: MüKoBGB, 9. Aufl. 2022, BGB § 327e Rn. 14).

Gemäß § 327e Abs. 3 BGB gehört die Kompatibilität mit üblicher Hard- und Software auch zu objektiven Anforderungen an die Qualität digitaler Produkte, die unabhängig von einer entsprechenden Parteivereinbarung vorliegen müssen, damit ein digitales Produkt frei von Produktmängeln ist. Nach § 327e Abs. 3 S. 1 Nr. 2 BGB entspricht ein digitales Produkt den objektiven Anforderungen an die Produktqualität, wenn „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". Anders als die Kompatibilität ist die IOP dagegen nur als subjektive Anforderung und nicht auch als objektive Anforderung i.S.d. § 327e Abs. 3

5 Bei anderen Verbraucherverträgen ergibt sich eine entsprechende Informationspflicht aus § 312a Abs. 2 BGB i.V.m. Art. 246 Abs. 1 Nr. 8 EGBGB.

6 Eine entsprechende Regelung für Kaufverträge wurde durch das Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags vom 25.6.2021 (BGBl. 2021 I 2133) in § 434 Abs. 2 S. 2 BGB n.F. eingefügt.

vorgesehen. Dem liegt die Überlegung zugrunde, dass der Unternehmer, der die digitalen Produkte bereitstellt, nicht für die unüberschaubare Vielfalt nicht regelmäßig verwendeter Kombinationen der digitalen Produkte mit Hard- und Software Vorkehrungen treffen kann (Schulze, in: HK-BGB, 11. Aufl. 2021, BGB § 327e Rn. 14).

Die hier genannten Vorschriften sind auch für Verträge über den Zugang zu digitalen Plattformen (z. B. Social Media Plattformen) und Messaging-Diensten relevant. Zu den nach § 327e Abs. 3 S. 1 Nr. 2 BGB zu beachtenden objektiven Anforderungen an Messaging-Dienste gehört danach die Kompatibilität mit der üblichen Hard- und Softwareumgebung. Der Umfang der Kompatibilität (etwa die Verwendbarkeit mit verschiedenen Versionen eines Betriebssystems) hängt davon ab, welche Beschaffenheit „bei digitalen Produkten derselben Art üblich ist und […] die der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann“ (§ 327e Abs. 3 S. 1 Nr. 2 BGB). Eine IOP mit anderen Messaging-Diensten kann dagegen aus der Perspektive des Verbrauchervertragsrechts grundsätzlich nicht erwartet werden, da die IOP nach § 327e Abs. 3 BGB nicht zu den objektiven Qualitätsanforderungen digitaler Produkte zählt.

3 Interoperabilität in der Plattformökonomie

3.1 Besonderheiten von digitalen Plattformdiensten & Status quo der Interoperabilität

Belleflamme und Peitz (2021) resümieren, dass beim Aufbau einer Plattform positive Netzwerkeffekte zu einer Spirale der Attrahierung führen. Bei Plattformen sind meistens indirekte Netzwerkeffekte maßgeblich, die über zwei oder mehrere Nutzerseiten wirken. Somit gehen Plattformen über reine Netzwerke hinaus, woraus sich die Notwendigkeit einer detaillierteren Betrachtung der genauen Wechselwirkungen der Gruppen, über die gruppeninhärenten Externalitäten hinaus, ergibt. Messaging-Dienste, die in ihrer Kernfunktion eine Nutzergruppe bedienen und deren genauen Eigenschaften in Kapitel 4.1 detaillierter erläutert werden, erfahren via direkter Netzwerkeffekte eine steigende Attraktivität des Dienstes, je mehr Bekannte und Kontaktpersonen diesen Dienst bereits nutzen. Zwar sind reine Messenger nicht als mehrseitige Plattform im Sinne der Auslegung in Kapitel 2.1.1.2 zu betrachten, liefern aber eine unmittelbare Erläuterung für die Wirkungsweise von direkten Netzwerkeffekten.[7] Die Anzahl der Nutzer übt dabei einen gruppeninhärenten („within-group“) positiven direkten Netzwerkeffekt auf weitere potenzielle Nutzer aus. Die gleiche Wirkungsweise eines innerhalb der Gruppe wirkenden Netzwerkeffektes gilt bei sozialen Netzwerken wie Facebook oder Instagram unter Vernachlässigung von Werbepartnern zwischen den Nutzern des Netzwerkes. Je mehr Nutzer in einem sozialen Netzwerk aktiv sind, desto attraktiver ist die Interaktion für andere (potenzielle) Nutzer.

Dabei können asymmetrische Preisstrukturen und Quersubventionierungen zwischen verschiedenen Marktseiten durch Plattformbetreiber im Gleichgewicht auftreten. Wright (2004) verweist als Beispiel für die Quersubventionierung von Matching-Plattformen auf Nachtklubs, in denen Frauen und Männer die Gruppen mit der gruppenübergreifenden gegenseitigen positiven Wertschätzung darstellen (Wright, 2004). Als digitale Pendants hierzu gelten Online-Datingportale oder andere Matching-Plattformen wie AirBnB.

Anzumerken ist jedoch, dass Netzwerkeffekte auch negativ skalieren könnten. Unter Annahme eines bereits stark unter Mitgliederschwund leidenden sozialen Netzwerkes verliert dieses auch für verbleibende Teilnehmer (Nutzer sowie ggf. andere Marktseiten) an Attraktivität. Jedoch unterliegen Nutzer häufig einem Koordinierungsproblem, was eine „kritische Abwanderung“ erschwert.

---

7 In der Literatur finden sich ebenso Definitionen, die eine Plattformeigenschaft anhand der Koordinierung von Netzwerkeffekten und somit unabhängig mehrerer teilnehmender Marktseiten attestieren (Belleflamme und Peitz, 2021). Sanchez-Cartas und León (2021) geben einen umfassenden Überblick über die seit jeher bestehende Bandbreite an verschiedenen Definitionsansätzen von Plattformen.

Im Fall von Messaging-Diensten führen direkte Netzwerkeffekte zu einer Spirale der Attrahierung, die zu Konzentrationstendenzen am Markt führen kann. In diesem Zusammenhang existieren fundierte theoretische Untersuchungen zu den Phasen des starken Wachstums und dem Erreichen einer kritischen Masse (Evans, 2009; Evans und Schmalensee, 2010). Differenzierter sind diese Konzentrationstendenzen jedoch im Kontext gruppenübergreifender asymmetrischer Netzwerkeffekte, wie zum Beispiel bei werbefinanzierten Plattformen zu betrachten. Hier beeinflussen die Nutzer zwar die Werbetreibenden positiv, konträr dazu empfinden Nutzer jedoch mehr Werbetreibende nicht zwingend als Bereicherung (Armstrong, 2006). Im oben erläuterten Beispiel eines sozialen Netzwerkes wie Facebook üben dementsprechend die Nutzer eine positive Externalität auf die anderen Nutzer (positiver „within-group"-Effekt) und die Werbetreibenden (positiver „cross-group"-Effekt) aus. Die Werbetreibenden hingegen dürften auf die Nutzer bestenfalls keine Externalität, tendenziell in Form einer negativen Externalität (negativer „cross-group"-Effekt) wirken. Diese Konstellation von Netzwerkeffekten führt gemäß Belleflamme und Peitz (2021) zu einem Anziehungs-Abstoßungs-Pendel.

Ein weiterer relevanter Punkt, der sich aus den Netzwerkeffekten ergibt, sind datengetriebene Lerneffekte. Prüfer und Schottmüller zeigen, dass datengetriebene Lerneffekte zu einer stärkeren Marktkonzentration führen und somit auch Auswirkungen auf die Innovationsbereitschaft haben (Prüfer und Schottmüller, 2021). Je nachdem, ob das Lernen aus den Daten "within-user" (nutzerspezifisch) oder "across-user" (nutzerübergreifend) erfolgt, treten möglicherweise keine Datennetzwerkeffekte auf (Hagiu und Wright, 2020a). Im Falle nutzerspezifischer Lerneffekte erhöhen sich allerdings die individuellen Wechselkosten und somit der Lock-In des einzelnen Nutzers, da der entsprechende Anbieter die umfassendste Personalisierung anbieten kann. Dem könnte mit Datenportabilität oder einer Daten-IOP entgegengewirkt werden. Nutzerübergreifendes Lernen bezieht sich darauf, dass ein Unternehmen in der Lage ist, sein Produkt für jeden Kunden auf der Grundlage des Lernens aus Daten von allen Kunden zu verbessern. Dies kann in bestimmten Szenarien zu mit konventionellen Netzwerkeffekten vergleichbaren Effekten führen - zum Beispiel, wenn es mit kontinuierlichen Produktverbesserungen kombiniert wird (Hagiu und Wright, 2020b). Nutzerübergreifendes Lernen liegt dabei in einer Vielzahl von Vorhersage- und Empfehlungsmechanismen vor, da z. B. die Qualität von Verkehrsvorhersagen steigt, je mehr Anwender einen Verkehrsdienst nutzen.

Digitale Plattformmärkte neigen daher durch positive Netzwerkeffekte dazu an einem „Tipping"-Punkt zugunsten eines Unternehmens bzw. Dienstes „kippen", was dazu führt, dass die Netzwerkeffekte und der Vorsprung gesammelter Daten die Bestreitbarkeit eines Marktes im Sinne natürlicher Monopole erschweren können.[8] Gründe für diese „Kipppunkte" können in hohen Wechselkosten liegen, welche wiederum zu Lock-In-Effekten

8 Vgl. dazu Baumol et al. (1983) zur Bestreitbarkeit natürlicher Monopole. Anzumerken ist hierbei, dass klassische natürliche Monopole aufgrund der Kostenstruktur nicht bestreitbar sind, während bei digitalen Plattformmärkten primär die Nachfrageseite und deren positive gruppeninhärente Externalität zur

führen. So stellen beispielsweise im Kontext von sozialen Netzwerken die aufgebauten Kontakte einen „Netzwerk-Lock-in“ dar, welche wiederum die Wechselkosten zu anderen Diensten hin erhöhen. Ergänzend bei und abseits sozialer Netzwerke vorrangig, sind persönliche Lock-In-Effekte resultierend aus der Personalisierung eines Dienstes.[9] Bis zur Erreichung des markt- und segmentspezifischen „Tipping-Punktes“, besteht jedoch eine sogenannte „Henne-Ei-Problematik“. Diese besteht aus den fehlenden anfänglichen Netzeffekten während des Aufbaus einer Plattform, welche sich wiederum negativ auf die Attraktivität auswirkt. Zur Überwindung dieses Anfangsstadiums können unter anderen die Subventionierung der preissensitiveren Marktseite, Exklusivitätsverträge[10] aber auch eine anfänglich offenere Plattform-Governance dienen. Im Hintergrund steht hierbei die Entwicklung eines „Ökosystems, das im Zuge eines „Envelopments“ von durch die Netzwerkeffekte tangierten Märkten gebildet wird (Eisenmann et al., 2011). Durch die entstehende Bündelung zusätzlicher modularer Funktionen wird das Ökosystem und die eigene Plattform erweitert (Tiwana et al., 2010). Können große Nutzerbasen in digitalen Ökosystemen „eingeschlossen“ („walled-garden“) werden, liegt hier im Sinne Armstrongs (2006) ein „competitive bottleneck“ vor. Aus diesem Konzept leitet sich auch die Funktion digitaler Plattformen als „Gatekeeper“ her, da diese entsprechend über den Zugang zu großen Nutzergruppen in Absenz von Abhilfemaßnahmen verfügen können.

Auf Grund der oben ausgeführten Unterschiede hinsichtlich des Wachstums auf Plattformmärkten ergeben sich auch entsprechende Besonderheiten für die strategische Nutzung der Offenheit einer Plattform. Gemäß dem Autorité de la Concurrence und CMA (2014) werden offene Systeme über die Bereitstellung von Schnittstellen definiert, die es auch Dritten ermöglicht Komplemente bereitzustellen. Im Gegensatz hierzu ist bei geschlossenen Systemen eine Kompatibilität auf ausgewählte Komplemente beschränkt. Eisenmann et al. (2009) definieren Offenheit im Kontext einer Softwareplattform, höchstens mit „vertretbaren“ Einschränkungen hinsichtlich der Kontribution, Entwicklung, Nutzung und Kommerzialisierung, die obendrein alle Parteien vergleichbar betreffen. Benlian et al. (2015) formulieren die strategische Entscheidung zur vertikalen Offenheit von Plattformen als einen Trade-Off zwischen Diversität und Kontrolle.

Jedoch gibt es auch strategische Beschränkungen, so können z. B. eBooks und Apps aus dem Apple-Ökosystem in der Regel nicht auf Android-Geräten genutzt werden. Die Gründe hierfür liegen zum einen gezielten Strategien der Plattformfirmen, die ein Abwandern durch technische und vertragliche Gestaltung ihrer eigenen Dienste und Inhalte ver-

fehlenden Bestreitbarkeit führt(Jullien und Sand-Zantman, 2021). (Belleflamme und Peitz, 2021) wiederum sehen in der Möglichkeit zum Multi-Homing als Reduktion der Markteintrittskosten die klare Abgrenzung zu natürlichen Monopolen. Bzgl. des „Kippens“ digitaler Märkte siehe z. B. OECD (2018), Jacobides und Lianos (2021a).

9 Personalisierte Algorithmen für nutzerspezifische Vorschläge, Playlists, beobachtete Artikel o. Ä.

10 Siehe Lee (2013) zum Effekt von Exklusivitätsvereinbarungen in der US-amerikanischen Videospielindustrie.

hindern möchten, aber auch eine erhöhte Möglichkeit der Durchsetzung solcher Praktiken auf Basis des Urheberrechts (Doctorow, 2022). So wird z. B. der Einsatz von Reverse Engineering, Scraping Bots oder Bridges häufig rigoros durch Klagen verhindert.

3.1.1 Status quo: Bestehende Arten von Interoperabilität

Die Problematik der Konzentrationstendenzen und die Gratwanderung einer effizienten Gestaltung der Rahmensetzungen ist Gegenstand akademischer und politischer Diskussionen. Aus diesem Grund finden Plattformen und ihre Funktion als Gatekeeper zunehmend Berücksichtigung in der Ausgestaltung von Wettbewerbs- und Regulierungsrecht. So wurde im novellierten TKG (Anfang Dez. 2021 in Kraft getreten) die rechtliche Grundlage geschaffen, IOP-Verpflichtungen für NI-ICS aufzuerlegen. Die 10. GWB-Novelle berücksichtigt die Rolle von Gatekeepern ebenso wie das verabschiedete DMA-Gesetz der Europäischen Kommission. Ein kurzer Überblick über implementierte und geplante rechtliche Vorschriften ist in Kapitel 3.1.2 zu finden. Da Wechselkosten von großer Relevanz für die Wettbewerbsverhältnisse auf digitalen Märkten sind, ist eine Verringerung dieser Kosten essenzieller Bestandteil der Abhilfemaßnahmen. Aus technischer Betrachtung können durch Koordination der beteiligten Parteien häufiger niedrige Wechselkosten ermöglicht werden. Im Vergleich zu klassischen analogen und physischen Märkten sind verschiedene Formen von Portabilität, Kompatibilität und darauf aufbauend auch IOP im Kontext des digitalen Sektors aufgrund nachträglicher Produktanpassungen durch Soft- und Firmwareanpassungen vergleichsweise friktionsärmer zu realisieren. Klassische Telekommunikationsdienste wurden via Standardisierung zu interoperablen Diensten, waren dadurch jedoch im Verhältnis zu neuen webbasierten Kommunikationsdiensten langsamer in der Anpassungsfähigkeit gegenüber neuen Ansprüchen von Verbrauchern.

Im Folgenden werden der Status quo bestehender Arten der IOP und strategische Einschränkungen erläutert.

3.1.1.1 Meta/Facebooks Handhabung von Zugangsmöglichkeiten via API

Die Unterteilung in horizontale und vertikale Wirkungsweisen von IOP findet sich auch im aktuellen Status kompatibler und interoperabler Funktionalitäten. Meta bietet beispielsweise für den Dienst Instagram die Möglichkeit von Cross-Posting über Plattformen an, wenngleich diese Möglichkeit sich in den Optionen befindet und damit nicht offensichtlich ist (Scott Morton et al., 2021). Dieses Cross-Posting beschränkt sich dabei nicht auf weitere Unternehmen des Meta-Konzerns, sondern beinhaltet auch soziale Dienste im russischsprachigen Raum (VKontakte, OK.ru) und Twitter sowie Tumblr. Damit nutzt Instagram die Offenheit anderer sozialer Dienste via deren APIs strategisch für die Bekanntheit der eigenen Inhalte, was je nach expliziter Ausgestaltung und Nutzung der APIs asymmetrischer oder sogar vertikaler IOP entspricht. Gleichzeitig unternimmt Meta Anstrengungen die eigenen Plattformen weiter miteinander zu verbinden und somit, wenn

auch konzernintern, zu interoperabilisieren (vgl. hierzu Yurieff, 2020). Der Ende 2020 erweiterte Messenger in Instagram ist zum Facebook Messenger interoperabel, wohingegen beide aktuell noch keine IOP mit WhatsApp bieten (Meta, 2020). Detaillierte Erläuterungen zu den Hintergründen sind in Kapitel 4 zu finden.

Jedoch erläutern Scott Morton et al. (2021) auch gegenläufige und damit restriktivere Konzernpraktiken am Beispiel von Vine, einem inzwischen außer Dienst gestellten Kurzvideo-Dienst, bei welchem anfangs Nutzern anhand der „Freunde-finden"-API die Möglichkeit geboten wurde Videos an ihre „Facebook-Freunde" zu versenden. Nach Übernahme Vines durch Twitter, empfand Facebook augenscheinlich die Verknüpfung einer so essenziellen Funktion mit einem konkurrierenden sozialen Netzwerk als Bedrohung und änderte einseitig die API. Somit verlor Vine eine attraktive Funktion und Facebook konterkarierte einen mutmaßlich treibenden Grund der Übernahme Twitters. Letztendlich konnte sich Vine nicht am Markt behaupten und wurde eingestellt. Andererseits bietet und bot das soziale Netzwerk Facebook viele Möglichkeiten Funktionalitäten des eigenen Ökosystems (beispielsweise Facebook-Login, Like-Button, „Teilen auf Facebook") zur vertikalen Nutzung (im Fall Facebook-Login) oder Erweiterung der eigenen Plattform-Inhalte („Teilen auf Facebook"). Letzteres Motiv schien auch Bestandteil der ursprünglichen Handhabung von Inhalten des Kurzvideodienstes Vine zu sein, bis mit Twitter ein „schärferer" Konkurrent diesen übernahm. Auch dass Facebook zunehmend die starke Wachstumsphase verlassen hat, dürfte in diesem Kontext eine Rolle spielen. Aus wettbewerblicher Sicht ist aus diesem gemachten Unterschied seitens des Meta-Konzerns interessant, dass zum einen die Konkurrenzsituation zwischen den sozialen Netzwerken Auswirkungen auf die strategische Nutzung von Offenheit hat als auch, dass asymmetrische Cross-Postings einer strategischen Steuerung des Aufmerksamkeitsflusses folgen.

3.1.1.2 Amazon Selling Partner API

Als Beispiel vertikaler IOP kann die Amazon Selling Partner API (SP-API) betrachtet werden. Diese stellt vertikalen Anbietern von Produkten auf dem Amazon Marketplace unter anderem die Möglichkeit ihre Produkte einzustellen, Preise zu aktualisieren, Käufer zu kontaktieren oder den Versandstatus einzusehen bzw. zu aktualisieren. Die genauen Funktionen und der Aufbau der API werden seitens Amazons umfangreich dokumentiert (Amazon, 2022). Die Bereitstellung eines Frameworks für Drittanbieter auf der eigenen Plattform ist Bestandteil des Strategiewechsels von Amazon vom Einzelhändler zum Anbieter einer Verkaufsplattform. Amazon konkurriert dabei weiterhin als Einzelhändler mit den Anbietern auf dem Marketplace, gleichzeitig bietet es jedoch mit dem Versand für Marketplace-Anbieter eine nachgelagerte Dienstleistung an.

3.1.1.3 PSD2 und Open Banking

Die zweite Payment Services Directive (PSD2) der Europäischen Kommission ist ein regulatorischer Rahmen für Bezahl- und Bankendienstleistungen und sollte Geldüberweisungen zwischen Banken vereinfachen und beschleunigen. Ferner werden Zahlungsdienstleister angehalten, Zugriff auf einzelne Funktionalitäten (beispielsweise Kontostandabfragen, Identifikation) zu ermöglichen. Hiervon versprach sich die Kommission eine Effizienzsteigerung des europäischen Marktes für Zahlungsdienstleistungen und innovative Dienste, welche auf diese nun verfügbaren Funktionen aufbauen sollten (Europäische Kommission, 2015). Zur Wahrung der Souveränität des Kunden wird eine explizite Einwilligung vorausgesetzt. Gleichzeitig wurde im Vereinigten Königreich mit der Gründung der Open Banking Working Group, diese beauftragt, den Rahmen eines offenen API-Standards zu begründen. In diesem Standard sollen Zusatzfunktionen im Sinne der PSD2 ermöglicht werden, aber darüber hinaus auch ein gemeinsamer technischer Rahmen für die Schaffung eines Ökosystems von Dienstleistungen des Finanzsektors. Auf Basis dieses Standards sollen einzelne Dienstleistungen im Banken- und Finanzierungssektor disaggregiert und modular angeboten werden. Eine mögliche Folge davon wäre neben der Reduktion von Lock-In-Effekten und Wechselkosten eine Plattform auf der Kunden aus den Angeboten multipler Anbieter frei wählen könnten (Open Banking, 2022a). Für das zweite Quartal 2021 gibt Open Banking 319 Drittanbieter als Teilnehmer des Open Banking-Ökosystems mit über 800 Millionen API Abrufen pro Monat an (Open Banking, 2022b).

3.1.1.4 Apple NFC-Schnittstelle

Seit der 6. Generation der iPhones von 2014 ist in den Geräten ein NFC-Chip verbaut, ein offener Standard zur drahtlosen Übertragung geringer Datenmengen im Nahbereich. Die Funktionalität des NFC-Chips war dem Apple-eigenen Bezahldienst Apple Pay vorbehalten, obwohl die Spezifikation des Standards selber öffentlich einsehbar ist und eine Implementation auch Dritten möglich gewesen wäre. ACM (2019) berichtet von „dismay“ [Bestürzung] seitens App-Entwicklern über die Beschränkungen in der Nutzung. Zum Zeitpunkt des ACM-Berichts (2019) war es sogar der niederländischen Regierung nicht möglich für einen e-Identifizierungsdienst einen Zugang auf die Schnittstelle zu erhalten, während dies für Android-Geräte möglich war. Ferner berichtet ACM (2019) von gleichartigen Beschränkungen für eine App der britischen Regierung, was einem zitierten Bericht der BBC aus Sicherheitsgründen und kommerziellen Erwägungen stattfand (Wheeler, 2018). ACM (2019) verweist auf dem Umstand, dass die NFC-Schnittstelle bei Android für Dritte bereits ab 2010 möglich war, es allerdings auch Anmerkungen zu Sicherheitsbedenken in diesem Zuge gab. Ferner wird von einem Bezahldienst berichtet, der ACM gegenüber angegeben hat seinen Bezahldienst auf Grund des fehlenden Zugangs zur Schnittstelle eingestellt haben zu müssen. Die Europäische Kommission untersucht seit Juni 2020 wettbewerbliche Beschränkungen seitens Apple hinsichtlich des

Marktes für mobile Bezahldienste. In einer Stellungnahme zu den vorläufigen Ergebnissen erklärte Vestager den Verdacht, dass Apple seine Marktmacht im Ökosystem iOS zur Behinderung des Wettbewerbs zwischen Bezahldiensten missbraucht habe. Ferner verweist Vestager auf den Umstand ausgebliebener Innovationen durch den restriktiven Zugang zu Schnittstellen für Dritte (Europäische Kommission, 2022b). Mit dem Update auf die Betriebsversion iOS 14 (2021) wurde seitens Apple die Nutzung des NFC-Chips ermöglicht, jedoch beschränkt auf von Apple zugelassene und limitierte Funktionalitäten.[11]

3.1.1.5 Voice Interoperability Initiative

Im September 2019 kündigte Amazon an, in Zusammenarbeit mit weiteren namhaften Unternehmen wie Baidu, Microsoft und Spotify an einer interoperablen Lösung für digitale Sprachassistenten zu arbeiten. Dabei steht die Entwicklung eines Frameworks zur Integration mehrerer Sprachassistenten mit Hilfe unterschiedlicher Aktivierungswörter auf einzelnen Geräten im Mittelpunkt. Lyles (2020) merkt jedoch an, dass ein Jahr später unter den 70 für die Initiative gewonnenen Unternehmen, die Konkurrenten Apple, Google und Samsung fehlen. Damit sei der Erfolg dieser Initiative fraglich, da die relevanten Marktteilnehmer mit großen Kundenstämmen nicht teilnähmen. Roettgers (2021) berichtet in einem Artikel über den Lautsprecherhersteller Sonos, der Google vorwirft, obengenannte Form des Mix-und-Matches vertraglich zu unterbinden. Gleichzeitig weist Lyles darauf hin, dass genau diese großen US-Unternehmen jedoch im Rahmen der IoT-IOP zusammenarbeiten, weswegen dieses Thema im Folgenden ebenfalls kurz erörtert werden soll.

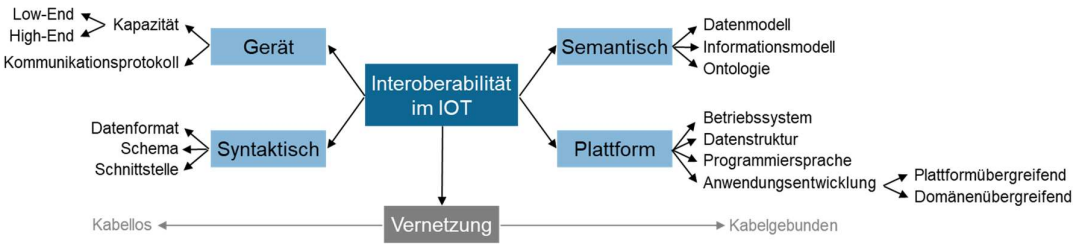
3.1.1.6 Internet of Things – Initiativen zur Interoperabilität

Das Internet of Things (IoT) ist als Kosmos smarter Geräte zu betrachten, die sich mit „smarten“ Eigenschaften von ihren herkömmlichen Pendants absetzen. Die Basis dieser smarten Eigenschaften ist eine Kommunikation mit Servern und anderen interoperablen Geräten. McKinsey gibt in einer Studie zum wirtschaftlichen Potenzial von IoT-Implementierungen an, dass 40 % der Vorteile einer IoT-Implementierung durch fehlende IOP ungenutzt blieben (Manyika et al., 2015). Hier sei die Beschränkung auf bestimmte Geräte oder Software einzelner Hersteller ein Hinderungsgrund für die Nutzung der Potenziale, da grundlegende Eigenschaften der IOP nicht über die Plattformen hinaus möglich sind und auf Konverter zurückgegriffen werden müsse. Im Bereich Smart-Home ist durch die Verwendung physischer Geräte bereits auf Geräteebene fehlende Kompatibilität möglich, so werden beispielsweise mit Bluetooth und ZigBee zwei inkompatible Funktechnologien verwendet, was eine Austauschfähigkeit im Sinne der obigen Arbeitsdefinition ohne Konverter unmöglich macht. Aber auch unterschiedliche Protokolle wie CoAP und MQTT

11 Beispielsweise App-Clips (Apple, 2021) oder CarKey (Apple, 2022).

werden verwendet, beide sind dediziert für die einfache Kommunikation zwischen Maschinen (M2M) entwickelt worden. Abbildung 3-1 zeigt die vielschichtigen Aspekte, welche eine IOP im Kontext von IoT-Geräten erschweren und zeigt zugleich, dass auch hier der Bedeutung von Plattformen große Bedeutung zugemessen wird. Mit dem Apple Homekit, Google Brillo, Amazon AWS IoT und IBM Watson werden seitens Noura et al. fünf IoT-Plattformen genannt, deren IOP durch die Verwendung unterschiedlicher Programmiersprachen oder Software Development Kits (SDKs) erschwert wird. Ein Hersteller eines IoT-Produktes müsse entsprechend die spezifischen Besonderheiten der Programmierschnittstellen lernen. Aus diesem Grund gebe es Bemühungen in IoT-Industrie und Forschung, die sich mit Adapter-Lösungen aber auch interoperablen Standards beschäftigen. Dies wird jedoch durch eine fehlende umfangreiche Dokumentation oder einen gemeinsamen Standard erschwert, was sowohl eine IOP einschränkt als auch die Entwicklung und Verbreitung von IoT hemme (Noura et al., 2019).

Abbildung 3-1: Taxonomie des IoT-Ökosystems



Quelle: Noura et al. (2019), S. 799. Übersetzung WIK-Consult.

Im Mai 2021 kündigte die Connectivity Standards Alliance (früher ZigBee Alliance) die Entwicklung eines offenen, globalen Standards (Matter, ehemals Project Connected Home over IP, CHIP*)* für die IOP zwischen Smart-Home-Geräten und IoT-Plattformen an (BusinessWire, 2021). Als Unterstützer der Allianz werden auf der Website unter anderen Amazon, Apple, Google und Huawei aufgeführt (CSA, 2022).

3.1.1.7 Covid19-Tracing

Ein Beispiel kooperativer IOP war die Bereitstellung des Covid19-Tracing Frameworks für iOS und Android, die mobilen Betriebssysteme von Apple und Alphabet. Sie entwickelten eine interoperable API, mit der die Nutzer nach Opt-in zertifizierte Apps nutzen konnten, um einen Proxy für die Dauer des Kontakts und räumliche Nähe zu erkrankten Personen zu bekommen. Hierfür verwendeten sie den Funkstandard Bluetooth Low Energy, über den sie eine anonymisierte ID an die umliegenden Geräte sendeten und gleichzeitig die IDs der Personen aufzeichnete und 14 Tage lang speicherte (Panzarino,

2020). Nach einem positiven Test war es der Person möglich die eigene ID an die Datenbank der App zu senden, wodurch ein Abgleich bei anderen Nutzern realisiert werden konnte. Aufbauend auf dieser API wurde auch die deutsche Corona-Warn-App programmiert (Reelfs et al., 2020). Damit jedoch diese Funktionalität nicht auf die Geräte innerhalb des eigenen Betriebssystems beschränkt war, entwickelten Apple und Google eine interoperable API inklusive Datenstruktur, Syntax und Semantik. Gleichzeitig veröffentlichten sie in einer umfangreichen Dokumentation, wie der Zugriff auf die API stattfindet, die ausgetauschten Daten aufgebaut sind und welcher Referenzstruktur die Datenbank der auf dieser Funktion aufbauenden App zu gestalten sei (Apple, 2020; Google, 2020).

3.1.2 Aktuelle Gesetzesentwicklungen & Forderungen nach einer Interoperabilitätspflicht

3.1.2.1 Implementierte rechtliche Vorgaben

Das novellierte Telekommunikationsgesetz (TKG) trat am 01.12.2021 in Kraft und führte neben der Erweiterung des Geltungsbereichs der TK-Vorschriften für interpersonelle Kommunikationsdienste auch anwendbare Vorschriften zur IOP ein. Der neu eingefügte § 21 Abs. 2 TKG sieht in Umsetzung von Art. 61 Abs. 2 UAbs. 2 lit. c RL (EU) 2018/1972 die Möglichkeit vor, dass die Bundesnetzagentur als zuständige Behörde Anbieter von NI-ICS unter engen Voraussetzungen zur IOP verpflichten kann. Eine Verpflichtung zur IOP kann nur für NI-ICS angeordnet werden, die eine „nennenswerte Abdeckung und Nutzerbasis“ aufweisen (§ 21 Abs. 2 Nr. 1 TKG). Nach Erwägungsgrund 151 RL (EU) 2018/1972 setzt dies voraus, dass die geografische Abdeckung und die Zahl der Endnutzer eine kritische Masse im Hinblick auf die Erreichung des Ziels einer durchgängigen Konnektivität erreicht. Erforderlich ist ferner, dass die durchgehende Konnektivität zwischen Endnutzern aufgrund der mangelnden IOP zwischen NI-ICS bedroht ist (§ 21 Abs. 2 Nr. 2 TKG) und die Anordnung von IOP zur Herstellung durchgehender Konnektivität notwendig ist (§ 21 Abs. 2 Nr. 3 TKG). In verfahrensrechtlicher Hinsicht ist darüber hinaus erforderlich, dass die Europäische Kommission Durchführungsmaßnahmen nach Art. 61 Abs. 2 UAbs. 2 ii RL (EU) 2018/1972 erlässt. Dies wiederum setzt voraus, dass die Kommission nach vorheriger Konsultation von GEREK feststellt, dass in mindestens drei Mitgliedstaaten die durchgehende Konnektivität zwischen Endnutzern in nennenswertem Ausmaß bedroht ist. Der europäische Gesetzgeber hat somit sehr hohe Hürden für eine Anordnung von IOP für Anbieter von NI-ICS aufgestellt (BT-Drs. 19/26108, 258; Stamm, 2022). Die restriktiven Regelungen des § 21 Abs. 2 TKG stehen damit in einem Spannungsverhältnis zu den neuen IOP-Verpflichtungen aus dem DMA.

Rechtliche Vorgaben hinsichtlich der Gewährleistung von IOP enthält auch § 19a GWB. Die im Rahmen der 10. GWB-Novelle neu eingefügte Regelung, die am 19.01.2021 in Kraft trat, ermöglicht es dem Bundeskartellamt, durch Verfügung die überragende marktübergreifende Bedeutung eines Unternehmens für den Wettbewerb festzustellen und

dem betreffenden Unternehmen bestimmte wettbewerbsschädliche Verhaltensweise zu untersagen. Insbesondere kann das Bundeskartellamt mit den erweiterten Befugnissen die Bevorzugung eigener Angebote (self-preferencing), das Übertragen der Marktmacht auf bislang nicht beherrschte Märkte, sowie Maßnahmen zur Einschränkung der IOP und Portabilität von Daten untersagen (§ 19a Abs. 2 Nr. 5 GWB).

3.1.2.2 Policy-Reports und geplante rechtliche Implementierungen

Im Zuge der Relevanz von etwaigen IOP-Vorschriften erschienen mehrere Policy-Reports: Crémer et al, 2019; Furman, 2019; Scott-Morton et al., 2019, 2021; Cabral et al., 2021; sowie Bourreau et al. 2022. Diese Policy-Reports stehen neben der aktuellen akademischen Debatte auch im Zusammenhang mit den mittlerweile verabschiedeten rechtlichen Vorschriften im DMA der Europäischen Kommission. Dieser sieht unter anderem verpflichtende Vorschriften zur Bereitstellung von IOP für NI-ICS vor, enthält aber auch Regeln für andere Bereiche, die die aktuell geltende rechtliche Grundlage zum möglichen Einsatz von Verpflichtungen dahingehend verschärfen, dass auch vertikale IOP adressiert wird.

So schreibt Artikel 6(4) vor, dass Gatekeeper - in Bezug auf ihre Kernplattformdienste - "die Installation und tatsächliche Nutzung von Softwareanwendungen oder Softwareanwendungsspeichern Dritter, die Betriebssysteme dieses Gatekeepers verwenden oder mit diesen interoperieren, gestatten und den Zugriff auf diese Softwareanwendungen oder Softwareanwendungsspeicher über andere Mittel als die Kernplattformdienste dieses Gatekeepers ermöglichen sollten. Der Gatekeeper darf nicht daran gehindert werden, verhältnismäßige Maßnahmen zu ergreifen, um sicherzustellen, dass Softwareanwendungen oder Softwarestores Dritter die Integrität der vom Gatekeeper bereitgestellten Hardware oder des Betriebssystems nicht gefährden", während Artikel 6(7) festhält, dass Gatekeeper "*Geschäftsnutzern und Anbietern von Zusatzdiensten den Zugang zu und die Interoperabilität mit demselben Betriebssystem, derselben Hardware oder denselben Softwarefunktionen ermöglichen sollten, die bei der Bereitstellung von Zusatzdiensten durch den Gatekeeper verfügbar sind oder verwendet werden*".

Das Parlament schlug vor, die Verpflichtung in Artikel 6(7) dahingehend zu erweitern, dass "*Anbieter von Diensten und Anbieter von Hardware unentgeltlich Zugang zu und Interoperabilität mit denselben Hardware- und Softwarefunktionen erhalten, auf die über ein Betriebssystem zugegriffen wird oder die über ein Betriebssystem gesteuert werden*, sofern das Betriebssystem gemäß Artikel 3(9) identifiziert wird, das für die vom Gatekeeper bereitgestellten Dienste oder Hardware verfügbar ist. „*Den Anbietern von Zusatzdiensten soll ferner der Zugang zu und die Interoperabilität mit denselben Betriebssystemen, Hardware- oder Softwarefunktionen gestattet werden, unabhängig davon, ob diese Softwarefunktionen Teil eines Betriebssystems sind, wenn diese einem von Gatekeepern bereitgestellten Zusatzdiensten zur Verfügung stehen."* Das Parlament sprach sich auch

für eine Verpflichtung zur IOP für NI-ICS aus, die Eingang in das verabschiedete Gesetz fand und in Kapitel 4 diskutiert wird.

In Bezug auf die Übertragbarkeit sah der mittlerweile verabschiedete Vorschlag (vgl. Artikel 6(9)) vor, dass Gatekeeper-Plattformen "*eine wirksame Übertragbarkeit von Daten, die durch die Tätigkeit eines geschäftlichen Nutzers oder Endnutzers erzeugt wurden, gewährleisten und insbesondere Werkzeuge für Endnutzer bereitstellen, um die Ausübung der Datenübertragbarkeit* im Einklang mit der Verordnung (EU) 2016/679 zu erleichtern, unter anderem durch die Bereitstellung eines kontinuierlichen Echtzeit-Zugriffs." Das Parlament schlug erfolgreich eine weitere Erweiterung vor, wonach die Datenübertragbarkeit kostenlos bereitgestellt werden muss.

Ähnliche Gesetzesvorhaben sind im Vereinigten Königreich zu beobachten, in dem die CMA als Wettbewerbsbehörde erweiterte rechtliche Grundlagen für Plattformen anstrebt. In diesem Kontext werden ebenfalls Vorschriften zur Datenportabilität, IOP und FRAND-Zugang genannt (Batchelor et al., 2021; Belleflamme und Peitz, 2021). Auch der ACCESS Act (“Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021”), welcher am 11.06.2021 im amerikanischen Repräsentantenhaus vorgebracht wurde, hat zum Zweck Wettbewerb, niedrigere Eintrittsbarrieren und reduzierte Wechselkosten zu bewirken. Dies ist unter anderem durch rechtliche Vorschriften zur Portabilität und IOP geplant, womit er sich in die vergleichbaren rechtlichen Vorhaben der Europäischen Kommission und der britischen Regierung einreiht.

3.2 Potenziell erwünschte Effekte von Interoperabilität

Nachdem Kapitel 2.2 zu erwartende Wettbewerbswirkungen verschiedener IOP-Konzepte allgemein dargelegt hat, wird nachfolgend deren Anwendbarkeit auf Märkten der Plattformökonomie untersucht. Die Analyse unterscheidet systematisch zwischen horizontalen und vertikalen IOP-Regelungen und führt konkrete Fallbeispiele vor, in denen IOP-Aktivitäten bereits erfolgt sind oder vielversprechend erscheinen.

3.2.1 Horizontal: Reduzierung von Marktkonzentration und Lock-In Effekten

Horizontale IOP auf digitalen Plattformmärkten hat vor allem die Absicht Interaktion zwischen Nutzern verschiedener Plattformen zu ermöglichen, ohne dass dafür ein Anbieterwechsel oder das Verwenden mehrerer Nutzerkonten (Multi-Homing) nötig ist. In dieser Hinsicht könnten beispielsweise so Nutzer eines sozialen Netzwerks Profilseiten von Nutzern eines konkurrierenden Netzwerks ansehen, Freundschaft-Links herstellen und Inhalte im gegenseitigen Newsfeed platzieren.[12] Durch die IOP solcher Kernfunktionen

12 Generell kann die technische Umsetzung eines solchen Cross-postings gewährleistet werden, da es zwischen einzelnen Netzwerken bereits marktgetrieben vorliegt. So können Instagram (Meta) Inhalte beispielsweise auch auf anderen Apps gepostet werden, auch solchen, die außerhalb des Meta-Ökosystems liegen (Facebook, Twitter, Tumblr, Ameba, VKontakte, OK.ru).

werden firmenspezifische Netzwerkeffekte aufgelöst und zu marktweiten Effekten aggregiert (Scott Morton et al., 2021). Bestehende Netzwerkeffekte unter IOP sind nicht länger firmenspezifisch, sondern wirken wie ein öffentliches Gut und fallen gleichmäßig bei allen Marktteilnehmern an. Die Gefahr von kippenden Märkten zu nur einer dominanten Plattform kann somit ausgeschlossen werden, da nun netzwerkeffekt-auslösende Kernfunktionen allen Marktteilnehmern im gleichen Maße zur Verfügung stehen.

Wettbewerb unter horizontaler IOP findet dann nicht mehr um den Plattformmarkt statt sondern innerhalb des Marktes und zwischen den Plattformen (Bourreau et al., 2022). So können eine Reihe von Ineffizienzen verhindert werden und statische Wohlfahrtsvorteile wie niedrigere Preise oder eine verbesserte Qualität entstehen (Crémer et al., 2019; Furman, 2019). Da Wettbewerb in den interoperablen Kernfunktionen nicht mehr möglich ist, ist zu erwarten, dass Differenzierungen verstärkt in anderen Produktdimensionen vorangetrieben werden. Mögliche Beispiele im Kontext sozialer Netzwerke sind beispielsweise unterschiedliche Businessmodelle (Nutzung gegen Entgelt vs. Nutzung gegen Daten/Aufmerksamkeit), Content Moderation Policies (stärkeres Filtern von Hate-Speech) oder erweiterte Einstellungen zu Privatsphäre und Datenschutz, die über den festgelegten Standard der Kernfunktionen hinausgehen. Das Neutralisieren von anbieterspezifischen Netzwerkeffekten führt dazu, dass die Wahl der Plattform unabhängig der Größe ihrer jeweiligen Nutzerbasis getroffen werden kann und vielmehr auf den inhärenten Präferenzen der Nutzer beruht.

Bei einem potenziellen Anbieterwechsel weg von der dominanten Plattform bestehen für Nutzer somit keine Wechselkosten mehr durch die Reduktion der für sie relevanten Netzwerkgröße (Farrell und Klemperer, 2007). Eine Lock-In Situation von Verbrauchern und eine starke Marktkonzentration kann somit durch horizontale IOP von Kernfunktionen abgeschwächt werden. Hinsichtlich Nicht-Kernfunktionen bestehen dann allerdings weiterhin auch teilweise firmenspezifische Netzwerkeffekte (vgl. Bourreau et al., 2022). Historisch sind auf digitalen Plattformmärkten aber bereits dominante Marktakteure entstanden (Facebook, Apple- und Android-App Store, Google Ads, Amazon Marketplace). Auch wenn IOP Wechselkosten reduziert, ist dennoch mit einem ineffizienten Verharren im Status quo (Status Quo Bias) zu rechnen (Samuelson und Zeckhauser, 1988). Polites und Karahanna (2012) zeigen auf, dass dies insbesondere bei einem Wechsel von einem Incumbent-System oder einer Incumbent-Plattform auf eine neue vorliegt. Ein Wechsel findet daher nur statt, wenn eine alternative Plattform deutlich günstiger ist oder besser den entsprechenden Produktpräferenzen entspricht. Insbesondere vor diesem Hintergrund erscheint es wichtig, dass IOP nur Kernfunktionen betrifft von denen Netzwerkeffekte ausgehen und somit gleichzeitig genügend Spielraum zur Produktdifferenzierung erhält.

Eine wichtige Voraussetzung für die Effektivität horizontaler IOP ist, dass Inhalte auf allen interoperablen Plattformen diskriminierungsfrei behandelt werden müssen. Scott Morton et al. (2021) benennen diesen Aspekt als „equitable“ IOP, also „gleichberechtigt“ in dem Sinne, dass eine Plattform Inhalte von konkurrierenden Plattformen nicht unterschiedlich zu ihren eigenen behandeln darf. Im Kontext sozialer Netzwerke muss die angewendete

Methodik zur Moderation der Inhalte, der Prominenz der Inhaltsplatzierung oder die Art der Inhalts-Monetarisierung somit identisch zur der der eigenen Inhalte sein. Erfolgt die wechselseitige Einbettung von Inhalten zwischen interoperablen Diensten nicht diskriminierungsfrei, besteht die Gefahr, dass hierdurch anbieterspezifische Nachfrageexternalitäten (Netzwerkeffekte) wieder aufgebaut werden. Vergleichbar ist dies zu historischen On-Net und Off-Net Tarifen zwischen Telekommunikationsanbietern. Hier sind die Netzwerke zwar interoperabel (Jeder Nutzer ist von jedem Netzwerk aus erreichbar), jedoch bestehen unterschiedlich hohe Kosten. Laffont et al. (1998) argumentieren, dass hierdurch anbieterspezifische Netzwerkeffekte künstlich hergestellt werden und eine Marktkonzentration zu einem Anbieter verstärkt wird. Diskriminierungsfreiheit bei der Implementierung horizontaler IOP ist somit essenziell zum Erhalt der prokompetitiven Wirkung der Maßnahme. Diskriminierungsfreiheit im Kontext vertikaler IOP ist hingegen eng mit Gefahren zu Foreclosure und Self-Preferencing verknüpft und wird in Kapitel 3.3.3 gesondert thematisiert.

Szenario: Horizontale Interoperabilitätsverpflichtung für Facebook

Das Ziel einer verpflichtenden horizontalen Interoperabilität (IOP) für Facebook oder für soziale Netzwerke generell ist es, plattformspezifische Netzwerkeffekte aufzulösen und diese auf Marktebene zu aggregieren. Die nachfolgenden Umsetzungsvorschläge zur Erreichung dieses Ziels beruhen maßgeblich auf den Arbeiten von Scott Morton und Kades (2021) und Scott Morton et al. (2021).

Kernfunktionen sozialer Netzwerke, die zwischen allen interoperablen Plattformen ermöglicht werden, umfassen das Verknüpfen mit Freunden, Browsen von Profilseiten und das Erstellen und Anzeigen von Inhalten (Posts). Die Darstellungsart von Inhalten fremder Netzwerke sollte stilistisch (Schriftart- und Größe) identisch und diskriminierungsfrei sein zu eigenen Inhalten aber als plattformfremder Inhalt gekennzeichnet werden. So ist es Nutzern möglich Rückschlüsse auf die tatsächliche Nutzerbasis der interoperablen Netzwerke ziehen zu können.

Um die technischen Voraussetzungen für eine solche API zu schaffen, müssen Standards für die Übertragung der einzelnen Datenformate der Kernfunktionen definiert werden. Im Kontext sozialer Netzwerke beinhaltet dies volle Protokoll-IOP von Datenformaten zu Bild-, Video-, Text- und Kalenderinhalten.

Die Berechtigung, dass ein Datenaustausch zwischen zwei Plattformen stattfindet, soll nutzerspezifisch erfolgen. Sobald eine „Freundschaftsanfrage“ gegenseitig bestätigt wurde, werden erstellte Inhalte beider Personen wechselseitig zwischen den Netzwerken übermittelt. Es findet kein ganzheitlicher Austausch von Inhalten der gesamten Nutzerbasis statt. Die Ausgestaltung der APIs soll darüber hinaus nur die Übermittlung von Inhalten sicherstellen. Rückschlüsse über das Nutzungsverhalten von Nutzern auf anderen Netzwerken, sowie Einblicke in Algorithmen und anderer proprietärer Prozesse konkurrierender Netzwerke müssen zum Erhalt von Wettbewerbsinteressen ausgeschlossen werden.

Die Festlegung der Übertragungsstandards sollte über eine SSO (Standard Setting Organisation) mit technischer Expertise erfolgen. Es erscheint sinnvoll neutrale Experten und Anforderungen kleiner Netzwerke priorisiert in diesem Prozess zu berücksichtigen, um eine zu starke Einflussnahme Facebooks zu verhindern. Ebenfalls sollten ex-post Änderungen an APIs von Regulierungsbehörden vor in Kraft treten genehmigt werden müssen, um negativen Wettbewerbseffekten vorzubeugen. Vor diesem Hintergrund erscheint eine Selbstregulierungs-Lösung und APIs unter der Kontrolle von Facebook als fahrlässig, da hier starke Anreize zu einer kontinuierlichen Qualitätsverschlechterung der API bestehen. Diese können beispielsweise durch eine hohe Anpassungsfrequenz, schlechte Dokumentation oder häufige Downtimes seitens Facebook operationalisiert werden.

3.2.2 Vertikal: Stimulierung von Innovationen

Vertikale IOP ermöglicht eine modulare Kombinationsmöglichkeit einer Plattform oder eines Systems mit komplementären Diensten verschiedenster Wertschöpfungsstufen (sog. „Mix and Match“) und vergrößert so mögliche Absatzmärkte vor- und nachgelagerter Anbieter (Matutes und Regibeau, 1988). Innovationsanreize komplementärer Anbieter steigen hierdurch deutlich und neue Geschäftsmodelle werden durch vertikale IOP teilweise erst ermöglicht (Farrell und Simcoe, 2012b). Eine verlässliche IOP-Regelung mit Verpflichtungscharakter schafft zudem zusätzliche Sicherheit, dass kritische Schnittstellen auch in Zukunft zur Verfügung stehen werden (Scott Morton et al., 2021). Einem nachträglichen Abschalten oder einer Qualitätsverschlechterung wichtiger Innovationsschnittstellen kann somit vorgebeugt werden.

Ein Beispiel für die innovationsfördernde Wirkung von offenen Schnittstellen zur vertikalen IOP kann in der marktgetriebenen Bereitstellung von APIs zum IBM Mainframe in den neunziger Jahren gefunden werden. Infolgedessen wurde eine Vielzahl komplementärer Software, teilweise kollaborativ, entwickelt (Porell, 2020). Eine weiteres Positivbeispiel ist der kürzlich eingeführte Open-Banking Standard bzw. API, die es einer Reihe an Fintech

Anbietern ermöglicht auf Bankkonten von britischen Nutzern zuzugreifen und so komplementäre Dienste anzubieten (Open Banking, 2022a).

Um die positiven Innovationswirkungen zu erhalten ist eine behördliche Kontrolle der definierten APIs angeraten, da eine marktgetriebene oder selbstregulatorische Bereitstellung solcher APIs ist aus Sicht einer dominanten Plattform nicht immer anreizkompatibel ist. Vertikale IOP und entstehende komplementäre Dienste fördern zwar den Wert und die Attraktivität der Plattform bzw. des Systems, es ist jedoch für den Plattformbetreiber nur bedingt möglich diese Renten für sich zu extrahieren. Als Konsequenz dessen, ist oft zu beobachten, dass Plattformen zu Beginn zwar vertikal interoperabel sind, dies jedoch zu reduzieren versuchen je etablierter ihre Marktposition wird (Eisenmann et al., 2009). Operationalisiert wird dies beispielsweise durch die Einschränkung entsprechender APIs, der Akquisition von komplementären Anbietern oder der Entwicklung eigener ähnlicher Produkte (sog. „Sherlocking“).

Neben einer nötigen Aufsicht ist ebenfalls zu klären, wie weitreichend vertikale IOP ausgestaltet werden soll. Eine Freigabe aller existierenden privaten APIs ist sicherlich unter dem Gesichtspunkt der Innovationsförderung der Goldstandard, ist praktisch und juristisch jedoch fragwürdig. Die Bereitstellung von eigenen APIs zu einem spezifischen, komplementären Innovations- bzw. Entwicklungsvorhaben ist in dieser Hinsicht sicherlich einfacher zu operationalisieren. Grundsätzlich ist der Zusammenhang zwischen der Offenheit eines Systems und komplementären Innovationen nicht linear (Boudreau, 2010; Boudreau, 2012). Ein zu offener Zugang oder zu einfach umzusetzender IOP-Standard könnte daher eine Flut an komplementären Diensten niedriger Qualität fördern. Ein solches Übermaß verringert eher die Attraktivität der Plattform aus Verbrauchersicht und schafft zu starken Wettbewerbsdruck aus Sicht von komplementären Anbietern mit hochqualitativen Services (Bourreau et al., 2022). Ein gesundes Mittelmaß an vertikaler IOP zur Förderung von Innovationen bzw. komplementären Wettbewerb ist vor diesem Hintergrund ratsam (Aghion et al., 2005).

Ebenfalls ist zu berücksichtigen, dass unter vertikaler IOP Innovationsanreize stark asymmetrisch verteilt sind entlang der Wertschöpfungskette. Die entgeltlose Zugangsgewährung zu einer Plattform im Sinne einer „essential facility“ reduziert, ceteris paribus, natürlicherweise die Anreize zur Bereitstellung und Investition in diese (Krämer und Schnurr, 2014). Im Gegensatz dazu werden Innovationen von vor- und nachgelagerten komplementären Anbietern gefördert oder erst ermöglicht. Diese gegenläufigen Anreize verschiedener Interessensgruppen müssen im Implementierungsprozess vertikaler IOP-Regelungen berücksichtigt werden (Bourreau et al., 2022).

Erwünschte Effekte von Interoperabilität

- **Horizontale IOP** ermöglicht die **Auflösung firmenspezifischer Netzwerkeffekte**, so dass Interaktionen zwischen Nutzern verschiedener Plattformen auch ohne Anbieterwechsel oder das Verwenden mehrerer Nutzerkonten (Multi-Homing) stattfinden können
- Bestehende Netzwerkeffekte wirken dann wie ein öffentliches Gut und fallen gleichmäßig bei allen Marktteilnehmern an, so dass die **Gefahr von kippenden Märkten** zu einer dominanten Plattform **verringert** wird und Wettbewerb nicht mehr *um* den Markt stattfindet, sondern *innerhalb* des Marktes zwischen Plattformen.
- **Vertikale IOP** ermöglicht eine **modulare Kombinationsmöglichkeit** einer Plattform oder eines Systems mit komplementären Diensten unterschiedlicher Wertschöpfungsstufen (sog. „Mix and Match“) und **vergrößert** so mögliche **Absatzmärkte** vor- und nachgelagerter Anbieter

3.3 Potenziell unerwünschte Effekte von Interoperabilität

Die Implementierung von IOP-Regelungen birgt neben vereinzelten Vorteilen auch Risiken, die einerseits fundamental als auch prozedural begründet sind. Nachfolgend wird auf diese nachteiligen Effekte abgestellt, die analog zu Kapitel 3.2 hinsichtlich vertikaler als auch horizontaler IOP differenziert werden.

3.3.1 Horizontal: Substituierung von Multi-Homing und Reduzierung von Wettbewerb um den Markt

In Kapitel 2.2.1.4 wurde bereits der imperfekt substitutive Charakter zwischen Multi-Homing und einer vertikalen IOP-Regelung angesprochen, der an dieser Stelle in Bezug auf Wettbewerbswirkungen auf digitalen Plattformmärkten spezifiziert wird. Durch Multi-Homing ist es Nachfragern ebenso möglich firmenspezifische Netzwerkeffekte verschiedener Anbieter gleichzeitig zu nutzen und dienstspezifische Funktionalitäten voll auszuschöpfen. Multi-Homing fördert dadurch den Wettbewerb innerhalb des Plattformmarktes und verhindert somit das „Kippen“ zu einer dominanten Plattform, ähnlich zur Wirkung von horizontaler IOP.

Ob IOP-Verpflichtungen oder Multi-Homing eher den Wettbewerb fördern und ein Kippen von Märkten verhindern oder die Bestreitbarkeit von digitalen Märkten fördern, ist ex-ante unklar. Sowohl Multi-Homing als auch IOP haben jeweils spezifische Vor- und Nachteile. Ein Nachteil von Multi-Homing ist, dass hierbei im Vergleich zu IOP zusätzliche Kosten

verursacht werden. Diese können beträchtlich sein, z. B. wenn zusätzliche teure Hardware (beispielsweise ein weiteres Smartphone bei Multi-Homing zwischen Betriebssystemen) erworben werden muss. Andererseits können, gerade bei digitalen Diensten, die unmittelbaren Kosten des Multi-Homings auch sehr gering ausfallen (beispielsweise Installieren einer weiteren Applikation auf dem bestehenden Smartphone) und vorrangig nicht-monetärer Natur sein (z. B. Registrierungs-, Lern- und andere Transaktionskosten). Unterstützt wird dies durch ein Ergebnis der repräsentativen Nutzerumfrage der Bundesnetzagentur (2020), in der 73% der Nutzer von Messaging-Diensten angeben, mehrere Dienste parallel zu nutzen. Eine horizontale IOP-Regelung würde den Anreiz hierzu deutlich abschwächen und eine Reihe von Vorteilen durch Multi-Homing de-facto ausschließen (vgl. Bourreau et al., 2022). Wenn hierdurch substanzielle Kosten des Multi-Homings vermieden werden können, kann dies durchaus wohlfahrtsfördernd sein. Oft ist der Trade-off jedoch unklar wie Kroon und Arnold (2018) zeigen. Weiterhin stellen sie den zusätzlichen Verbrauchernutzen durch unterschiedliche Funktionalitäten von verschiedenen Anbietern heraus. Ein spezifischer Nachteil von IOP ist es, dass in der Praxis keine vollständige Kompatibilität hergestellt werden kann. Dies trifft insbesondere für digitale Dienste zu, die einer hohen Innovationsdynamik unterliegen. So verbleibt aus Konsumentensicht eine spürbare Inkompatibilität (z. B. hinsichtlich neuer Funktionalitäten wie selbstlöschende Nachrichten oder Reels und digitaler Inhalte wie etwa bestimmte Emoticons und animierte GIFs), sodass signifikante Netzwerkeffekte verbleiben (s. auch Bourreau et al., 2022). Im Gegensatz dazu besteht dieses Problem bei Multi-Homing nicht, da hier die Konsumenten in jedem Netzwerk mit dem jeweils vollen Funktionsumfang interagieren können.

Beide Alternativen avisieren dennoch das gleiche Ziel, der Schaffung von horizontalem Wettbewerb innerhalb eines Plattformmarktes und somit dem Erhalt von statischer Effizienz. Demgegenüber steht jedoch die Möglichkeit zum Wettbewerb um den Markt, der in der Plattformökonomie typisch ist. Sollte es in einem solchen Szenario zu einem Markteintritt eines innovativen Anbieters kommen, hat dieser es schwerer ausschließlich auf Basis der nicht-interoperablen Funktionalitäten entsprechende Nachfragewirkungen zu erzeugen. In Verbindung mit einem möglichen Status Quo Bias der Nutzer (siehe Kapitel 3.2.1) ist zu erwarten, dass die etablierte Plattform einen Großteil ihrer Nutzer behält.

Aus dieser Abschwächung des Wettbewerbs um den Markt kann zusätzlich eine Gefahr für die dynamische Effizienz des betrachteten Plattformmarktes entstehen. Sollte ein Marktzutritt eines Anbieters erfolgen, der über ein effizienteres Produkt verfügt (z. B. mit mehr Features, einer besseren Technologie oder das kostengünstiger angeboten werden kann) , ist es wohlfahrtsökonomisch wünschenswert, wenn dieser möglichst schnell Marktanteile gewinnt. Unter horizontaler IOP ist das Erreichen einer kritischen Masse jedoch nicht mehr möglich, da firmenspezifische Netzwerkeffekte weitestgehend negiert werden. Ein ökonomisch sinnvolles Ablösen der dann ineffizienten Incumbent-Plattform durch den neuen Anbieter ist in einem solchen Szenario nicht zu erwarten (Bourreau et al., 2022).

Multi-Homing hingegen erhält den Wettbewerbsdruck um den Markt aufrecht, da das Gewinnen einer kritischen Masse an Konsumenten immer noch möglich ist. Weiterhin obliegt in diesem Fall ein vollständiges Ersetzen oder „Kippen“ des Marktes der Konsumentscheidung der Nutzer, da diese jederzeit das Multi-Homing einstellen können. Dies ist dann gegeben, wenn die Vorteile durch den neuen superioren Dienst und mögliche Kosteneinsparungen durch das Unterlassen des Multi-Homings den Nutzenverlust durch eine möglicherweise geringere Netzwerkgröße überwiegen. Multi-Homing führt somit zu „Competition for the Market“, während IOP die Möglichkeit zu „Competition in the Market“ erhält. Ein Schumpeterscher Innovationswettbewerb im Sinne einer schöpferischen Zerstörung (sukzessive Ablösung gekippter Märkte durch neue innovative Markteintritte) ist somit immer noch möglich. IOP verhindert zwar das Kippen von Märkten, schließt aber gleichzeitig das Ablösen ineffizienter Incumbents aus. Multi-Homing erhält somit die generelle Wirksamkeit von anbieterspezifischen Netzwerkeffekten, den Wettbewerb um den Markt und somit die dynamische Effizienz.

Eine Horizontale IOP-Regelung und Multi-Homing stellen im Kontext der Plattformökonomie daher nur imperfekte Substitute dar und implizieren einen Trade-off. Vielversprechende Faktoren, die bei der Abwägung zwischen statischer und dynamischer Markteffizienz berücksichtigt werden sollten, sind einerseits das Vorliegen von Multi-Homing und zu welchen Kosten die parallele Nutzung von Diensten möglich ist. Andererseits auch die Einschätzungen über die Wahrscheinlichkeit und Frequenz von Markteintritten als auch die Disruptivität möglicher Kosten- und Produktinnovationen (Bourreau et al., 2022). Der Analyserahmen in Kapitel 3.7 diskutiert diese entscheidungsrelevanten Faktoren genauer und leitet entsprechende Handlungsempfehlungen ab.

3.3.2 Horizontal & Vertikal: Patent Hold-up und Kollusionsgefahren bei der Festlegung von Standards

Der Prozess zu einer Festlegung eines technischen Standards soll idealerweise die objektiv beste technologische Grundlage standardisieren. In dieser Hinsicht sollen so die aus Verbrauchersicht essenziellen Grundfunktionalitäten von Plattformdiensten horizontal interoperabel gemacht werden bei gleichzeitiger Zukunftssicherheit des Standards. Auf vertikaler Ebene sollen so wichtige Innovationsschnittstellen für vor- und nachgelagerte Anbieter sichergestellt werden. Nichtsdestotrotz bestehen Anreize für Firmen, den Festlegungsprozess zu beeinflussen mit dem Ziel eigene Technologien und Patente in die Standarddefinition zu integrieren. Die spätere Nutzung des Standards erfolgt dann nur unter entsprechenden Lizenzzahlungen an den Eigentümer dieser sog. „Standard-essenziellen Patente“ und sichert durch die verpflichtende Einhaltung des Standards eine konstante Monetarisierung der eigenen Patente zu. Diese Problematik ist der Ökonomie als „Patent Ambush oder Patent Hold-up“ bekannt und führt dazu, dass solche Standards entgegen ihrer eigentlichen Motivation durch ihre hohen Lizenzkosten als Eintrittsbarriere fungieren können (Farrell et al., 2007; Scott Morton et al., 2021).

Grundsätzlich kann das Ausgliedern des Standard-Festlegungsprozesses an neutrale SSOs (Standard Setting Organisations) als ein Selbstverpflichtungsmechanismus („commitment device“) und eine glaubhafte Unternehmensstrategie angesehen werden (Shapiro und Varian, 1998b; Sirbu und Hughes, 1986). Dennoch zeigen jüngere Beispiele in der digitalen Plattformökonomie, dass SSOs in der Praxis anfällig sind für die Interessen dominanten Anbieter. Beispielsweise ist Google im World Wide Web Consortium (W3C) als SSO deutlich überrepräsentiert und ist in der Lage, eigene Interessen bei Standarddefinitionen bevorzugt zu etablieren (Claburn, 2020). Ähnlich hierzu stellt der Majority Staff Report and Recommendations und Subcommittee on Antitrust (2020) des US Repräsentantenhauses zum Wettbewerb auf digitalen Märkten fest, dass eigentlich neutrale SSOs oft von Google zu Vertriebsorganen für eigene Funktionen oder bereits getroffene Business-Entscheidungen reduziert werden. Vor diesem Hintergrund erscheint es sinnvoll, dass nicht nur die nachträgliche Einhaltung eines IOP-Standards von öffentlicher Seite überwacht wird, sondern bereits auch der Festlegungsprozess.

Hinsichtlich des Festlegungsprozess eines IOP-Standards hat Kapitel 2.2.1.6.2 bereits erläutert, dass mengenvariable Zahlungen zu vermeiden sind. Darüber hinaus bestehen jedoch zusätzliche Gefahren für horizontale Kollusion, die die positiven Effekte des Standards konterkarieren. Zunächst findet im Zuge des Prozesses zwangläufig eine Kommunikation zwischen horizontal konkurrierenden Unternehmen statt, die einen Austausch über möglicherweise anfallende Lizenzzahlungen einschließen. Zur Bestimmung solcher „FRAND“-Zahlungen werden Informationen geteilt, die Auskunft über die jeweiligen Kostenstrukturen der Unternehmen geben. Sidak (2009) weist darauf hin, dass solche Informationen ein konzertiertes Preissetzungsverhalten auf nachgelagerten, standardrelevanten Endkundenmärkten deutlich vereinfachen. Neben diesem möglichen Kanal zu expliziten Absprachen besteht zusätzlich die Gefahr von impliziter Kollusion durch die Wechselseitigkeit möglicher Lizenzzahlungen. Beinhaltet ein Standard essenzielle Patente von mehreren horizontal konkurrierenden Unternehmen, sind gegenseitige Zahlungen für die Nutzung unbedingt zu vermeiden. Ökonomisch betrachtet würden hierdurch die Gewinne der jeweiligen Unternehmen miteinander verknüpft, da größere Profite der Konkurrenten anteilig durch erhaltene Lizenzzahlungen in das eigene Betriebsergebnis einfließen. In einem solchen Fall internalisieren die Unternehmen die Auswirkungen des eigenen Verhaltens auf die Konkurrenz, was zwangsläufig zu einem geringeren Wettbewerbsdruck führt (Shapiro, 2001). Infolgedessen ist insbesondere die Wechselseitigkeit solcher Zahlungen auf horizontaler Ebene zu vermeiden.

3.3.3 Vertikal: Foreclosure-Abwägungen durch vertikal integrierte Plattformen und „Multi market contact“

Kapitel 2.2.1 hat bereits dargelegt, dass Anreize zur Bereitstellung von vertikaler IOP unterschiedlich ausgeprägt sind zwischen zugangssuchenden und zugangsgewährenden Unternehmen. Die Anreizdynamik wird hingegen zunehmend komplexer, wenn ein oder mehrere involvierte Plattformunternehmen vertikal integriert sind und auf mehreren

Wirtschaftsstufen miteinander konkurrieren (van Wegberg, 2004). So weisen Bourreau et al. (2022) darauf hin, dass für eine zugangsgewährende Plattform die Möglichkeit zur strategischen Diskriminierung des zugangssuchenden komplementären Anbieters auf vorgelagerter Stufe besteht. Ziel dessen ist die Erzielung klarer Wettbewerbsvorteile auf nachgelagerten Märkten. Operationalisiert wird dies beispielsweise über kostentreibende Maßnahmen zur Erzielung eines sog. „margin squeeze“ (Bostoen, 2018), Sabotage oder Qualitätsverschlechterungen der APIs oder deren Dokumentationen (Mandy, 2000; Mandy & Sappington, 2007) oder andere Formen von Selbst-Bevorzugung (Padilla et al., 2020). Im Extremfall können diese Praktiken zu einem völligen Verdrängen, sog. „Foreclosure“, von nachgelagerten Anbietern führen, da diese nicht mehr kostendeckend operieren können. Bourreau et al. (2022) führen als Beispiel hierfür den Wettbewerbsfall gegenüber Microsoft an, nachdem das Unternehmen den Zugang zu vertikalen IOP-Schnittstellen nach seinem Markteintritt im Bereich Workgroup-Server deutlich erschwert bzw. gänzlich eingestellt hatte. Per Gerichtsurteil wurde dem Unternehmen nachträglich das Wiederherstellen dieser Schnittstellen auferlegt (Kerber und Schweitzer, 2017).

Vor dem Hintergrund von vertikal integrierten Unternehmen, kann vertikale IOP daher als ein zweischneidiges Schwert betrachtet werden. Einerseits ermöglicht es Wettbewerb von komplementären Produkten auf vor- bzw. nachgelagerten Wirtschaftsstufen, es bietet jedoch andererseits, wenn gänzlich marktgetrieben, einen Kanal zu antikompetitivem und missbräuchlichem Verhalten des zugangsgewährenden Unternehmens. Andererseits kann das gleichzeitige Vorliegen von freiwillig bereitgestellten vertikalen Interoperabilitäten und vertikalen Verflechtungen einer Gatekeeper-Plattform oder konkurrierender Unternehmen einen Bedarf anzeigen, entsprechende IOP-Schnittstellen exogen zu standardisieren und deren Einhaltung, wenn möglich, zu überwachen (ähnlich zur Zugangsregulierung auf Telekommunikationsmärkten). Nichtsdestotrotz sollte das alleinige Vorliegen dieses Sachverhalts keine IOP-Maßnahme zur Verhinderung von Foreclosure-Aktivitäten rechtfertigen, da Grenzen zwischen Wirtschaftsstufen in der digitalen Plattformökonomie zunehmend unscharf sind und somit Wettbewerbseffekte von potenzieller horizontaler wie vertikaler IOP ineinanderfließen (Krämer und Schnurr, 2021). Unter Berücksichtigung des effektiven Urteils zum obigen Wettbewerbsfall um Microsoft, halten beispielsweise auch Bourreau et al. (2022) einen ex-post Ansatz zur Wahrung von fairer vertikaler IOP bei komplexen vertikalen Verflechtungen als vielversprechend.

3.3.4 Horizontal: Geringerer Spielraum zur Produktdifferenzierung

Die Umsetzung von horizontaler IOP impliziert, dass eine Reihe von Kernfunktionen definiert wird, die interoperabel standardisiert werden und Nutzern aller Plattformdienste zur Verfügung stehen. Wettbewerbliche Differenzierungsmöglichkeit bestehen daher nur in nicht-standardisierten Funktionen. Scott Morton et al. (2021) argumentieren, dass insbesondere solche Funktionen standardisiert und interoperabel sein sollten, die einerseits besonders von Konsumenten wertgeschätzt werden, und andererseits kritisch sind, um

bestehende firmenspezifische Netzwerkeffekte aufzulösen. Folgt die Definition von standardisierten Kernfunktionen sinnvollerweise dieser Argumentation, verbleiben jedoch gleichzeitig nur weniger attraktive Produktdimensionen über die Differenzierung und Wettbewerb stattfinden kann. Bourreau et al. (2022) weisen darauf hin, dass hierdurch eine starke Homogenisierung horizontal konkurrierender Dienste erfolgt mit negativen Auswirkungen auf die Produktvielfalt und Konsumentennutzen (siehe auch Kapitel 2.2.1.5).

Die Besorgnis über zu geringe Möglichkeiten zur Produktdifferenzierung wird ebenfalls von der Monopolkommission (2021) in ihrem 12. Sektorgutachten zum Telekommunikationsmarkt als ein Hauptargument gegen eine verbindliche horizontale IOP-Verpflichtung im Markt für Messaging- und Videodienste geteilt und auf die Gefahr hingewiesen, dass eine zu starke Homogenisierung durch horizontale IOP dazu führen könnte, dass Kunden sogar weniger geneigt sein könnten, zwischen verschiedenen Anbietern zu wechseln (vgl. auch Kapitel 3.3.1).

3.3.5 Horizontal: Reduzierte Anreize für Innovation

Implikationen für Innovationsanreize unter horizontaler IOP wirken entlang des gleichen Wirkungskanals von einer reduzierten Möglichkeit zur Produktdifferenzierung. Durch die Definition von interoperablen Kernfunktionen wird der derzeitige Technologiestand, durch die Standardisierung „zementiert“ (Bundeskartellamt, 2021). Innovationen werden somit in Produktdimensionen gelenkt, die nicht zu den standardisierten Kernfunktionen zählen. Bei digitalen Plattformdiensten können dies beispielsweise Designaspekte sein, eine einfachere Handhabung, erweiterte Funktionen zur Kommunikation (Video, Dateitransfer) oder eine stärkere Verschlüsselung und Privacy-Einstellungen. Wenn diese nicht-interoperablen Funktionen jedoch im Vergleich zu Kernfunktionen nur eine geringe Wertschätzung erfahren und von ihnen keine gesteigerten Nachfrageeffekte ausgehen, dann sind entsprechende Innovationsvorhaben nur wenig attraktiv (Scott Morton et al., 2021).

Sollten dennoch Innovationen außerhalb interoperabler Kernfunktionen für Nutzer attraktiv sein und folglich bedeutende Nachfragewirkungen induzieren, könnten sie zunehmend als de-facto essenzielle Funktionalitäten angesehen werden, obwohl sie nicht in der Definition des Standards enthalten sind. Die festgelegten Kernfunktionen im Rahmen eines IOP-Standards hinken somit der eigentlichen Verbraucherwahrnehmung strukturell hinterher. Erfolgreiche Innovationen schwächen somit die Wirkungsweise von interoperablen Kernfunktionen auf horizontaler Ebene ab und konstituieren einen klassischen Zielkonflikt (Bourreau et al., 2022). Eine zügige Eingliederung von erfolgreichen Produktinnovationen einzelner Anbieter in den IOP-Standard, würde diese Funktionalitäten zwar auch anderen Anbietern zusprechen und IOP wieder herstellen, gleichzeitig aber wichtige Innovationsrenten entwerten. Unter Gesichtspunkten von dynamischer Effizienz ist horizontale IOP somit kaum zu rechtfertigen.

3.3.6 Horizontal & Vertikal: Umsetzungskosten von Standards für kleinere Firmen

Die Implementierung von IOP über Standards erfordert die Konsultation bereits aktiver Anbieter von Plattformdiensten. Dies stellt gleichzeitig jedoch ein strukturelles Problem dar, da Anliegen von noch nicht existierenden potenziellen neuen Marktteilnehmern im Standard-Festlegungsprozess unterrepräsentiert sind. Bereits existierende Anbieter haben so grundsätzlich die Möglichkeit einen entsprechenden Standard so zu beeinflussen, dass er für kleine innovative Unternehmen schwer umzusetzen ist. Die technische Komplexität der standardisierten Technologie, mögliche Lizenzzahlungen oder auch eine zu große Anzahl an interoperablen Kernfunktionen, denen neue Dienste genügen müssen, können die Kosten für eventuelle Markteintritte erhöhen. Verpflichtende IOP-Standards können somit als strategische Marktzutrittsschranke zweckentfremdet werden und eine alternative „Escape-Entry“ Strategie im Sinne von Aghion et al. (2009) für bereits etablierte Anbieter darstellen. Erste Indizien für diese Gefahr sind in der Befragung von 44 Anbietern von Messaging- und Videodiensten des Bundeskartellamt (2021) zu finden. Hier wird angemahnt, dass „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, S. 93). Im Festlegungsprozess des Standards ist somit zu bewerten, wie realistisch Markteintritte sind, um somit das Aufbauen von Marktzutrittsschranken zu vermeiden.

3.3.7 Horizontal & Vertikal: Datenschutzrisiken für Verbraucher

Aus datenschutzrechtlicher Sicht ist die Implementierung von IOP-Regeln in der Plattformökonomie und bei Messaging-Diensten ambivalent. Einerseits könnten IOP-Verpflichtungen Markteintrittsbarrieren für Anbieter verringern, die einen besonderen Wert auf den Schutz der Privatsphäre ihrer Nutzer liegen (VZBV, 2021, S. 24). Dies könnte sich positiv auf das Datenschutzniveau im Gesamtmarkt auswirken. Andererseits ergeben sich mit der Implementierung einer IOP-Verpflichtung auch neue Datenschutzrisiken für Verbraucher, da sowohl horizontale als auch vertikale IOP einen wechselseitigen Austausch von Daten zwischen verschiedenen Anbietern voraussetzt.

Aus datenschutzrechtlicher Perspektive ist die Übermittlung von Daten im Horizontal- oder Vertikalverhältnis als Datenverarbeitung im Sinne von Art. 4 Abs. 2 DSGVO (Datenschutz-Grundverordnung) zu qualifizieren. Sie muss daher den Anforderungen an die Rechtmäßigkeit der Verarbeitung nach Art. 6 Abs. 1 DSGVO entsprechen (Becker et al., 2021, S. 126). Soweit kein anderer Erlaubnistatbestand eingreift, ist für die Herstellung der IOP somit grundsätzlich eine Einwilligung des Nutzers nach Art. 6 Abs. 1 lit. a DSGVO erforderlich.

Besondere Datenschutzrisiken können sich z. B. bei einer horizontalen IOP von Messaging-Diensten ergeben, sofern für die Übermittlung von Nachrichten zwischen unterschiedlichen Anbietern eine Aufhebung der Verschlüsselung erforderlich ist. Selbst wenn eine Ende-zu-Ende Verschlüsselung (vgl. Kapitel 4.2.4) sichergestellt ist, fallen bei der Übermittlung von Nachrichten Metadaten an (Angaben zu Absender und Empfänger der Information, Zeitpunkt der Kommunikation, Standort der Nutzer etc.). In einem interoperablen Netzwerk haben auch Anbieter Zugriff auf diese Metadaten, zu denen der Nutzer in keiner direkten Geschäftsbeziehung steht. Damit entzieht sich in einem föderierten System der Umfang der Datenverarbeitung durch Dritte der unmittelbaren Kontrolle durch die Nutzer (Bundesnetzagentur, 2021). Mit Blick auf den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSVO) sollte sich die Verarbeitung von Metadaten daher auf den für die Herstellung der IOP zwingend notwendigen Umfang beschränken (Cyphers und Doctorow, 2021).

Bei der Beurteilung möglicher Datenschutzrisiken ist allerdings auch zu berücksichtigen, dass sich IOP im Vergleich zum Multi-Homing als die datenschutzfreundlichere Alternative erweisen könnte. Je nach Ausgestaltung der IOP-Verpflichtung könnte sich dieses Szenario daher im Ergebnis als datenschutzfreundlicher erweisen, als wenn die Nutzer eine Vielzahl von Messenger-Apps auf ihren Endgeräten installieren, um mit ihren Kontakten zu kommunizieren (VZBV, 2021, S. 27).

Unerwünschte Effekte von Interoperabilität

Horizontal

- Horizontale IOP kann die **Anreize zum Multi-Homing** und damit Wettbewerb um den Markt und **disruptive Innovationen einschränken**, da die Exploration und Nutzung von alternativen Diensten weniger nötig wird
- Eine zu starke Homogenisierung **reduziert Differenzierungsmöglichkeiten** für Firmen im Wettbewerb. Dies kann zu einer reduzierten Produktvielfalt und weniger Anbieterwechseln sowie Multi-Homing führen.
- Eine **(fehlerhafte) Definition von Kernfunktionen oder Standards** kann bestehende Technologien zementieren, Innovationsanreize in weniger relevante Produktdimensionen lenken (oder das Ziel der Auflösung von firmenspezifischen Netzwerkeffekten verfehlen)

Vertikal

- IOP kann **strategisch eingeschränkt** und diskriminierend genutzt werden, um Wettbewerber auf nachgelagerten Märkten zu schädigen. (Dominante) Plattformen bzw. Anbieter können verstärkt interoperable Produkte oder Funktionen externer Firmen kopieren und in ihr eigenes Angebot integrieren (**„Sherlocking“**)

Horizontal & Vertikal

- Standardisierungsprozesse können **Kollusionsgefahren** und **“Patent Hold-up"** bewirken, wenn (markt-)mächtige Firmen durch Einflussnahme eigene Technologien und Patente gegen Lizenzzahlungen in Standarddefinition einbringen können
- **Implementierungskosten** von interoperablen Standards und Schnittstellen können gerade für kleine Firmen eine zusätzliche **Markteintrittshürde** darstellen
- Unter IOP haben Anbieter, zu denen die Nutzer in keiner direkten Geschäftsbeziehung stehen, ggf. **Zugriff auf (Meta-)Daten**, Damit entstehen **Datenschutzrisiken**, da sich der Umfang der Datenverarbeitung durch Dritte der unmittelbaren Kontrolle durch die Nutzer entziehen kann

3.4 Interoperabilität und digitale Souveränität

3.4.1 Dimensionen der digitalen Souveränität

In den letzten Jahren hat sich die "strategische Autonomie" als Trend unter den politischen Entscheidungsträgern in den großen globalen Wirtschaftsblöcken herauskristallisiert. Die COVID-19-Krise hat diese Entwicklung verstärkt, so dass die Länder ihre Widerstandsfähigkeit und Abhängigkeit von ausländischen Anbietern kritischer Dienstleistungen und Produkte, insbesondere aus Ländern außerhalb ihrer jeweiligen Wirtschaftsblöcke, zunehmend überprüfen. In Bezug auf wichtige IKT-Infrastrukturen wird diese strategische Autonomie oft als "digitale Souveränität" bezeichnet.

Kroon et al. (2020) haben die Ansätze zur digitalen Souveränität in Europa und im Vereinigten Königreich verglichen und festgestellt, dass die politischen Entscheidungsträger der digitalen Souveränität unterschiedliche Aufgaben und Ziele zuschreiben und unterschiedliche Begriffe verwenden, z. B. Technologiesouveränität oder strategische Autonomie. Trotz dieser unterschiedlichen Definitionen konnten die folgenden gemeinsamen Dimensionen identifiziert werden: 1) (privater) Datenschutz, 2) Cybersicherheit und 3) strategische Interessen (Kroon et al., 2020).

1. Bei der Dimension des **Schutzes der Privatsphäre** geht es um die Souveränität des Einzelnen, der sein digitales Leben und seine persönlichen Daten kontrollieren kann. Die Themen reichen hier von der Möglichkeit, die gesammelten persönlichen Informationen von Plattformen zu extrahieren, über Transparenz und Kontrolle über den Ort, an dem Ihre persönlichen Daten gespeichert werden, bis hin zur Verschlüsselung persönlicher Unterhaltungen.
2. Bei der Dimension **Cybersicherheit** geht es um die Souveränität der Länder und der EU in Bezug auf die Cybersicherheit und die Widerstandsfähigkeit der digitalen Infrastruktur. Diese Dimension war die Erste, die in Europa anerkannt und umgesetzt wurde (Kroon et al., 2020). Die laufende Debatte über den Ausschluss bestimmter Lieferanten für Europas neue Mobilfunknetze aufgrund von Sicherheitsrisiken ist dieser Dimension zuzuordnen.
3. Die **strategische Dimension** betrifft die (Wieder-)Erlangung wirtschaftlicher Kontrolle und Führung im digitalen Bereich. Dies geschieht durch Investitionen auf EU-Ebene in Schlüsseltechnologien wie künstliche Intelligenz, Robotik, Chipproduktion und Hochleistungscomputer, die für die künftige wirtschaftliche Entwicklung von entscheidender Bedeutung sind, aber auch unsere europäischen Werte beeinträchtigen könnten, da große Nicht-EU-Konzerne in bestimmten digitalen Bereichen eine beherrschende Stellung einnehmen (z. B. aus China und den USA).

Wenngleich wettbewerbliche Aspekte für die Beurteilung der IOP überwiegen, ist digitale Souveränität bei der Bewertung zu berücksichtigen. Der für den Binnenmarkt zuständige

Kommissar Thierry Breton stellte fest, digitale Souveränität sei "… not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent." (Breton, 2019) ([Digitale Souveränität] ist kein protektionistisches Konzept, es geht einfach darum, europäische technologische Alternativen in wichtigen technischen Geschäftsfeldern zu haben, bei denen wir derzeit abhängig sind).

Kroon et al. (2020) betonten, dass die meisten Maßnahmen zur digitalen Souveränität in Europa darauf abzielen, ein Gleichgewicht zwischen dem Erreichen der eigenen Autonomie und der Aufrechterhaltung eines diversifizierten Portfolios von Anbietern und internationalen Handelsbeziehungen zu finden, die für viele EU-Volkswirtschaften wichtig sind.

In den folgenden Abschnitten werden wir untersuchen, wie sich IOP auf die verschiedenen Dimensionen der digitalen Souveränität auswirken könnten.

3.4.2 Auswirkungen von Interoperabilität auf die Dimension persönlicher Daten

Bei der Dimension des Schutzes der Privatsphäre geht es um die Souveränität des Einzelnen, die Gestaltung seines digitalen Lebens zu bestimmen und damit auch die Weitergabe persönlicher Daten kontrollieren zu können. Vertikale IOP, die den Funktionsumfang bestimmter Plattformen um zusätzliche Funktionen und/oder Anwendungen wie Zahlungsmöglichkeiten erweitert, würde in der Weitergabe bestimmter Nutzerdaten resultieren, um die Funktion der ergänzenden Anwendungen zu ermöglichen (vgl. auch Kapitel 3.3.7). Darüber hinaus werden durch die Einbindung etwaiger Tracker bzw. Anzeigen oder Einbindungen wie Kartendienste als vertikale Zusatzdienste häufig nicht aktiv kommunizierte Daten an die bereitstellenden Unternehmen gesendet. Ein Aspekt der im Rahmen der DSGVO für Webseiten angegangen wurde.

Die Umsetzung einer horizontalen IOP setzt ebenfalls voraus, dass bestimmte Nutzerdaten ausgetauscht werden, damit beispielsweise eine Identifizierung des Nutzers ermöglicht wird. Gegenwärtig haben sich die Verbraucher aus verschiedenen Gründen für bestimmte Dienste entschieden, sei es aufgrund ihrer Funktionalität oder ihrer Beliebtheit (die meisten Bekannten sind Nutzer dieses Dienstes), während eine höhere Sicherheit, ein besserer Datenschutz oder, im Kontext von sozialen Netzwerken, eine differenzierte Art der Inhalte ausschlaggebend für die Wahl des Dienstes ist. Diese Aspekte von Verbraucherinteressen, die sich in der horizontalen Differenzierung der Dienste abbilden, sind unter Souveränitätsaspekten bei der Ausgestaltung von IOP zu berücksichtigen.

Der differenzierte Umgang mit Datenschutz und Sicherheitsaspekten ist über die Produktdifferenzierung hinaus auch für die Ausgestaltung von IOP relevant. So könnte horizontale IOP die Sicherheitsstandards von Diensten senken, da es schwierig ist, zwei unterschiedliche Verschlüsselungstechnologien und unterschiedliche Sicherheitsansätze

vollständig und ohne Kompromisse in Einklang zu bringen.[13] Daher kann ein Kompromiss auf niedrigeren Sicherheitsstufen nicht ausgeschlossen werden. Ferner ist im Kontext von IOP die nachträgliche Implementierung von Schnittstellen, sei es zur Realisierung horizontaler IOP zwischen sozialen Netzwerken oder vertikal im Zuge von Content Moderation, denkbar. Eine nachträgliche Öffnung von Diensten, die möglicherweise nicht für diesen Zweck konzipiert wurden, können zu zusätzlichen Sicherheitsrisiken führen und möglicherweise den Missbrauch dieser Schnittstellen begünstigen. In diesem Kontext ist die missbräuchliche Verwendung einer Facebook-API seitens Cambridge Analytica, eines britischen Beratungsunternehmens, zu nennen. Cambridge Analytica nutzte eine für akademische Zwecke programmierte Anwendung mit Zugang zur Facebook API und griff dabei nicht nur auf die Daten von Testteilnehmern, die einwilligten, sondern auch auf die Daten derer Facebook-„Freunde“ zu. Während die Nutzungsbedingungen nur eine Sammlung von Daten der Einwilligenden vorsah und eine kommerzielle Weiterverwertung ausschloss, war es Cambridge Analytica dennoch möglich mit der Einwilligung von mehreren hunderttausend Nutzern Daten für über 50 Mio. Nutzer vom sozialen Netzwerk zu erheben. (Cadwalladr und Graham-Harrison, 2018) In Kapitel 4.2 werden diese Bedenken hinsichtlich Messaging-Diensten eingeordnet und die technischen Aspekte analysiert.

3.4.3 Auswirkungen von Interoperabilität auf Cybersicherheit

Die Cybersicherheit im Kontext der nationalen Souveränität konzentrierte sich auf die Verhinderung von Cyberangriffen auf wichtige nationale Infrastrukturen. Dies hat aufgrund der fortschreitenden Digitalisierung und insbesondere während der COVID-Krise an Bedeutung gewonnen. Das zunehmende geopolitische Machtspiel zwischen den USA, China und Europa hat die nationale und europäische Cybersicherheit noch stärker in den Fokus gerückt.

IOP-Vorschriften könnten z. B. auch die Sicherheitsstandards von Messaging-Diensten senken. Dieser Aspekt wird in Kapitel 4 dieser Studie ausführlich beschrieben und diskutiert. Allerdings beziehen sich diese Sicherheitsbedenken jedoch eher auf die persönliche Ebene und nicht auf die nationale und europäische Sicherheitsebene, die im Allgemeinen bei der Überprüfung der Cybersicherheitsdimension der digitalen Souveränität berücksichtigt wird. Es könnte aber einige Aspekte geben, die eher auf nationaler und europäischer Ebene liegen: Wenn in der EU aktive Messaging-Dienste ihre Daten in Nicht-EU-Clouds speichern oder wenn IOP zwischen in der EU und außerhalb der EU aktiven Messaging-Plattformen implementiert wird. WhatsApp-Daten werden beispielsweise in US-amerikanischen Cloud-Diensten gespeichert, so dass sie unter das US-Cloud-Gesetz[14]

13 Hierunter können die Speicherung der Kommunikation auf Servern, das Senden von Daten in die Cloud oder nur auf Servern im jeweiligen Land und das Erfordernis einer persönlichen Identifizierung für das Abonnement fallen.

14 Nach dem US Cloud Act unterliegen Daten, die in den USA oder von amerikanischen Unternehmen gespeichert werden, dem US-Recht, unabhängig davon wo sich die Daten befinden. Siehe (US Kongress, 2018).

fallen, während andere Nicht-EU-Messaging-Dienste wie WeChat weitreichenden Abhörmaßnahmen durch die nationalen Sicherheitsbehörden im eigenen Land unterliegen könnten bzw. am physischen Ort der Server, an dem ein Teil der aggregierten EU-Nutzerdaten gespeichert werden würde. Aber auch hier betrifft dieser Aspekt vornehmlich den Schutz personenbezogener Daten.

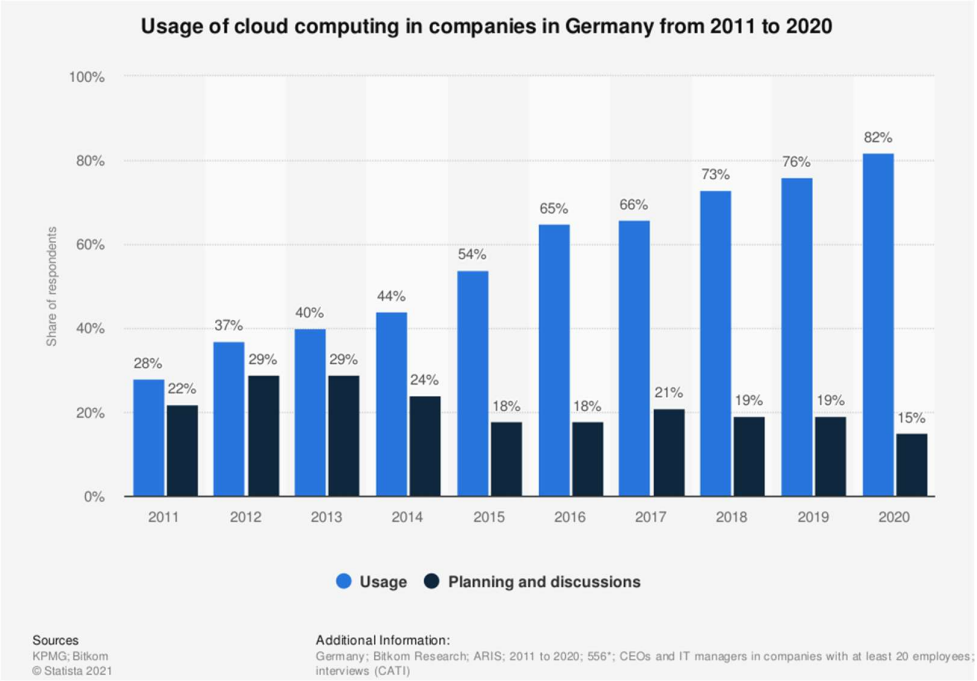
3.4.3.1 Zunehmende Bedeutung von robusten Cloud-Infrastrukturen

Für die EU wichtige Kommunikationsdienste, aber auch Plattformen benutzen häufig Cloud basierte Infrastrukturen, die sich physisch innerhalb und außenhalb den EU befinden. Zusätzlich spielen oft die gleichen Cloud-Dienste eine immer wichtigere Rolle für Geschäftskunden, aber auch für staatliche Stellen und können deshalb auf nationaler und europäischer Ebene als kritische Infrastruktur betrachtet werden. Diese Cloud-Dienste können infrastruktur-, plattform- oder dienstbezogen sein (IaaS, PaaS, SaaS).[15] Neben diesen Kategorien von Cloud-Diensten gibt es auch die Möglichkeit, eine Cloud unter eigener Kontrolle zu betreiben (private Cloud) oder öffentliche Cloud-Dienste von z. B. AWS oder eine Mischung (hybride Cloud) zu nutzen.

Die folgenden Zahlen zeigen die zunehmende Bedeutung von Cloud-Diensten in Deutschland und Europa. Die Ausfallsicherheit dieser Infrastruktur wird damit zu einem Aspekt der digitalen Souveränität.

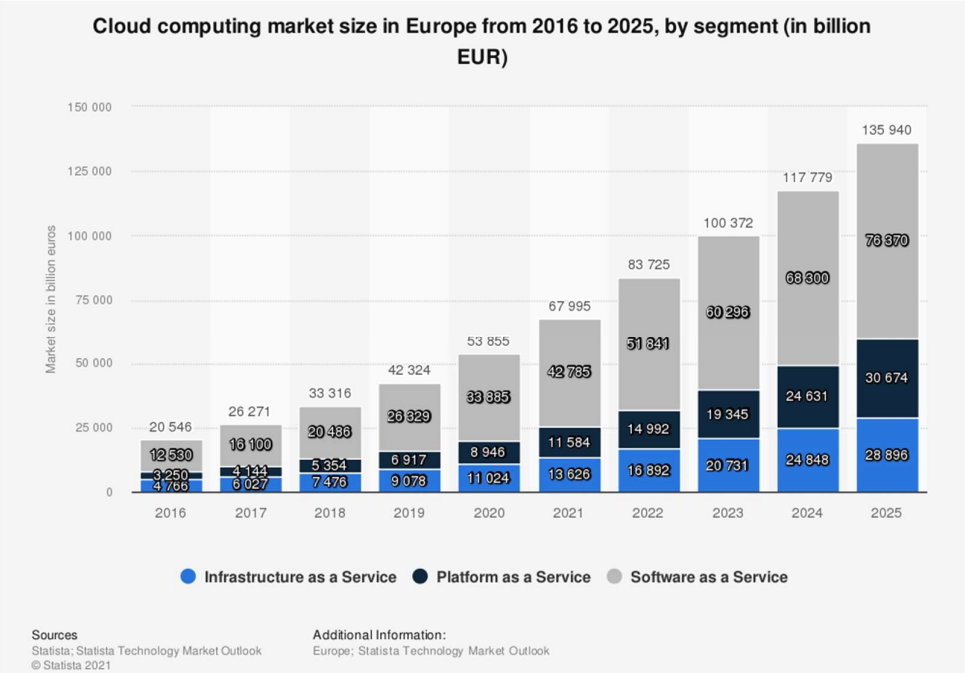
15 Bezeichnet als Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS).

Abbildung 3-2: Nutzung von Cloud-Computing deutscher Unternehmen von 2011 bis 2020



Quelle: Statista (2021)

Abbildung 3-3: Umsatz von Clouddiensten nach Produktart von 2016 bis 2026 (Prognose)



Quelle: Statista (2022)

3.4.3.2 Interoperabilität als Gewährleistung für ein Multi-Cloud-Setup

Im Hinblick auf die Ausfallsicherheit hat es sich bei kritischen digitalen Infrastrukturen schon immer bewährt, sich nicht auf einen einzigen Anbieter zu verlassen (d. h. ein Backup zu haben), weshalb viele Unternehmen eine so genannte Multi-Cloud-Konfiguration bevorzugen. Diese Anforderung wird von der Branche berücksichtigt, so dass die führenden Marktteilnehmer wie AWS, MS, IBM und Google (horizontale) IOP zwischen Multi-Cloud-IaaS-Umgebungen anbieten. Hier scheinen mehrere zusammenhängende Faktoren eine Rolle zu spielen: von der Kundenpräferenz für eine Multi-Cloud-Konfiguration über das Vorhandensein vieler Standards für IaaS bis hin zum kommerziellen Interesse der Anbieter, diese Integration anzubieten, um die Marktakzeptanz von IaaS sicherzustellen.

Lewis (2013) beschrieb bereits in ihrer frühen Forschung zu IOP für Cloud-Dienste, wie horizontale IOP für IaaS-Cloud-Dienste funktioniert, und identifizierte vier typische IOP-Anwendungsfälle für Cloud-Computing wie Workload- und Datenmigration, Benutzerauthentifizierung und Workload-Management. Darüber hinaus stellte sie fest, dass sich die Standardisierungsbemühungen hauptsächlich auf diese grundlegenden Anwendungsfälle im IaaS-Segment konzentrieren (Lewis, 2013).

Ungeklärt bleiben jedoch die Auswirkungen einer weiteren Konsolidierung des IaaS-Cloud-Marktes mit den PaaS- und SaaS-Märkten. Das Multi-Cloud-Konzept für den IaaS-Markt scheint zumindest eine vollständige Dominanz der in den USA ansässigen IaaS-Cloud-Dienste zu verhindern und sich daher positiv auf die digitale Souveränität auszuwirken. Hierbei muss man bemerken, dass der Cloud-Markt sehr differenziert ist und sich noch immer sehr dynamisch entwickelt. Daher könnte (horizontale) IOP keine allgemeine Lösung sein, sondern nur in Bezug auf bestimmte definierte und standardisierte Anwendungsfälle ein künftiges Instrument sein.

Ein damit zusammenhängender strategischer Aspekt der digitalen Souveränität besteht darin, dass europäische IaaS-Cloud-Anbieter durch die Gewährleistung eines Multi-Cloud-Konzepts für Kunden zumindest die Chance haben, ihre Position gegenüber den hauptsächlich in den USA ansässigen Marktführern zu behaupten. In diesem Zusammenhang ist auch der Vorschlag für den europäischen Data Act zu sehen, in dem eine neue Generation von EU-Cloud-Diensten vorgeschlagen wird, die die höchsten Standards für Datenübertragbarkeit und IOP erfüllen sollen.[16]

Das Multi-Cloud-Setup kann sich jedoch auch negativ auf die Widerstandsfähigkeit der digitalen Infrastruktur auswirken. Ein Artikel von TechRepublic aus dem Jahr 2019 ergab, dass eine Multi-Cloud-Umgebung die Sicherheitsrisiken verdoppelt; 52 % der Multi-Cloud-Umgebungen wurden im Jahr 2019 angegriffen, verglichen mit 24 % der Unternehmen, die eine Hybrid-Cloud oder Single-Cloud nutzten (Sanders, 2019). Darüber hinaus stellte auch Nominet (2019) fest, dass Multi-Cloud-Umgebungen häufiger von Sicherheitsverletzungen betroffen sind: 69 % dieser Organisationen berichten von 11 bis 30 Sicherheitsverletzungen, im Gegensatz zu 19 % der Single-Cloud-Organisationen und 13 % der Hybrid-Cloud-Nutzer.

3.4.4 Auswirkungen von Interoperabilität auf strategische Aspekte

Wie bereits erwähnt, fokussieren die strategischen Aspekte der digitalen Souveränität auf der (Wieder-)Erlangung wirtschaftlicher Kontrolle und Führung im digitalen Bereich. Dies reicht von Initiativen in den Bereichen KI, Hochleistungsrechnen bis hin zur Herstellung von Chips und Cloud-Standardisierungs- bzw. Vereinheitlichungsbemühungen wie GAIA-X sowie der Kontrolle über "EU-Daten".[17]

Ein praktisches Problem ist die sehr starke Marktposition von nicht in der EU ansässigen Unternehmen wie Cloud-Anbietern, Messaging-Diensten, Soziale Netzwerke und E-Commerce-Plattformen mit Sitz in den USA, aber auch von Hard- und Softwareherstellern aus Asien.

---

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.

17 Hiermit sind Daten gemeint, die von europäischen Unternehmen stammen und/oder von europäischen Verbrauchern gewonnen werden.

Im Bereich der Informations- und Kommunikationstechnik (IKT) gibt es mehrere Normungsgremien, von denen die bekanntesten das ETSI (European Telecommunications Standards Institute), die ITU (International Telecommunication Union), die GSMA (Groupe Speciale Mobile Association) und das 3GPP (3rd Generation Partnership Project) für Telekommunikationsdienste sind. Für Internet-Standards ist des Weiteren die IETF (Internet Engineering Task Force) und für Standards im World Wide Web das W3C zuständig. IKT-Firmen sind Mitglieder dieser Gremien und wirken an den Normungsprozessen mit, die auf Vereinbarungen zwischen den Mitgliedern der Gremien beruhen. Darüber hinaus haben Anbieter von Hard- und Software in der Vergangenheit Allianzen gebildet, um bestimmte Technologiestandards auf den Markt zu bringen, mit dem Ziel diese als De-facto-Standard zu etablieren.

Im Allgemeinen liefern die Mitglieder von Normungsgremien Beiträge zu geplanten Standards und stellen Vertreter für Arbeitsgruppen oder so genannte Task Forces bereit, die die vorgeschlagenen Standards im Detail diskutieren. Diese Expertengruppen erstatten dann ihren Mitgliedern und dem Vorstand des Normungsgremiums Bericht. In dedizierten Sitzungen werden Konsensentscheidungen zu den vorgeschlagenen Normen getroffen.[18] Dieser Prozess kann einige Zeit in Anspruch nehmen und folglich beträchtliche zeitliche und personelle Ressourcen der Mitglieder binden. Dies bedeutet, dass etablierte größere Unternehmen mit mehr finanziellen Mitteln es sich leisten können, sich länger und intensiver an diesen Normungsprozessen zu beteiligen als beispielsweise Start-ups. Daher ist es wahrscheinlicher, dass Standards in diesen Prozessen so ausgestaltet werden, dass es den größeren Marktteilnehmern entgegenkommt.

Viele Segmente des IKT-Marktes sind bereits sehr konzentriert (z. B. Messaging-Dienste, Sozialen-Medien-Plattformen, aber auch Software oder Cloud-Infrastruktur), und insbesondere US-amerikanische Unternehmen haben eine dominante Stellung. Unter diesen Aspekten der digitalen Souveränität kann der Einsatz von IOP-Vorschriften in Erwägung gezogen werden, um europäische Wettbewerber in die Lage zu versetzen, ihre Marktposition gegenüber diesen marktbeherrschenden Unternehmen auszubauen oder zu behaupten. Um IOP für IKT im Allgemeinen zu ermöglichen, braucht man jedoch bestimmte Standards, um syntaktische und semantische Kompatibilität sicherzustellen, wodurch Funktionen und Daten zwischen Anwendungen und/oder Plattformen integrierbar und/oder verknüpfbar werden. Wie oben beschrieben, sind gerade die großen Marktteilnehmer in der Lage, den Normungsprozess entweder zu verzögern oder in eine ihrerseits präferierte Richtung zu lenken, die für kleinere EU-Unternehmen jedoch nicht von Vorteil sein muss. Deshalb ist eine Aufsicht und/oder ein geregelter Prozess für Standardisierungsvorhaben erforderlich. So kann gewährleistet werden, dass Standards in einem angemessenen Zeitrahmen vereinbart und die Interessen der Mitglieder unabhängig von der Marktgröße und der „investierten Kosten“ angemessen vertreten werden.

18 Siehe zum Beispiel ETSI (2022) und IETF (2022).

Im Zusammenhang mit der Standardisierung ist auch GAIA-X erwähnenswert, da es darauf abzielt, eine europäische standardisierte Dateninfrastruktur zu schaffen, die dem europäischen Recht entspricht, die Datenübertragbarkeit, die höchsten Kriterien der Datensicherheit, Transparenz über die Datenverwendung und die geltenden Vorschriften der EU-Mitgliedstaaten widerspiegelt und Innovationen fördert. Die Standardisierung spielt in diesem Ökosystem eine wichtige Rolle, da bestehende Infrastrukturen der GAIA-X-Mitglieder interoperabel miteinander verbunden und über eine gemeinsame Benutzeroberfläche zugänglich gemacht werden und einheitlichen Open-Source-Standards und Benutzerregeln unterworfen werden sollen.[19]

Für europäische Cloud-Anbieter bietet GAIA-X die Möglichkeit, virtuelle Skalierung innerhalb eines offenen Ökosystems und die Skalierbarkeit von Diensten anzubieten, ein Aspekt der bisher einen großen Wettbewerbsvorteil der (hauptsächlich US-) Hyperscaler darstellte.

Wirkung von Interoperabilität auf Digitale Souveränität

Auswirkung von IOP auf den Schutz der Privatsphäre

- Vertikale IOP birgt die Gefahr der Intransparenz über die Weitergabe und Speicherung von Daten über Unternehmensgrenzen hinweg.
- Horizontale IOP für Messaging-Dienste könnte die Sicherheitsstandards und das Datenschutzniveau von Messaging-Diensten senken. In der Praxis kann ein ähnliches Nutzenniveau durch Multi-Homing seitens der Nutzer erreicht werden.

Auswirkung von IOP auf Cybersicherheit

- Aufgrund der zunehmenden Bedeutung von Cloud-Diensten wird die Ausfallsicherheit dieser Infrastruktur zu einem Aspekt der digitalen Souveränität, dem durch ein Multi-Cloud-Setup entgegengewirkt werden kann.
- Aus einer Vielzahl von Gründen bietet die Industrie selbst (horizontale) IOP zwischen Multi-Cloud IaaS-Umgebungen an. Dies ist sowohl für die Ausfallsicherheit als auch für die Marktposition der europäischen IaaS-Cloud-Anbieter gegenüber den, hauptsächlich in den USA ansässigen, Marktführern von Bedeutung.

Auswirkung von IOP auf strategische Aspekte

- Es besteht ein Interessenkonflikt, da marktbeherrschende Parteien eine Lenkungsfunktion in Standardisierungsprozessen haben können, die für IOP erforderlich sind. Daher sollte eine objektive Aufsicht über diese Prozesse stattfinden, um Verzögerungen zu vermeiden und sicherzustellen, dass die

19 Siehe https://www.data-infrastructure.eu/GAIAX/

Interessen aller Branchenmitglieder unabhängig von der Marktgröße vertreten werden.
- Horizontale IOP könnte theoretisch dazu beitragen, die Marktkonzentration bei Messaging-Diensten zu verringern. Untersuchungen zeigen jedoch, dass die Verbraucher in Deutschland trotz Netzwerkeffekten im Durchschnitt knapp vier Dienste gleichzeitig nutzen. Dies ist auf Produktdifferenzierung, Innovationen, geringe Kosten von Multi-Homing und einen heterogenen Kreis von Kontakten zurückzuführen, was darauf hindeutet, dass IOP nicht erforderlich ist.

3.5 Interoperabilitätsverpflichtungen als Lösungsansatz

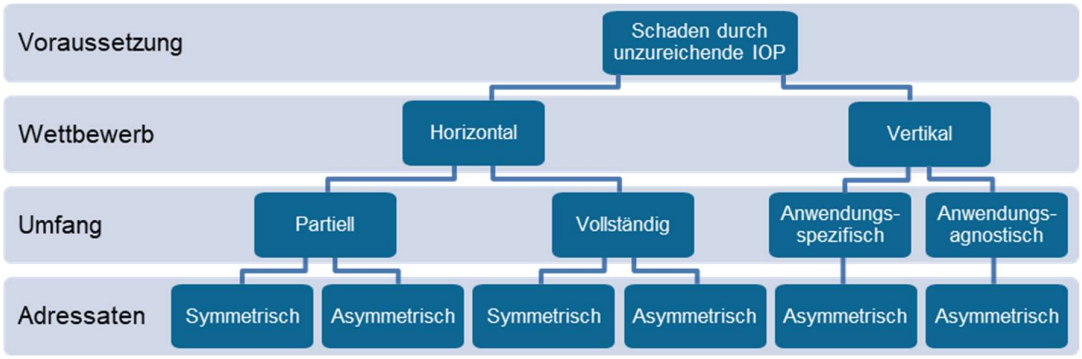
In diesem Kapitel soll aufgeschlüsselt werden unter welchen Bedingungen der potenzielle Schaden durch mangelnde IOP mit Hilfe von spezifischen IOP-Vorschriften adressiert werden kann. Daher wird im Folgenden ein Analyserahmen vorgestellt, welcher es erlaubt IOP-Vorschriften anhand verschiedener Dimensionen granular und fallspezifisch zu analysieren.

Dieses Vorgehen hat den Vorteil, dass die spezifischen positiven Effekte und Risiken von potenziellen IOP-Vorschriften anhand der vorherrschenden Marktbedingungen und moderierenden Faktoren differenziert betrachtet werden können und mit Hilfe des Analyseschemas IOP im Kontext beliebiger Dienste evaluiert werden kann. Mit Hilfe des folgenden allgemeinen Analyseschemas kann daher eine erste Einschätzung zu IOP-Vorschriften bei beliebigen Dienstekategorien auf digitalen Märkten vorgenommen werden.

3.5.1 Analyseschema

Die Übersicht in Abbildung 3-4 verdeutlicht zunächst den allgemeinen Ablauf einer Analyse zu möglichen IOP-Verpflichtungen. Dazu muss zunächst als Voraussetzung ein Schaden durch unzureichende IOP und damit ein Marktversagen festgestellt werden, welcher einen regulatorischen Eingriff in Form einer IOP-Verpflichtung rechtfertigt bzw. eine notwendige Umsetzung europäischer Rechtsvorschriften, denen eine entsprechende Bewertung bereits zugrunde liegt.

Abbildung 3-4: Grafische Darstellung des Analyseschemas



Quelle: WIK-Consult

Anschließend ist der Wettbewerbskontext in einer spezifischen Dienstkategorie zu bewerten. Handelt es sich um vornehmlich gleichartige Dienste auf derselben Wertschöpfungsstufe handelt es sich um einen Fall horizontaler IOP. Befindet sich der Zugang auf eine spezifische Stufe in der Wertschöpfungskette durch vor- oder nachgelagerte Dienste im Kern der Problematik handelt sich um einen Fall vertikaler IOP.

Wenn nach der bis hier erfolgten Beurteilung die Vorteile von IOP unter den vorherrschenden Marktbedingungen und moderierenden Faktoren die Einführung einer IOP-Verpflichtung rechtfertigen, ist im Weiteren über die Ausgestaltung einer solchen Verpflichtung zu entscheiden.

Dies betrifft zunächst den Umfang der IOP-Verpflichtung im Hinblick auf den Grad der abgedeckten Funktionalitäten und Anwendungsszenarien, sowie den Adressatenkreis der von der Regulierung betroffenen Unternehmen. Wie bereits im DMA vorgesehen können Verpflichtungen auch asymmetrisch auferlegt werden und daher nur Unternehmen ab einer bestimmten Größe oder Nutzerzahl einschließen.

3.5.1.1 Wettbewerbsbeziehungen und Interoperabilitätsvorschriften

Nach der Feststellung von unzureichender IOP bzw. bei Notwendigkeit, europäische Vorgaben in nationales Recht umzusetzen, müssen die Vor- und Nachteile einer IOP-Verpflichtung im Kontext des Wettbewerbsumfelds evaluiert werden. Tabelle 3-1 fasst dazu systematisch die moderierenden Marktbedingungen, sowie die positiven und negativen Effekte übersichtlich zusammen. In der Spalte Bewertung findet sich eine erste generelle Einschätzung zu IOP-Verpflichtungen unter den entsprechenden Wettbewerbsverhältnissen.

Tabelle 3-1: Wettbewerbsbeziehungen und IOP-Vorschriften

	Ursache	Moderierende Bedingungen	Positive Effekte von IOP	Risiken von IOP	Bewertung
Horizontal	**Marktkonzentration** durch firmenspezifische (datengetriebene) Netzwerkeffekte	• Verfügbarkeit freiwilliger IOP • Verhinderung „adversarialer IOP“ • Kosten von Multi-Homing • Level von Multi-Homing • Wahrscheinlichkeit innovativer Markteintritte • Innovationsdynamik • Bestehendes Level von Datenschutz / Privacy / Security • Technische Komplexität des Dienstes	• Reduzierung von Marktkonzentration (firmenspezifische Netzwerkeffekte) • Innovationsanreize für nicht interoperable Features u. Qualität • Vorteil für kleine Unternehmen (zum Nachteil für größere Unternehmen) • Reduzierung von Lock-In Effekten	• Geringerer Spielraum für Produktdifferenzierung • Reduzierte Anreize für Innovation bei interoperablen Features (Entrant) • Patent Hold-up und Kollusionsgefahren bei der Standardisierung • Hemmung des Wettbewerbs um den Markt • Reduzierter Datenschutz / Privacy / Security • Reduzierter Anreiz für Multi-Homing (Abh. der Entrants von IOP Standards) • Umsetzungskosten	Risiken überwiegen falls • Kosten von Multi-Homing gering • Level von Multi-Homing hoch • Marktinteresse gering, z. B. angezeigt durch geringe Bemühungen bzw. Verhinderungsversuche zu „adversarialer“ IOP
Vertikal	**Fehlende Innovationsschnittstellen** verhindern Zugang zu Wertschöpfungsstufen	• Verfügbarkeit freiwilliger IOP • Verhinderung „adversarialer IOP“ • Vertikale Integration von Ökosystemen • Wahrscheinlichkeit innovativer Markteintritte • Innovationsdynamik • Bestehendes Level von Datenschutz / Privacy / Security • Technische Komplexität des Dienstes	• Stimulierung von Innovationen (Planungssicherheit) • Reduzierte Marktzutrittsbarrieren und erhöhter Wettbewerb für komplementäre Dienste • Reduzierung von Lock-In Effekten	• Patent Hold-up und Kollusionsgefahren (bei multi-market contact) bei der Standardisierung • Geringere Innovationsanreize bei Zugangsgeber • Doppelte Marginalisierung (über mehrere Wertschöpfungsstufen) • „Sherlocking“[20] • Reduzierter Datenschutz / Privacy / Security • Umsetzungskosten (Standardisierung) • Regulatorische Kosten (Implementierung, Monitoring, Compliance, Redress)	Vorteile überwiegen falls • Vertikale Integration hoch (Ökosysteme) • Geringe Verfügbarkeit freiwilliger IOP

Quelle: WIK-Consult

20 "Sherlocking" bedeutet, dass der Betreiber einer/s Plattform/Dienstes/Betriebssystems Funktionen adaptiert und integriert, welche die Installation eines existierenden (beliebten) Drittanbieter-Tools überflüssig machen. Die Wortschöpfung geht auf den ersten prominenten Fall der Mac-Software „Watson“ zurück, welche Informationen aus dem Internet in einer nativen Suchoberfläche in Mac OS als Komplement zur Apples eigener Suchoberfläche „Sherlock“ anbot. Die Applikation Watson war sehr beliebt, bis Apple mit Mac OS X 10.2 die Version Sherlock 3 veröffentlichte. In dieser Version replizierte Apple fast alle Features der Watson-Software und machte Watson damit faktisch aus Anwendersicht obsolet.

3.5.1.2 Umfang und Adressaten von Interoperabilitätsvorschriften

In Tabelle 3-2 fassen wir die Erkenntnisse zum Umfang möglicher IOP-Vorschriften zusammen. Wie bereits dargelegt ist IOP in verschiedenen Dimensionen (z. B. Funktionsumfang, Zeit etc.) als Kontinuum anzusehen. An dieser Stelle wird daher der Trade-Off zwischen partieller und vollständiger IOP im Fall horizontalen Wettbewerbs, bzw. anwendungsspezifischer und anwendungsagnostischer IOP im Fall vertikalen Wettbewerbs diskutiert. Im ersteren Fall steht im Vordergrund, dass Schnittstellen zwischen verschiedenen Wertschöpfungsstufen für spezifische Anwendungsfälle entwickelt werden. Diese können in einem gewissen Umfang auch „zweckentfremdet" verwendet werden, stoßen dabei aber auch an ihre Grenzen, da nicht alle wünschenswerten Funktionalitäten für bisher nicht bedachte Einsatzzwecke abgebildet sind. Damit benötigt anwendungsagnostische IOP erheblich allgemeinere und damit umfangreichere Schnittstellen, um auch neue Anwendungsszenarien abbilden zu können.

Tabelle 3-2: Umfang von IOP-Vorschriften

	Umfang	Moderierende Bedingungen	Positive Effekte von IOP	Risiken von IOP	Bewertung
Horizontal	Partiell	• Geschwindigkeit der Standardisierung • Technische Komplexität des Dienstes	• Höherer Spielraum für Produktdifferenzierung u. Innovationen	• Kann IOP-Vorschriften unwirksam machen • Schwierigkeit der Ermittlung und Dynamik von relevanten Kernfunktionen	Bei Trennbarkeit von nachfragerelevanten Kernfunktionen und anderen Zusatzfunktionen für Nischen.
	Vollständig	• Geschwindigkeit der Standardisierung • Technische Komplexität des Dienstes	• Ausgeglichenes Wettbewerbsumfeld	• Kein Spielraum für Produktdifferenzierung/Innovationen (nur im Markt / nicht um den Markt) • Umsetzungskosten	Falls Trennbarkeit von nachfragerelevanten Kernfunktionen und anderen Zusatzfunktionen für Nischen nicht ausreichend möglich.
Vertikal	Anwendungsspezifisch	• Verfügbarkeit offener APIs • Bestehende Anwendungsszenarien in vertikal integrierten Ökosystemen	• Wettbewerb mit vertikal integrierten Diensten möglich • Innovation innerhalb bestehender Anwendungskategorien • Neue Kompositionen bestehender Anwendungen	• Komplexe Zugangspreisbestimmung • Umsetzungskosten • Disintermediation von Matchmakern	Falls • Wettbewerb (Preise) in vor- und nachgelagerten Wertschöpfungsstufen gering (hoch) • Umsetzungskosten bzw. Komplexität hoch.
	Anwendungsagnostisch	• Bestehen privater APIs ohne öffentliche Freigabe • Eingeschränkter Zugriff auf Hardwareschnittstellen	Zusätzlich: • Innovation durch neue Anwendungskategorien	• Komplexe Zugangspreisbestimmung • Umsetzungskosten	Falls • Innovation in vor- und nachgelagerten Wertschöpfungsstufen gering • Umsetzungskosten bzw. Komplexität moderat.

Quelle: WIK-Consult

In Tabelle 3-3 wird der Geltungsbereich bzw. Adressatenkreis einer IOP-Verpflichtung im Verhältnis zu den Wettbewerbsverhältnissen verdeutlicht. Hier ist zunächst festzuhalten,

dass im Fall von vertikalem Wettbewerb keine symmetrische IOP möglich ist, da hier der Zugang zu einem essenziellen Teil der Wertschöpfung unter Kontrolle eines Unternehmens im Vordergrund steht. Im Fall horizontaler Wettbewerbsverhältnisse ist zu klären, ob die IOP-Verpflichtung nur für bestimmte Unternehmen gelten soll, welche eine starke Marktposition innehaben (z. B. Finanzkraft, Anzahl Nutzer etc.), oder gleichermaßen für alle Anbieter eines bestimmten Diensttyps (z. B. Messenger).

Tabelle 3-3: Adressaten von IOP-Vorschriften

	Horizontal	Vertikal
Asymmetrisch (Betroffen ab Grenzwert z. B. für Unternehmensgröße, Anzahl aktiver Nutzer, Umsatz etc.)	Wettbewerbsvorteil für kleinere Unternehmen.	Zugang für Drittanbieter zu Kerndiensten möglich.
Symmetrisch (Betrifft alle Unternehmen einer Dienstekategorie gleichermaßen.)	Ausgeglichenes Wettbewerbsumfeld für kleine u. große Unternehmen.	Nicht möglich

Quelle: WIK-Consult

3.5.2 Analyseparameter für die spezifische Fallanalyse

Bei der Evaluierung bestimmter Dienstekategorien oder der Position einzelner Unternehmen in der Wertschöpfungskette sollten darüber hinaus weitere Faktoren berücksichtigt werden. Je nach Sektor, Marktstruktur und Wettbewerbsumfeld können verschiedene Parameter die Beurteilung beeinflussen, z. B. inwiefern insbesondere multifunktional ausgestaltete und/oder zu vertikal integrierten Ökosystemen zugehörige Dienste (ggf. sogar gleichzeitig) in horizontalem oder vertikalem Wettbewerb stehen. Weitere Faktoren werden im Folgenden näher erläutert.

3.5.2.1 Bestehende Interoperabilität und Standards

Zunächst sollte in diesem Zusammenhang evaluiert werden welche Formen von IOP bereits möglich sind bzw. in einem marktwirtschaftlichen Umfeld freiwillig angeboten werden und ob diese auch genutzt werden. Ebenso sollte geprüft werden, ob eine gezielte Verhinderung bzw. künstliche Erschwerung von IOP (adversarial) beobachtet werden kann. Auch die Nutzung bestehender (kommerzieller) Angebote kann durch unverhältnismäßige Nutzungsbedingungen oder Preise gezielt eingeschränkt werden.

Ebenso relevant erscheint die Verfügbarkeit von Standards in einer bestimmten Dienstekategorie oder für bestimmte Anwendungen. IOP kann von Unternehmen ebenfalls durch die gezielte Implementierung von (oder dem Beharren auf) proprietären Technologien trotz der Verfügbarkeit von adäquaten standardisierten Alternativen verhindert werden.

In diesem Zusammenhang sollte ebenfalls geprüft werden, ob Unternehmen in der Vergangenheit bereits IOP angeboten haben und diese beispielsweise erst bei eigenem Vorstoß in angrenzende Geschäftsfelder gestoppt wurde.

3.5.2.2 Geschäftsmodelle und Daten

Geschäftsmodelle in mehrseitigen Märkten basieren häufig auf dem Matchmaking bzw. der Zusammenführung von Transaktionspartnern, also dem Zusammenbringen von zwei (oder mehreren) Marktseiten durch eine Plattform. Dies ist beispielsweise der Fall bei AppStores (Endnutzer/Entwickler), online Werbung (Endnutzer/Werbetreibende) und mobilen Zahlungsdienstleistungen (Käufer/Verkäufer). Verpflichtende vertikale IOP kann daher solche Geschäftsmodelle durch „Disintermediation“ bedrohen. Der Begriff beschreibt einen Bedeutungsverlust von Intermediären durch den Wegfall der Kontrolle über einzelne essenzielle Wertschöpfungsstufen.

Darüber hinaus besteht ein fundamentaler Unterschied in der Monetarisierung zwischen werbefinanzierten und bezahlten Diensten. Während datengetriebene Netzwerkeffekte einen direkten Einfluss auf die Monetarisierung von werbefinanzierten Diensten haben, ist dies bei bezahlten Diensten nur mittelbar durch Qualitätsverbesserungen der Fall. IOP und der Zugriff auf Daten in Echtzeit kann daher einen unterschiedlichen Effekt auf Dienste dieser Kategorien haben.

Beispielsweise führt ein „within-user“ optimierter Algorithmus zu einer Verstärkung des persönlichen Lock-ins. Dieser Lock-In lässt sich aber verhältnismäßig einfach durch einen einmaligen Portabilitätsprozess auflösen. Im Gegensatz dazu ist das Ergebnis eines „across-user“ optimierenden Algorithmus (z. B. Empfehlungen auf Basis von Trendanalysen aller Nutzer) nicht ohne Weiteres durch Datenportabilität übertragbar. Allerdings kann auch IOP einen solchen Datennetzwerkeffekt nicht direkt transferieren, aber unter Umständen eine stärkere Nutzung alternativer Dienste induzieren (Wechsel und /oder Multi-Homing) und damit diese datengetriebenen Netzwerkeffekte indirekt übertragen.

3.5.2.3 Switching und Multi-Homing

Je nach Marktgegebenheiten und -situation können sich Switching und Multi-Homing in ihrer Wirkung gegenseitig substituieren, dies ist aber nicht generell der Fall.

Switching ermöglicht dabei im weiteren Sinne auch das Ausüben von Multi-Homing. Im engeren Sinne bezeichnet Switching den Wechsel von Anbietern im Fall von Single-Homing, also das Wechseln auf einen anderen, vergleichbaren Dienst, wobei der ursprüngliche Dienst nicht weiter genutzt wird. Daher ist ein niedriges Niveau von Multi-Homing nicht per se problematisch, insbesondere dann nicht, wenn ein Wechsel des Anbieters einfach möglich ist. Daher ist eine zentrale Frage in der Evaluation spezifischer Dienste oder Wertschöpfungsstufen ob ein Anbieterwechsel und Multi-Homing überhaupt

praktisch möglich sind und welche Kosten beim Wechsel bzw. der Mehrfachnutzung faktisch anfallen.

(Daten-)IOP kann dennoch auch im Fall von bestehendem Multi-Homing, also der fortwährenden parallelen Nutzung mehrerer Dienste, dabei helfen, Datenstände wie Adressbücher oder Playlisten synchron und aktuell zu halten. Bei reinem Switching hingegen würde ein einmaliges, einseitiges Portieren der Daten ausreichen.

Darüber hinaus ist das tatsächlich beobachtete Niveau von Multi-Homing relevant, da es zeigt, ob Kunden von dieser Option, fehlende IOP zu umgehen praktisch auch Gebrauch machen. Hohe Kosten können beispielsweise ein niedriges Niveau von Multi-Homing erklären, sind aber dafür nicht hinreichend (z. B. wenn die Kosten fehlender IOP sehr hoch sind). Diese Kosten können von Anbietern auch direkt und indirekt gesteuert werden, beispielsweise durch das Design der Benutzeroberfläche oder die Vertragsgestaltung.

3.6 Technische Voraussetzungen für verschiedene Interoperabilitätslösungen

Im Kontext digitaler Plattformen ist bezüglich der technischen Voraussetzungen von IOP hervorzuheben, dass die zu betrachteten digitalen Plattformen auf modularen Komponenten basieren, die zur Erfüllung einer Funktion zusammenwirken. Tiwana et al. (2010) definieren softwarebasierte Plattformen wie Betriebssysteme als umfangreiche Basis von Softwarecode, deren Grundfunktionalität durch interoperable Module erweitert wird, welche auf Schnittstellen zurückgreifen. Insbesondere Betriebssysteme basieren hierbei auf einer umfangreichen Funktionserweiterung durch Module. Tiwana und Konsynski (2010) bezeichnen dies als Prozess der Aufweichung monolithischer Architekturen hin zu Modularität. De Reuver et al. (2018) sehen im Kontext mobiler Betriebssysteme die Applikationen, welche gegenüber dem Endnutzer Funktionalitäten bereitstellen, als eine Vereinigung verschiedener Layer von modularen Ressourcen an. Diese modularen Ressourcen sind Funktionen des Betriebssystems, Hardware, Software Development Kits und Funktionen von Programmschnittstellen (APIs). Damit neue Apps programmiert werden können, müssen diese jedoch eine syntaktische und semantische IOP zu den Funktionen und Schnittstellen herstellen. Neben dieser Austauschfähigkeit und Kompatibilität bedarf es ebenfalls einer detaillierten Dokumentation, welche die Nutzbarkeit sicherstellt. Inwiefern eine digitale Plattform diese bereitstellt und in welchem Umfang, wird in der Literatur mit der „Offenheit“ von digitalen Plattformen charakterisiert. Diese Offenheit einer Plattform steht mit der Governance-Struktur einer Plattform in Verbindung und erfordert gemäß Benlian et al. (2015) eine sorgfältige Abwägung von Kontrolle und Autonomie von Komplementärdiensten. Tabelle 3-4 zeigt die von Benlian et al. vorgeschlagenen Kriterien zur Einordnung des Offenheitsgrades digitaler Plattformen. Obwohl sich diese Kategorisierung insbesondere auf mobile Betriebssysteme bezieht, lässt sich das Konzept der Offenheit auch auf weitere Plattformen und damit andere vertikale Beziehungen übertragen.

Tabelle 3-4: Indikatoren des Offenheitsgrades von digitalen Plattformen

	Transparenz	Zugänglichkeit
Technische Ebene	• Die Plattform bietet Funktionen, die es Entwicklern ermöglichen, mit anderen Entwicklern zu kommunizieren und sich auszutauschen *(Austausch zwischen Entwicklern)* • Die Dokumentation der technischen Plattform enthält alle relevanten Informationen für die Entwicklung von Anwendungen *(technische Dokumentation)* • Die Plattform bietet die Möglichkeit, sofortige technische Unterstützung vom Plattformanbieter zu erhalten *(technische Unterstützung durch den Anbieter)*	• Es ist einfach, sich mit den technischen Standards der Plattform vertraut zu machen (*Erlernbarkeit der technischen Standards*) • Die Plattform bietet hilfreiche Tools, die die Entwicklung von Anwendungen erleichtern (*Verfügbarkeit von Entwicklungstools*) • Die Plattform unterstützt die technische IOP (*d. h. die Kompatibilität*) mit anderen Systemen oder Plattformen (*technische IOP*) • Der Funktionsumfang, der den Entwicklern (über APIs) zur Verfügung gestellt wird, ist begrenzt (*Funktionsumfang*) • Die technische Leistungsfähigkeit der Plattform schränkt das Funktionieren von Anwendungen ein (*technische Leistungsfähigkeit*) • Die anfänglichen Kosten für die technischen Anforderungen (*z. B. jährliche Gebühren für die Entwickler-Community, Hardwareanforderungen*) schränken den Zugang zur Plattform ein (*Kosten für die erforderliche technische Ausrüstung*)
Vertriebsweg	• Der Plattformanbieter kommuniziert offen die Prüfungs- und Vermarktungsrichtlinien (*Kommunikation über App-Prüfungs- und Vermarktungsrichtlinien*) • Die Bedingungen des Marktplatzes der Plattform (d. h. für die Bewerbung und den Verkauf von Apps) sind transparent (*Transparenz der Bedingungen*) • Die Mitteilungspraxis des Plattformanbieters (z. B. über geplante Änderungen der Geschäftsbedingungen) ist transparent (*Mitteilungspraxis*) • Die Such-, Filter- und Ranking-Mechanismen von Anwendungen (d. h. die Auffindbarkeit von Anwendungen) auf dem Marktplatz sind für Entwickler klar (*Transparenz der Marktmechanismen*) • Der Plattformmarktplatz ermöglicht und unterstützt die Kommunikation zwischen Anwendungsentwicklern und Endnutzern (*Kommunikation mit Endnutzern*)	• Die Kosten für den Verkauf von Anwendungen auf dem Marktplatz der Plattform (*z. B. an den Plattformanbieter gezahlte Umsatzbeteiligung, Gebühren für das Abrechnungssystem usw.*) schränken die Entwickler beim Vertrieb ihrer Anwendungen ein (*Verkaufskosten*) • Die Geschäftsbedingungen des Marktplatzes (*z. B. Auszahlungspläne und Schwellenwerte*) schränken die Entwickler in ihren Verkaufsaktivitäten ein (*Vertriebsbeschränkungen in den Geschäftsbedingungen*) • Die Richtlinien für die Anwendungsprüfung und das Marketing schränken die Entwickler bei der Verbreitung ihrer Anwendungen ein (*Einschränkungen durch die Richtlinien für die Anwendungsprüfung und das Marketing*)

Quelle: Benlian et al. (2015, S. 10) – Übersetzung WIK-Consult

Digitale Plattformen unterliegen dabei nach De Reuver et al. (2018) dem Paradox des Wandels, einem Zielkonflikt zwischen Stabilität und Beständigkeit des Systems bei gleichzeitiger Anpassung an dynamische Prozesse des Wachstums und der Funktionserweiterung. Im Beispiel mobiler Betriebssysteme werden dafür Software Development Kits (SDKs) als umfangreiche Frameworks zur Verfügung gestellt, die Drittanbietern ei-

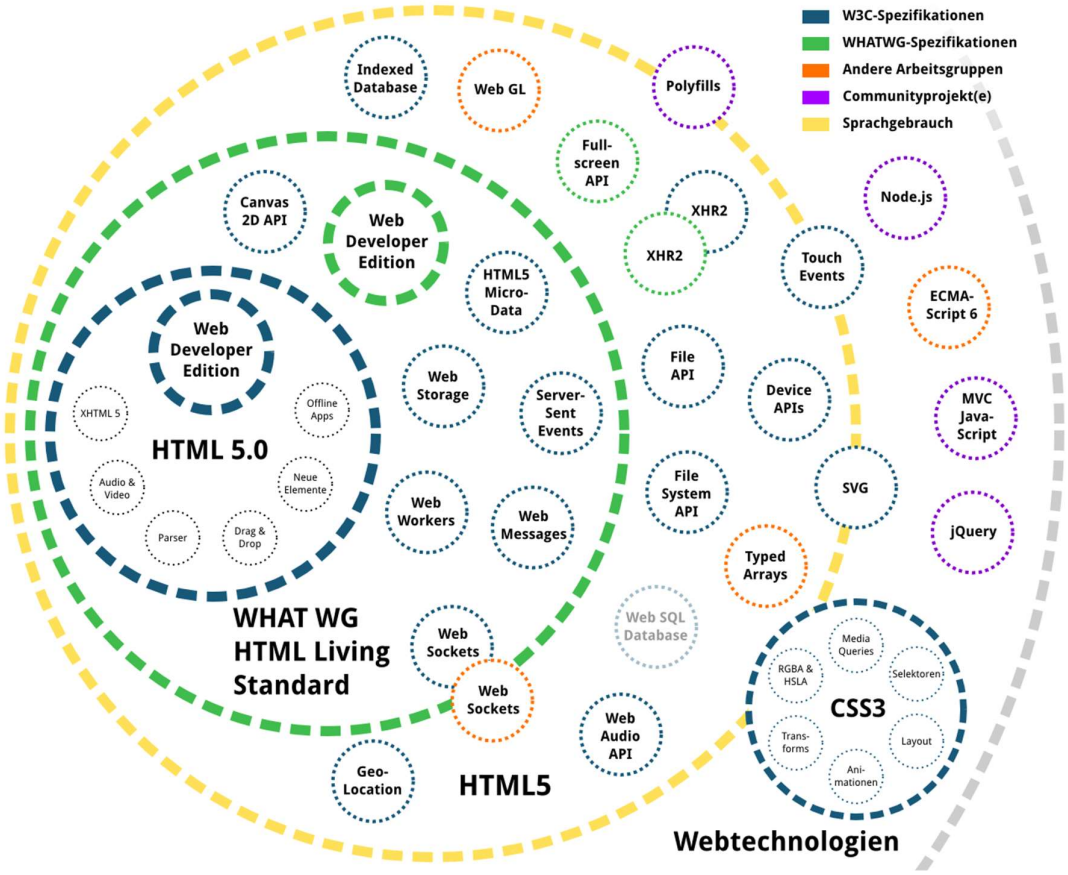
nen strukturierten und kontrollierten Zugang zu den (aktuellen) Funktionalitäten eines Betriebssystems bereitstellen. Auch für öffentlich zugängliche Dienste, die per Webservice erreichbar sind gibt es üblicherweise umfangreiche Dokumentationen, wenngleich hier Aspekte der Systemsicherheit weniger relevant sind.[21] Durch die zunehmende Nutzung von Web- und Cloudservices, die via Computersprachen wie HTML5 realisiert werden, dessen Visualisierung im Browser und damit unabhängig von den unterliegenden Betriebssystemen bereitgestellt wird, haben plattformunabhängige Anwendungen und Dienste zunehmend an Bedeutung gewonnen. Während aktive Inhalte und Videos früher via Flash oder dedizierten Apps realisiert wurden, basieren moderne Videos und einige aktive Inhalte auf HTML5. Dieses wird im Gegensatz zu Flash auch von mobilen Browsern nativ unterstützt und bedarf keines zusätzlich installierten Plug-Ins. Abbildung 3-5 zeigt die umfangreichen Funktionen, die von der W3C als Standardisierungsorganisation und der Arbeitsgruppe WHATWG (Web Hypertext Application Technology Working Group als Branchenarbeitsgruppe gegründet) einerseits als Standard definiert und andererseits im Kontext von HTML5 als Begriff verwendet werden. Die orangenen Kreise stellen hierbei Funktionen dar, die zwar mitunter im Rahmen von Browseranwendungen Verwendung finden, jedoch nicht zum Standard zählen. Darüber hinaus zeigt die Grafik durch die Relation der einzelnen Funktionalitäten auch den modularen Aufbau moderner Standards, welche für die Realisierung von Web-Services zusammenwirken.

Die im Rahmen der Leistungserbringung webbasierter Anwendungen anfallenden und ausgetauschten Daten sind aus der Beschaffungssicht gemäß Crémer et al. (2019) in drei Formen zu unterscheiden. Die freiwillige, in Teilen auch notwendige[22], Datenfreigabe durch den Nutzer sind Daten, die seitens des Nutzers aktiv angegeben werden. Hierunter können beispielsweise E-Mail-Adressen zur Identifizierung und Kontaktmöglichkeit der Nutzer oder darüber hinaus freiwillige Angaben wie Adressen oder Telefonnummern verstanden werden. Beobachtbare Daten hingegen können seitens der Dienste erst durch die aktive Nutzung erhoben werden und können beispielsweise Historien von besuchten Artikeln, Profilen oder die Häufigkeit wechselseitiger Kontaktaufnahmen darstellen. Auf diesen freiwillig angegebenen und beobachteten Daten aufbauend, liegt in der Verknüpfung von Daten und anschließender Inferenz von neuen Daten ein Großteil der Stärke der digitalen Ökonomie. Hergeleitete Daten können dabei aus neuen Produktvorschlägen, aufbauend auf dem Präferenzprofil eines Nutzers, bestehen. Dieser Prozess steht hierbei im Zusammenhang mit den in Kapitel 3.1 beschriebenen „erlernten“ datengetriebenen Netzwerkeffekten. Crémer et al. (2019) weisen jedoch darauf hin, dass eine genaue Abgrenzung dieser Formen nicht trivial und eindeutig ist.

21 Durch Sicherheitsdienstleistungen wie beispielsweise Cloudflare und Authentifizierungskeys bei APIs können offene Schnittstellen von Webservices gesichert werden.

22 Notwendig ist in diesem Kontext nicht gegensätzlich zu freiwillig zu verstehen, da anzugebende Daten als Bestandteil der vertraglichen Nutzungsvereinbarung durch den Nutzer akzeptiert werden. Notwendig kann darüber hinaus auch als für die Erbringung des Dienstes notwendig verstanden werden, beispielsweise wenn eine E-Mail-Adresse für das Zurücksetzen eines Passwortes benötigt wird.

Abbildung 3-5: Die Verhältnisse von Web-Technologien und Standards im Kontext von Web-Services



Quelle: Kröner und Divya (2013)

Darüber hinaus ist ebenso relevant, inwiefern diese Formen der Daten personalisiert genutzt werden. Hier unterscheiden Crémer et al. (2019) zwischen der identifizierbaren und der anonymisierten Nutzung von personalisierten Daten auf individueller Ebene. Oberhalb der Ebene der persönlichen Daten sind aggregierte Daten und kontextualisierte Daten zu verorten. Diese Unterscheidung in der Nutzung ist nicht nur hinsichtlich des Wettbewerbs relevant, sondern auch unter Aspekten des Datenschutzes, da im Falle eines Zugangs die Gefahr einer nicht intendierten Datenweitergabe besteht.

Ferner liegen Daten bei den entsprechenden Plattformen und digitalen Diensten üblicherweise in drei Typisierungen vor (Salinas und Nieto Lemus, 2017). Strukturierte Daten folgen einem standardisierten Schema. Diese Daten können beispielsweise in Datenstrukturen gespeichert und über standardisierte Sprachen wie SQL in Datenbanken ver-

waltet und abgefragt werden. Als Beispiel sei an dieser Stelle JSON als eines der gängigsten strukturierten Datenformate genannt, welches insbesondere hierarchisch strukturierte Daten speichern und übertragen kann. Weitere strukturierte Dateiformate werden in Kapitel 3.6.2 detaillierter erläutert. Strukturierte Daten sind in ihrer Güte und Weiterverarbeitbarkeit höher anzusiedeln als unstrukturierte Daten, die seitens Salinas und Nieto Lemus wiederum zeitlich wiederholend (beispielsweise Sensorendaten) oder ohne zeitliche Wiederholung (beispielsweise Texte, Bilder, Videos) vorliegen können.

Unstrukturierte Daten sind häufig mit großen Datenmengen und Big Data assoziiert und können beispielsweise via Sensoren erhoben werden oder bei der Nutzung eines Dienstes als beobachtete Daten anfallen. Allerdings bedarf es hierbei der Aufbereitung oder Interpretation. Im ersten Schritt ist eine „Bereinigung" der Daten notwendig, um danach eine konsistente Strukturierung vorzunehmen. Durch die weite Verbreitung von gängigen Dateiformaten und einer Vielzahl von Konvertern und Adaptern ist eine syntaktische Kompatibilität grundsätzlich erwartbar. Für die Vorhaltung der Daten sind Datenbanken notwendig, welche je nach Strukturierung der Daten entweder relational oder nicht-relational sind. Ein Konglomerat von Datenbanken wird entsprechend als Data-Warehouse (strukturiert) oder Data-Lake (unstrukturiert), beispielsweise im Fall von kontextfreien Rohdaten, bezeichnet. March et al. (2000) beschreiben den Data-Warehouse-Ansatz als das Ergebnis der syntaktischen und semantischen Aggregierung von mehreren verteilten operationalen Datenbanken. Der Prozess erfordert hierbei die Extraktion gefolgt von dem Beheben von Fehlern, der Ergänzung fehlender Beobachtungen und der anschließenden Konvertierung in ein einheitliches Format zur syntaktischen, strukturellen und semantischen Vereinheitlichung.[23] Die Schwierigkeit hierbei besteht laut March et al. in der Berücksichtigung von notwendigen Unterschieden zur Erhaltung der Kompatibilität mit spezifischen Systemen und der Nutzbarkeit von Informationen über die Grenzen dieser System hinweg. An dieser Stelle ist hervorzuheben, dass diese Vorgehensweise aufgrund der Distribution von datenverarbeitenden Prozessen über unterschiedliche Bereiche der digitalen Plattformen hinweg, eine Notwendigkeit zur effizienten Gestaltung interner Prozesse darstellt. Aus diesem Grund heben March et al. (2000) die Relevanz von *flexiblen Schemata mit Versionierung inklusive einer Dokumentation* hervor.

Während mit Art. 20 Abs. 1 DSGVO ein rechtlicher Rahmen für die Portabilität von personenbezogenen Daten exisitiert, ist IOP, wie in Kapitel 2.1 bereits erläutert, weitgreifender zu verstehen. Vor allem die zeitliche Unmittelbarkeit und gegebenenfalls die Reziprozität im Austausch von Daten erhöht den Koordinierungsbedarf von IOP gegenüber einer reinen Datenportabilität. Dennoch dient die Datenportabilität als bereits implementierter gesetzlicher Rahmen hinsichtlich der technischen Voraussetzungen als Beispiel für die größeren Herausforderungen, welche mit IOP einhergehen.

23 March et al. (2000) nennen hierbei Beispiele wie interne Konventionen der Benennung von Variablen oder die Konvertierung unterschiedlicher Einheiten (z. B. Währungen, Maßeinheiten).

Wie bereits in Kapitel 2.1.1.1 erörtert ist Daten-IOP als kontinuierliche Variante der Datenportabilität zu verstehen (Bourreau et al., 2022). Syrmoudis et al. (2021) zufolge zeigen sich in einer ersten Analyse bereits Diskrepanzen zwischen Vorgaben und Umsetzung der Datenportabilität. So beschränken sich die Vorgaben des Art. 20 Abs. 1 DSGVO auf eine Datenübertragbarkeit in einem „strukturierten, gängigen und maschinenlesbaren Format“., Weitergehende Spezifikationen enthält Art. 20 Abs. 1 DSGVO dagegen nicht, weswegen nach einer vorläufigen empirischen Untersuchung über 70 % der durchgeführten Datenimporte nicht vollständig funktionieren(Syrmoudis et al., 2021). Zur Verbesserung der Datenportabilität ist das „Data Transfer Project“ der Unternehmen Microsoft Google, Twitter und Facebook entstanden, welches auf Basis eines offenen Quellcodes Funktionen und Schnittstellen sowie Dateitypisierungen bereitstellt. Krämer et al. (2020) verglichen die Anzahl und Anteile der Quellcodeänderungen und fanden einen großen Anteil von über 80 % seitens Googles, währenddessen bleibt das Projekt und auch die Anzahl der Änderungen hinter anderen Open-Source-Projekten mit 44 Tausend Zeilen Code gegenüber populären Machine-Learning-Anwendungen wie Tensorflow (2.5 Mio. Zeilen Code) deutlich zurück. Krämer et al. (2020) schließen daraus, dass das Data Transfer Project entsprechend nicht mit starker Ressourcenallokation verfolgt wird.

Unter Berücksichtigung der eingangs beschriebenen modularen Zusammensetzung von Diensten in der Plattformökonomie gewinnt hinsichtlich des Mix-and-Match-Ansatzes die „Offenheit“ der Plattform an Bedeutung. Legt man den von Bourreau et al. (2022) vorgeschlagenen Ansatz der „Equivalence of Inputs“ zugrunde, ist unter rein technischen Aspekten der Zugang auf die Dokumentation von Schnittstellen, transparente Kommunikation von Anpassungen und eine umfassende semantische Erläuterung der Daten notwendig, so wie dies auch für eine vertikal integrierte Firma zur Verfügung steht. Nur auf diese Weise könnten in der Plattformökonomie alle Anbieter dasselbe Produkt oder denselben Dienst zu denselben Konditionen und Bedingungen (einschließlich Preis- und Leistungsniveau) über dieselben Systeme und Verfahren bereitstellen.

Benlian et al. (2015) weisen allerdings in diesem Kontext daraufhin, dass Transparenz und Zugangsmöglichkeiten in der Praxis keineswegs immer im Gleichklang stehen. Diese Unterscheidung kann an Apples Handhabung der NFC-Schnittstelle auf seinen mobilen Endgeräten erläutert werden. Während die kontaktlose Datenübertragung NFC selbst einer öffentlich zugänglichen Standardisierung folgt, war der Zugriff von Drittanbieter-Applikationen auf diese Schnittstelle innerhalb Apples mobilem Betriebssystem iOS zunächst weitgehend unmöglich. Daher schlussfolgern Benlian et al. (2015), dass beide Aspekte unabhängig voneinander zu definieren sind, aber dennoch im komplementären Verhältnis zueinander stehen, da eine Plattform nur durch beide Dimensionen als vollständig offen definierbar sei.

Die umfangreichste Ausprägung von IOP und auch die technisch anspruchsvollste ist die Protokoll-IOP, bei der auf Basis gemeinsam gewählter oder definierter Standards eine direkte vollständige und unmittelbare Interaktion der Systeme stattfindet. Dadurch wird

auch eine vollständige Substitution von Diensten ermöglicht, erfordert dafür jedoch auch das höchste Maß an Koordination und Dokumentation.

Als Voraussetzung für alle Ausprägungen von IOP und in Abgrenzung zur reinen Portabilität, sind nutzbare Programmierschnittstellen und offene respektive standardisierte Datenformate zu nennen, weswegen diese zwei Aspekte im Folgenden detaillierter betrachtet werden sollen.

3.6.1 Kontinuierlicher Zugang zu Daten und Funktionalitäten in Echtzeit

Application programming interfaces (APIs) stellen eine funktionale Brücke zwischen einer Software oder einem Dienst und der weiteren Verwendung dar. Sie sind als die Kommunikationsschnittstelle eines Programms gegenüber einem anderen zu verstehen. Dabei sind sie eine Vereinigung an vordefinierten Methoden und Objekten, mit deren Nutzung auf das Produkt der vorangegangenen Stufe zugreifen kann, ohne hierbei den Prozess oder die ursprünglichen Objekte vollständig zu implementieren. Mit dieser Abstrahierung von einzelnen Prozessen ist es möglich verteilte, komplexe Programme als Sammlung einzelner Modelle darzustellen. Die daraus resultierende Modularität verändert Stylos (2009) nach die Aufgabe von Programmierern von der grundlegenden Programmierung hin zum „Zusammennähen“ von Funktionalitäten. Aufgrund dieser Vereinfachung ist die weitverbreitete Nutzung von APIs im Zuge von digitalen Plattformen üblich (Stylos und Myers, 2006). Bereits Bloch (2006) stellte dabei die Bedeutung von gut funktionierenden APIs für den Erfolg des Unternehmens heraus. Ebenso merkt er an, dass Software und Funktionalitäten modular gedacht und programmiert werden müssen. Dabei sei jedes Modul mit einer Schnittstelle zu versehen, so dass die Module auch an anderer Stelle erneut verwendet werden können. Die Charakteristiken guter APIs definiert er für die Anwenderseite mit den Eigenschaften einer leichten Verständlichkeit und einfachen Nutzung, selbst ohne Dokumentation. In dieser Anforderung spiegelt sich das Kriterium der Usability als Voraussetzung für IOP wider. Gleichzeitig soll dabei berücksichtigt werden, dass der mutwillige oder unabsichtliche Missbrauch eingeschränkt wird. Für das technische Publikum sei eine einfache Lesbarkeit des Codes, bei gleichzeitiger einfacher Wartung und Erweiterbarkeit essenziell. Ferner stellt er die Bedeutung von guter Dokumentation heraus, welche für die oben genannte Weiterverwendung die Basis liefere (Bloch, 2006).

Im Kontext von Webservices und der Nutzung digitaler Dienste ist anzumerken, dass ein relevanter Bestandteil von Zusatzfunktionen über einsehbare oder „versteckte“ (private) APIs, die vom Browser abgerufen werden, realisiert wird. Auf der anderen Seite gibt es auch dediziert öffentliche APIs, wie beispielsweise die Google Maps Geocoding API, anhand derer Adressinformationen zu Geokoordinaten umgewandelt werden können (Google, 2022b). Dies kann als Beispiel einer API für eine modulare Funktionalität verstanden werden, welche von Dritten in ihren Dienst implementiert werden kann, ohne

dabei die Funktionalität dieser Komponenten in der eigenen Servicekomposition replizieren zu müssen. Eine datenfokussierte API wäre beispielsweise die Twitter API mithilfe der unter anderem gesammelte Kurznachrichten von Twitter zu einem bestimmten Thema abgerufen werden können. Durch Selektionskriterien können dann Thema und Umfang eingegrenzt werden (Twitter, 2022). Bei komplexeren APIs sind die Funktionalitäten oder Daten in „Endpoints“ gruppiert, um zielgerichtete und effiziente Anfragen zu ermöglichen.

Bei kommerziellen APIs ist die Verwendung eines personalisierten Schlüssels (Token) zur Identifizierung und Abrechnung üblich. Dies geschieht auch im Kontext der Vermeidung von nicht steuerbaren Überlastungen. Üblicherweise werden Abrufe von Funktionalitäten oder Daten als „Call“/“Hit“ verstanden, der gemäß zugrundeliegender Preisschemata abgerechnet werden kann. Die ökonomischen Aspekte von APIs und deren Abrechnung werden in Kapitel 3.7 im Rahmen der effizienten Implementierung erörtert. Insbesondere bei kommerziellen Angeboten wird üblicherweise eine umfangreiche Dokumentation bereitgestellt. Darüber hinaus existieren auch Internetplattformen wie Stack Overflow und spezifische Diskussionsforen, die offizielle Dokumentationen erweitern (Stack Overflow, 2022).

3.6.2 Standardisierte Daten- und Metadatenformate

Im Kontext digitaler Plattformen sind die gängigen Datenformate für strukturierte mitunter hierarchisch organisierte Daten beispielsweise JSON oder XML, für einfache strukturierte Daten CSV (Kommagetrennte Werte) oder Textdateien. Für Bild- und Videodateien existieren ebenfalls gängige Formate. Unter offenen Dateiformaten werden im Kontrast zu Closed-Source-Formaten, jene verstanden, deren Spezifikation veröffentlicht ist. Bei proprietären Datenformaten ist mitunter die Spezifikation des Formats veröffentlicht, das Eigentum und damit auch die Nutzungsrechte befinden sich allerdings beim Entwickler. Sollen proprietäre Datenformate innerhalb einer Software verarbeitet werden können, sind Lizenzvereinbarungen mit dem Entwickler zu treffen. Mit einer veröffentlichten Spezifikation kann seitens Softwareanbietern eine Austauschfähigkeit mit diesen Formaten sichergestellt werden. Dies stellt jedoch nur die syntaktische Kompatibilität bereit, garantiert dabei keineswegs auch die semantische Kompatibilität. Deswegen werden beispielsweise im Rahmen des Data Transfer Projects Datei-Modelle vorgeschlagen und implementiert, welche teilweise auf öffentlich zugänglichen Schemata basieren (Data Transfer Project, 2021). Diese Schemata stellen die semantische Kompatibilität durch Koordinierung her und liefern via mitgelieferter Metadaten zusätzliche Informationen zu Interpretation der Daten. Die Untersuchung von Syrmoudis et al. (2021) hinsichtlich der Dateiformate ausgewählter Datenportabilitäts-Exporte zeigt jedoch, dass zwar offene und maschinenlesbare Daten einen Großteil der Formate darstellten, teilweise jedoch auch auf schwerer zu verarbeitende Formate wie PDF zurückgegriffen wurde.

Empfehlungen zur einheitlichen Definition von Metadaten wurden im Ressource Description-Format (RDF) zusammengefasst, welches seitens des W3-Konsortiums konzipiert wurde und inzwischen als Bestandteil eines Frameworks des semantischen Webs Einzug erhielt. Mit dem Format JSON-LD (JSON für verlinkte Daten) werden die Empfehlungen von RDF als Metadatenformat in das offene Standardformat JSON eingebettet.

3.7 Implementierung von Interoperabilitätsregelungen

3.7.1 Ausgestaltung von Interoperabilitätsvorschriften

Die Ausgestaltung konkreter IOP-Vorschriften ist technisch anspruchsvoll, da diese der Komplexität spezifischer Dienste und deren bestehenden Implementierungen gerecht werden müssen. Dadurch ergeben sich unterschiedliche Anforderungen im Hinblick horizontale und vertikale IOP.

Unter horizontaler IOP lässt sich das Anforderungsprofil und existierende Funktionalitäten unterschiedlicher Anwendungen verhältnismäßig einfach erheben, katalogisieren und nach z. B. Nutzungshäufigkeit und Verbreitung einstufen. Somit lässt sich ein relativ klares Bild der relevanten und essenziellen Kernfunktionalitäten auf einer Wertschöpfungsstufe erheben. Es handelt sich daher immer um ein anwendungsspezifisches Anforderungsprofil für IOP, welches nur partiell oder vollumfänglich standardisiert werden kann.

Im Fall vertikaler IOP sind bestehende (private) APIs, welche beispielsweise bereits von vertikal integrierten Diensten einer Plattform genutzt werden, ebenfalls verhältnismäßig einfach für Wettbewerber auf anderen Wertschöpfungsstufen zu öffnen. Allerdings wurden bestehende APIs ursprünglich für spezifische Zwecke entwickelt und können damit nur beschränkt auch für andere Anwendungsszenarien genutzt werden. Diese APIs sind damit nur in seltenen Fällen anwendungsagnostisch entwickelt. Da in der Plattformökonomie neue Dienste auch durch die Komposition bestehender Module und Anwendungen erbracht werden, ist durch diese Limitierung die Entwicklung neuer innovativer Dienste auf den bestehenden Funktionsumfang beschränkt. Dementsprechend sind im Fall vertikaler IOP neben der Erhebung der bestehenden Anwendungsszenarien (z. B. ancillary services) auch die potenziellen Szenarien und Einsatzzwecke zu erheben, für welche zukünftig IOP hergestellt werden soll. Nur so kann das Innovationspotenzial vertikaler IOP gehoben werden. IOP definiert damit in diesem Fall vielmehr den Gestaltungsspielraum möglicher Servicekompositionen für eine Vielzahl von Anwendungsszenarien, während im Fall horizontaler IOP das Anwendungsszenario (wenn auch nicht alle zukünftig denkbaren Funktionalitäten) bereits festgelegt ist.

3.7.2 Festlegung der Art und Weise wie die Standards definiert werden

Standardisierung bzw. die Einigung auf einen Standard stehen im Kern aller IOP-Bemühungen. Wie bereits in Kapitel 2.1.3 dargelegt ist Standardisierung allerdings mit verschiedenen Unwägbarkeiten behaftet. Firmen haben oft bestehende Interessen bzgl. der verwendeten Technologien, insbesondere im Fall horizontaler IOP, die Prozesse sind zeit- und kostenintensiv und die Bildung von Allianzen kann das Ergebnis beeinflussen.

Als Institutionen zur Bildung von Standards haben sich Standardisierungsorganisationen bereits bewährt und sind damit am besten dafür geeignet einen solchen Prozess zu begleiten und ein für alle Beteiligten akzeptables Ergebnis herbeizuführen.

Allerdings muss dabei eine Reihe von Aspekten berücksichtigt werden. Da Standardisierung ein kostenintensiver Prozess ist, besteht die Gefahr, dass sich finanzstarke Marktteilnehmer in solchen Prozessen besser durchsetzen können als beispielsweise KMUs. Darüber hinaus besteht die Möglichkeit das solche Prozesse durch Kompromisslösungen die Qualität und Sicherheit bestehender Lösungen abschwächen könnten. Verbraucher sind üblicherweise an solchen Prozessen nicht beteiligt und können daher nur indirekt ihre Wünsche einbringen.

Diesen Bedenken muss durch Schranken und Vorgaben in dem Prozess zur Herstellung von IOP bei der Gestaltung von IOP-Vorschriften begegnet werden (vgl. auch Kapitel 3.3.2). Im Vergleich zu den benannten Problemen mit klassischen SSOs kann hier ggf. eine finale Entscheidungsgewalt beim Regulierer nötig sein. Dabei sollten neben den Incumbents auch weitere Stakeholder wie potenzielle Wettbewerber, Verbraucherorganisationen und unabhängige technologische Expertise einbezogen werden (Scott Morton et al., 2021).

4 Interoperabilität bei nummernunabhängigen interpersonellen Telekommunikationsdiensten

4.1 Einordnung NI-ICS

4.1.1 Abgrenzung

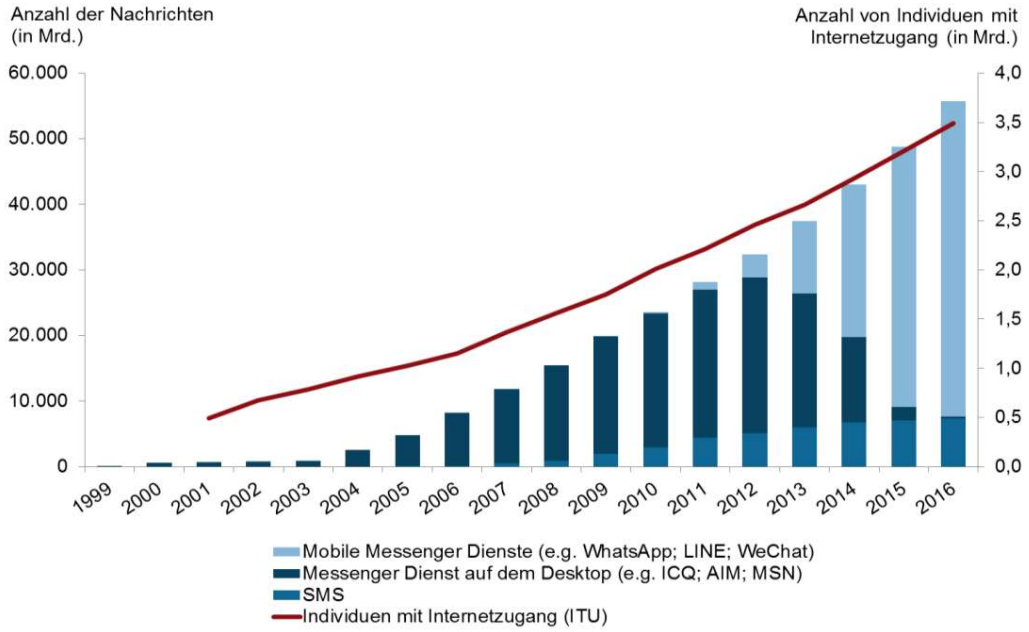
Mit dem Inkrafttreten der **Novelle des TKG** im Dezember 2021 werden NI-ICS, wie in Kapitel 3.1.2 erläutert, in Teile des Regulierungsregimes einbezogen. Laut Begriffsdefinition ist ein NI-ICS „ein interpersoneller Telekommunikationsdienst, der weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummernpläne, herstellt noch die Telekommunikation mit Nummern nationaler oder internationaler Nummernpläne ermöglicht“. Die zweite Gruppe interpersoneller Kommunikationsdienste, die nummerngebundenen interpersonellen Kommunikationsdienste (NB-ICS), grenzen sich von NI-ICS durch eben jene Nutzung öffentlicher Nummernressourcen ab.

Beide Arten von interpersonellen Kommunikationsdiensten werden 2018 erstmals in den novellierten europäischen Kodex für elektronische Kommunikation (engl. European Electronic Communications Code, EECC) unter der Definition für elektronische Kommunikationsdienste (engl. electronic communications service, ECS) (Artikel 2 Absatz 4 der Richtlinie (EU) 2018/1972) berücksichtigt. Diese Modifikation stellt eine Erweiterung des bis dahin geltenden ECS-Begriffs nach Artikel 2 c) der Richtlinie 2002/21/EG des Europäischen Parlaments vom 7. März 2002 dar, da nun nicht nur OTT-0-Dienste, sondern weitgehend auch OTT-1-Dienste von der ECS-Definition erfasst werden. Die Bezeichnungen OTT-0 und OTT-1 entstammen der Taxonomie des BEREC (2016) vor der Neufassung des EECC. Die Taxonomie diente dazu, elektronische Kommunikationsdienste nach der Richtlinie 2002/21/EG von Diensten, die eine Kommunikation über das (offene) Internet ermöglichen (Over-The-Top (OTT)-Dienste), abzugrenzen. Dabei bezeichnete ein OTT-0-Dienst einen OTT-Dienst, der dennoch in der Lage war, eine Verbindung zu klassischen Telefondiensten via Rufnummer herzustellen. Ein OTT-1-Dienst ohne diese Fähigkeit galt hingegen nicht als ECS, konnte jedoch potenziell mit diesem konkurrieren (BEREC, 2016).

Schon im frühen Entwicklungsstadium des Internets entstanden die ersten Kommunikationsprotokolle für die interpersonelle Kommunikation. Die E-Mail ist als standardisierte und somit vollständig protokoll-interoperable Möglichkeit der Kommunikation weit verbreitet. Um auch in Echtzeit direkt interagieren zu können wurde mit dem IRC-Protokoll (Internet Relay Chat) eine Möglichkeit geschaffen bilateral und in Gruppen zu kommunizieren. Auf diesem Prinzip bauten erste desktopbasierte Chat-Clients wie AOL Instant Messenger, ICQ und MSN-Messenger auf. In Abbildung 4-1 ist das besonders in den Jahren

2004 bis 2011 starke Wachstum der über diese Dienste versendeten Nachrichten dargestellt. Mobile Instant Messenger haben mit der Verbreitung von Smartphones und steigender Datenvolumina in Mobilfunkverträgen die Bedeutung klassischer Kurznachrichten (SMS) relativiert und desktopbasierte Messenger marginalisiert. Beginnend mit dem Jahr 2010 ist ein stetiges Wachstum der versendeten Nachrichten auf Kosten obengenannter Kommunikationsdienste zu beobachten.

Abbildung 4-1: Anzahl der jährlich versendeten Nachrichten via SMS und Online-Kommunikationsdiensten (weltweit in Milliarden Nachrichten; Individuen mit Internetanschluss in Milliarden)



Quelle: Arnold et al. (2017)

Folgt man der BEREC-Definition können Produkte wie Skype mit differenzierten Teilfunktionen unterschiedlichen OTT-Kategorien zugeordnet werden. So ist es, neben der Funktion einen Videoanruf zwischen zwei Skype-Nutzern (OTT-1) zu tätigen, ebenfalls möglich als Skype-Nutzer klassische Telefonanschlüsse anzurufen (OTT-0). Entsprechend sind nach BEREC (2016) die Leistungserbringer von OTT-0-Diensten üblicherweise nicht exklusiv ISPs, eine Abgrenzung, die im Rahmen der zunehmenden Nutzung von VOIP-Diensten an Relevanz verliert. Hier fallen Parallelen zur aktuellen Definition von NI-ICS und NB-ICS im EECC auf. Nichtsdestotrotz sind NI-ICS im Vergleich zur OTT-Taxonomie gemäß der BEREC-Definition von 2016 (BEREC, 2016) als Teilmenge von, jedoch nicht zwingend deckungsgleich mit OTT-1-Diensten zu verstehen.

Insgesamt legt der EECC in mehreren Erwägungsgründen Anforderungen fest, denen die einzelnen Dienste genügen müssen, um allgemein als interpersoneller Kommunikationsdienst zu gelten oder speziell in die Kategorie NI-ICS oder NB-ICS zu fallen. Bisweilen lassen sich NI-ICS und NB-ICS weder untereinander noch im Hinblick auf andere Dienste, die ebenfalls Kommunikation zulassen, vollständig trennscharf abgrenzen.

Sowohl für die Abgrenzung als auch die Beurteilung, ob neben horizontalem auch vertikaler Wettbewerb in einer Dienstekategorie vorliegt, ist es unter anderem entscheidend, ob offene (Massenkommunikation, z. B. soziale Medien) oder geschlossene (Individualkommunikation, z. B. einfache Messenger) Nutzergruppen vorliegen (Taş und Arnold, 2019). Allerdings sind die Grenzen zwischen diesen beiden Formen aufgrund der multifunktionalen Ausgestaltung vieler Dienste nicht immer trennscharf. Ähnlich wie bei Messaging-Diensten lassen sich bei sozialen Netzwerken Funktionalitäten beobachten, welche den Austausch von Direktnachrichten zwischen einzelnen Nutzern sowie geschlossene Nutzergruppen ermöglichen.

Auch die Kriterien eines interaktiven Austauschs bzw. einer Antwortmöglichkeit und die Beschränkung auf eine endliche Zahl von Personen (vgl. EECC, Richtlinie (EU) 2018/1972) führen nicht immer zu einer klaren Zuordnung. Das Fehlen einer eindeutigen Dichotomie zeigt sich insbesondere am Beispiel von Telegram, das auch über das Thema der IOP hinaus anhaltend diskutiert wird (vgl. Jäschke, 2021). Hier stellt sich unter anderem die Frage, inwiefern Gruppen mit bis zu 200.000 Nutzern noch als „geschlossen“ zu bezeichnen sind, gleichzeitig wird der Dienst in großen Teilen aber auch analog zu WhatsApp oder Signal für die bilaterale oder private Kommunikation in Gruppen genutzt. Durch die Kanalfunktion von Telegram ist sogar eine unbegrenzte Öffentlichkeit erreichbar, womit Telegram auf offene Nutzergruppen abzielt und Funktionen sozialer Medien implementiert. Anders als in klassischen sozialen Netzwerken müssen solche Kanäle aber proaktiv aufgesucht werden und werden nicht beispielsweise durch einen News-Feed akkumuliert. Das hier angesprochene Abgrenzungsproblem wird auch in *Erwägungsgrund 14 des Digital Services Act (DSA)* aufgegriffen. Dort wird einerseits betont, dass interpersonelle Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972 nicht unter den Plattformbegriff im Sinne des DSA fallen. Andererseits wird klargestellt, dass die Plattformregeln des DSA auf Dienste Anwendung finden, die es ermöglichen Informationen einer unbestimmten Zahl von Empfängern zugänglich zu machen, etwa durch öffentliche Gruppen und offene Kanäle. Als öffentlich sollen dabei Gruppen gelten, bei denen Nutzer automatisch registriert werden können, ohne dass ein Mensch über die Zulassung zur Gruppe entscheidet (siehe dazu Busch, 2022).

Von der rechtlichen Definition z. B. im Rahmen des *EECC (Art. 2, Abs. 4) bzw. TKG (§ 3 Nr. 24)* ist außerdem die Kommunikation ausgeschlossen, die nur eine „untergeordnete Nebenfunktion“ darstellt und untrennbar mit einem anderen Dienst verbunden ist. Neben eindeutigen Fällen wie der Chatfunktion eines Online-Spiels kann es aber auch hier zu Grenzfällen oder perspektivisch zu Umgehungsmöglichkeiten kommen. Eine Einschätzung, ob z. B die Privatnachrichtenfunktion des Dienstes Instagram als untergeordnete

Nebenfunktion von Instagram als sozialem Netzwerk anzusehen ist, lässt sich nicht immer basierend auf technischen Kriterien bestimmen und hängt unter Umständen von den dynamischen Nutzungsgepflogenheiten der Nutzer ab. Die Abgrenzung wird außerdem durch die Verbreitung von Diensten, die zu vertikal integrierten Ökosystemen gehören, erschwert. Dieser Aspekt wird in Kapitel 4.1.3.5 weiter aufgegriffen.

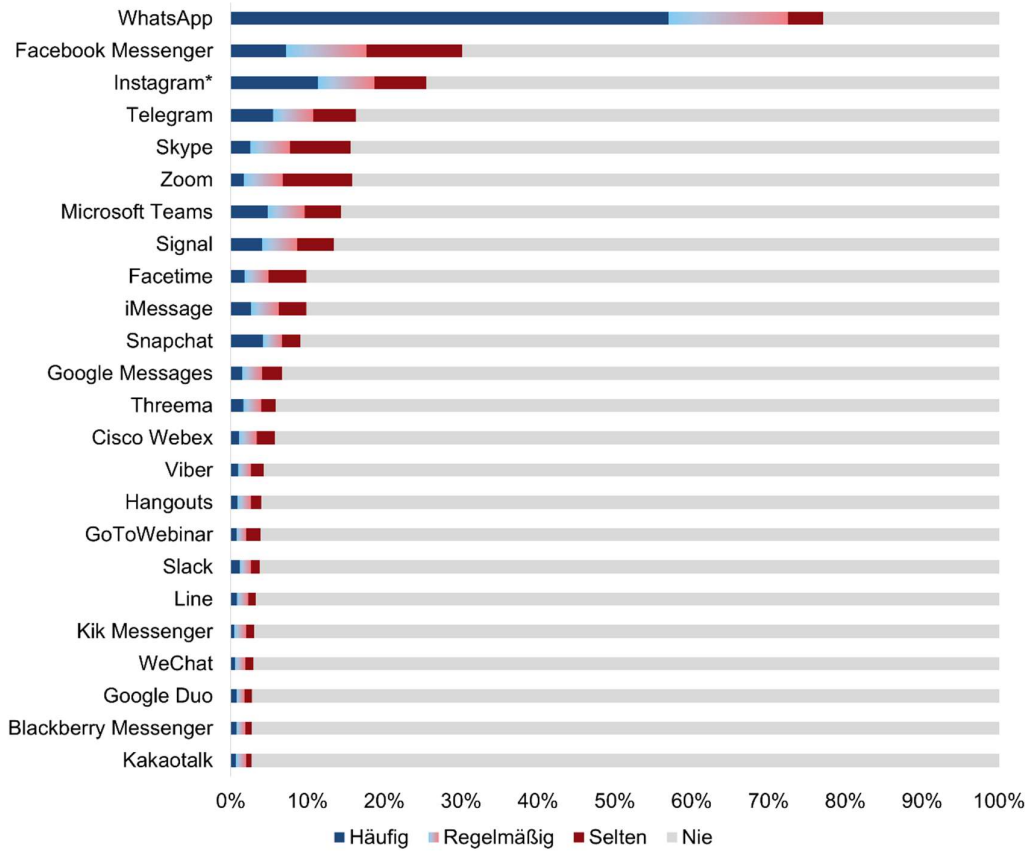
Aufgrund dieser Problematik wird im Folgenden bei der Marktdarstellung der Begriff „Online-Kommunikationsdienste“ verwendet. Online-Kommunikationsdienste ist dabei ein weiter gefasster Begriff, der allgemein über das Internet erbrachte Kommunikationsdienste unabhängig von ihrer jeweiligen regulatorischen Einordnung zusammenfassen soll (vgl. auch Bundesnetzagentur, 2022), wovon NI-ICS entsprechend eine Teilmenge mit einer konkreteren Legaldefinition darstellen.

4.1.2 Marktlage Online-Kommunikationsdienste

Zu den beliebtesten Online-Kommunikationsdiensten in Deutschland gehört vor allem WhatsApp. Laut den Ergebnissen der jährlichen Befragung des WIK zur Nutzung von Kommunikationsdiensten, die zuletzt Ende 2021 durchgeführt wurde, beläuft sich der Nutzeranteil von WhatsApp auf 77% der erwachsenen Bevölkerung.[24] Der Nutzeranteil von WhatsApp liegt damit weit über den Anteilen anderer bekannter Dienste wie Facebook Messenger und Instagram, die wie WhatsApp dem Meta-Konzern angehören, oder Telegram. Der Dienst WhatsApp wird nicht nur von den meisten Verbrauchern in Deutschland verwendet, sondern setzt sich auch in der Nutzungsfrequenz deutlich von anderen Online-Kommunikationsdiensten auf dem Markt ab. Die meisten Nutzer verwenden den Dienst nahezu täglich.

24 Als Nutzer gelten diejenigen Befragten, die angaben, über den Dienst eine andere Person kontaktiert zu haben oder von einer anderen Person kontaktiert worden zu sein.

Abbildung 4-2: Nutzung und Nutzungshäufigkeit ausgewählter Online-Kommunikationsdienste



Quelle: WIK-Consult. Sonderauswertung der jährlichen Umfrage des WIK. 2021: N=3.178. Deutsche Bevölkerung ab 18+ Jahre. Häufig: Mind. einmal am Tag; Regelmäßig: 2-6 mal in der Woche; Selten: Max. einmal pro Woche. *bezogen auf direkte Nachrichten, die gesendet oder empfangen wurden (Direktnachrichten).

Grundsätzlich beschränken sich Verbraucher jedoch nicht nur auf einen einzelnen Dienst, sondern nutzen in der Tendenz mehrere Dienste.

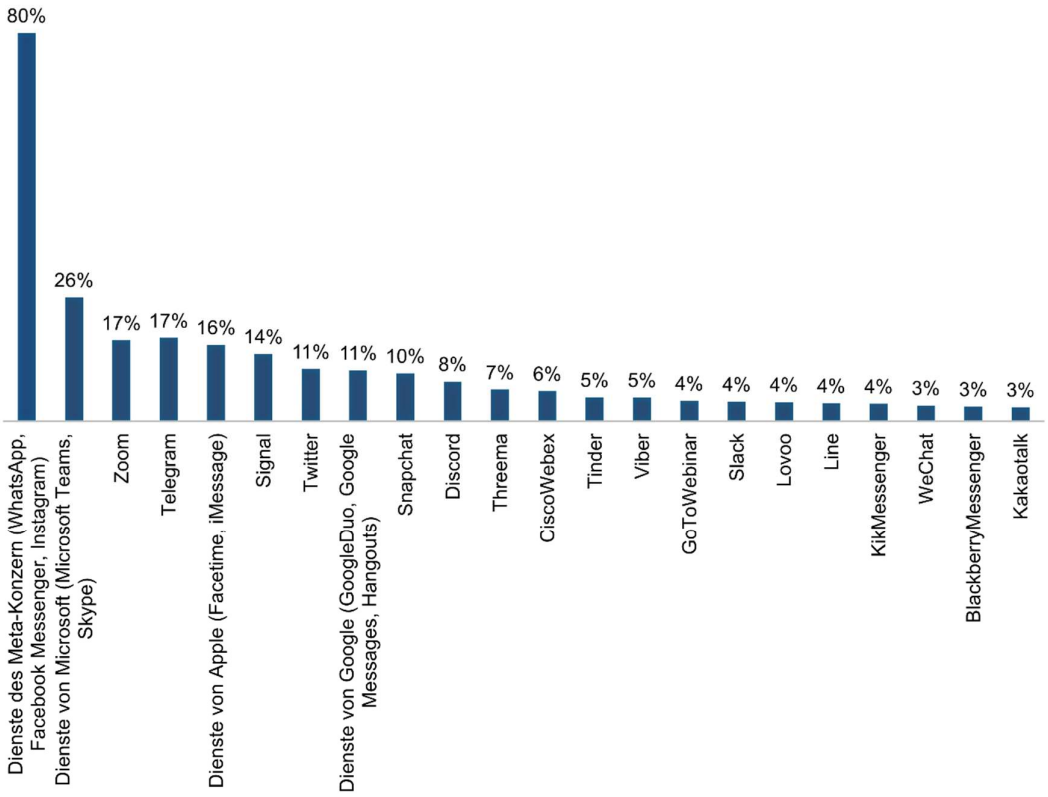
Die Daten aus der jährlichen Umfrage des WIK zur Nutzung 24 ausgewählter Online-Kommunikationsdienste zeigen, dass etwa 83% der Befragten mindestens einen der betrachteten 24 Online-Kommunikationsdienste nutzen.[25] Entweder werden die Nutzer über die jeweiligen Dienste kontaktiert oder sie kontaktieren andere Personen. Insgesamt 75% dieser Nutzer gaben an mindestens zwei Dienste zu verwenden und werden damit als Multi-Homer klassifiziert. Im Schnitt verwenden die Nutzer aus den 24 betrachteten

25 Ausgewählte Online-Kommunikationsdienste: 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.

Online-Kommunikationsdienste etwa 3,7 verschiedene Dienste. Dabei verwenden Nutzer in der Altersgruppe 18-24 Jahre im Durchschnitt etwa 6 Dienste, während Nutzer, die älter als 55 Jahre sind, durchschnittlich nur etwa 2 Dienste verwenden.

Drei der betrachten Dienste gehören zum Meta-Konzern, namentlich WhatsApp, Facebook Messenger und Instagram, und sind die drei am häufigsten genutzten Dienste in Deutschland. Etwa **80%** der Befragten in Deutschland haben in der Umfrage des WIK in 2021 angegeben, mindestens einen der Dienste des Meta-Konzerns zu verwenden. Demgegenüber stehen 52% die angeben, mindestens einen der restlichen 21 Online-Kommunikationsdienste zu nutzen (siehe Abbildung 4-3).

Abbildung 4-3: Nutzung von ausgewählter Online-Kommunikationsdienste – nach Unternehmen

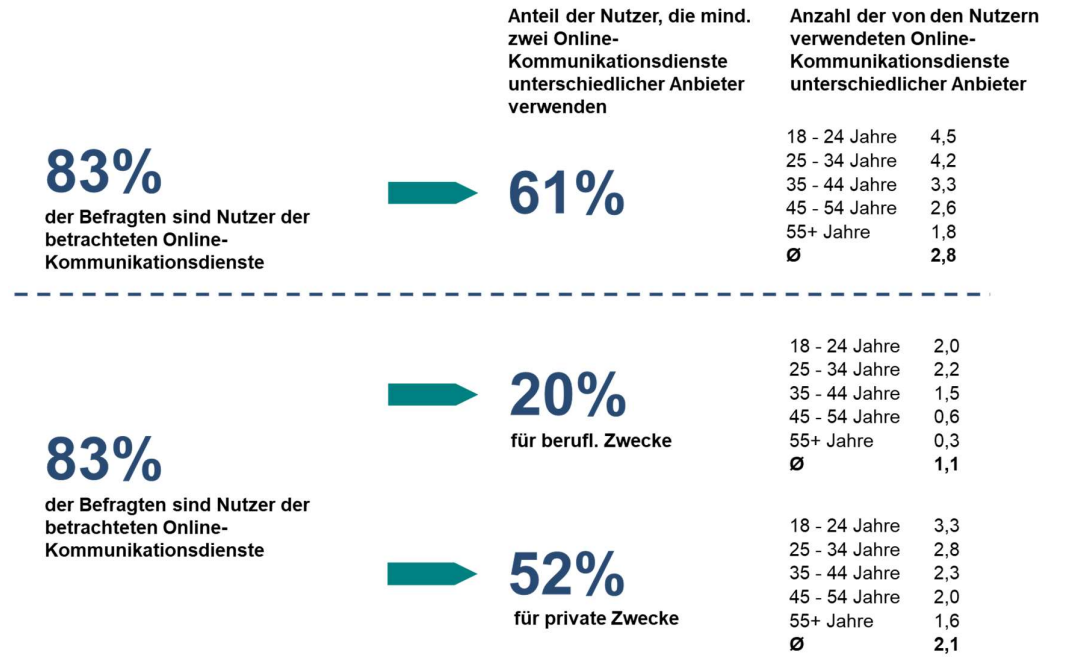


Quelle: WIK-Consult. Sonderauswertung der jährlichen Umfrage des WIK. 2021: N=3.178. Deutsche Bevölkerung ab 18+ Jahre. Ausgewählte Online-Kommunikationsdienste: Snapchat, Threema, Signal, Telegram, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Slack, Zoom, GoToWebinar, Cisco Webex sowie Dienste von Microsoft (Microsoft Teams, Skype), Dienste von Apple (Facetime, iMessage), Dienste von Google (GoogleDuo, Google Messages, Hangouts) und Dienste des Meta-Konzerns (WhatsApp, Facebook Messenger, Instagram), die für die Auswertung je als eine Einheit gewertet werden.

Abbildung 4-4 gibt die Ausprägung des wettbewerbsrelevanten Multi-Homings wieder. Hierfür werden die 24 ausgewählten Online-Kommunikationsdienste, die jeweils zu einem Konzern gehören, als eine Einheit zusammengefasst. Im Vergleich zu den obigen Ausführungen fällt bei dieser Auswertung der Anteil der Multi-Homer um **14 Prozentpunkte** geringer aus. Es reduziert sich ebenfalls die Anzahl der durchschnittlich genutzten Dienste um einen Dienst.

Das Multi-Homing scheint zumindest teilweise auf die Unterscheidung zwischen beruflicher und privater Nutzung von Online-Kommunikationsdiensten zurückzugehen. Die nachfolgende Abbildung zeigt, dass im Mittel einer der insgesamt drei im Durchschnitt genutzten Online-Kommunikationsdienste voraussichtlich für die berufliche Kommunikation verwendet wird und zwei für die private Kommunikation.

Abbildung 4-4: Multi-Homing ausgewählter Online-Kommunikationsdienste – Gesamt und nach Verwendungszweck



Quelle: WIK-Consult. Sonderauswertung der jährlichen Umfrage des WIK. 2021: N=3.178. Deutsche Bevölkerung ab 18+ Jahre. Ausgewählte Online-Kommunikationsdienste: Snapchat, Threema, Signal, Telegram, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Slack, Zoom, GoToWebinar, Cisco Webex sowie Dienste von Microsoft (Microsoft Teams, Skype), Dienste von Apple (Facetime, iMessage), Dienste von Google (GoogleDuo, Google Messages, Hangouts) und Dienste des Meta-Konzerns (WhatsApp, Facebook Messenger, Instagram), die für die Auswertung je als eine Einheit gewertet werden.

Verbraucher verwenden jedoch nicht nur Online-Kommunikationsdienste. In einer Umfrage des WIK aus dem Jahr 2020 gaben etwa 91% der Befragten an, weiterhin Festnetz- und/oder Mobilfunktelefonie zu nutzen. Im Vergleich zu WhatsApp oder den anderen

Diensten des Meta-Konzerns kommen Festnetz- und Mobiltelefonie jedoch weniger häufig zum Einsatz. Während 68% der Nutzer von WhatsApp angaben, den Dienst mehrmals täglich zu nutzen, liegt dieser Anteil bei Festnetz- und Mobiltelefonie nur bei knapp 30%. Klassische Kurznachrichten (SMS) werden hingegen noch viel seltener verwendet, obwohl immerhin 63% der Befragten Nutzer dieses Dienstes sind. Letzteres deutet darauf hin, dass sich die klassische Kurznachricht zu einem Rückfallkanal entwickelt hat (Taş et al., 2021).[26]

Multi-Homing in Deutschland[27]

- Dienste des Meta-Konzerns gehören in Deutschland zu den meist genutzten Online-Kommunikationsdiensten. Etwa **80% der Verbraucher in Deutschland ab 18 Jahren kommunizieren über WhatsApp, Facebook Messenger oder Instagram** mit ihren Kontakten. Dienste anderer Unternehmen verzeichnen einen Nutzeranteil von teilweise je weit weniger als 30%.
- Multi-Homing auf Diensteebene: Etwa 75% der Nutzer von Online-Kommunikationsdiensten nutzen zwei oder mehr unterschiedliche Dienste. Im Durchschnitt verwenden die Nutzer etwa 3,7 verschiedene Online-Kommunikationsdienste.
- Multi-Homing auf Unternehmensebene: Anteil der Nutzer von Online-Kommunikationsdiensten, die mindestens zwei Online-Kommunikationsdienste unterschiedlicher Unternehmen nutzen, liegt bei 61%. Im Schnitt werden von den Nutzern 2,8 Dienste unterschiedlicher Unternehmen verwendet.

4.1.3 Ökonomische Besonderheiten

4.1.3.1 Netzwerkeffekte

Insbesondere bei (nicht interoperablen) Diensten beeinflusst das Verhalten der Endnutzer die Marktkonzentration über Netzwerkeffekte. Im Bereich von Messaging-Diensten kommt den direkten Netzwerkeffekten eine besondere Bedeutung zu (vgl. u. a. ACCC, 2020). Je mehr Nutzer einen bestimmten Messaging-Dienst nutzen, desto attraktiver wird es tendenziell für neue Nutzer, sich ihm anzuschließen.

---

26 Einzelne Ergebnisse stammen zudem aus einer Sonderauswertung der jährlichen Umfrage des WIK aus dem Jahr 2020.

27 Basierend auf einer jährlichen Umfrage des WIK. 2021: N=3.178. Deutsche Bevölkerung ab 18+ Jahre. Ausgewählte Online-Kommunikationsdienste: Snapchat, Threema, Signal, Telegram, Viber, KikMessenger, Kakaotalk, Line, WeChat, Blackberry Messenger, Slack, Zoom, GoToWebinar, Cisco Webex sowie Dienste von Microsoft (Microsoft Teams, Skype), Dienste von Apple (Facetime, iMessage), Dienste von Google (GoogleDuo, Google Messages, Hangouts) und Dienste des Meta-Konzerns (WhatsApp, Facebook Messenger, Instagram). Ohne E-Mail.

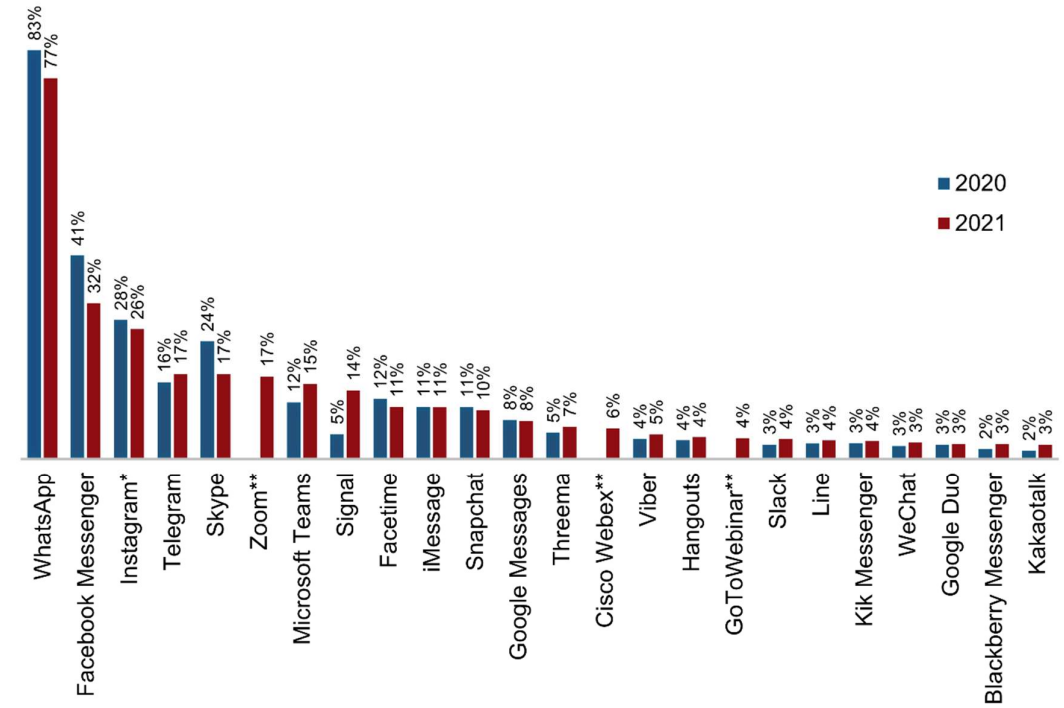
Im Vergleich zu klassischen Beispielen für Netzwerkgüter, bei denen der Nutzen eher von der reinen absoluten Anzahl anderer Nutzer abhängt und steigt, wirken die Netzwerkeffekte im Bereich von Messaging-Diensten häufig heterogener und spezifischer. Persönliche Kontakte und bestehende „Netzwerke“ im sozialwissenschaftlichen Sinne spielen hier eine stärkere Bedeutung. Das bedeutet, dass die Installation oder Nutzung eines bestimmten Dienstes tendenziell eher von der Nutzung ganz spezieller Personen aus dem Familien- oder engen Freundeskreis und nicht durch die Gesamtzahl anderer Nutzer geprägt ist. In der Literatur findet sich dafür teilweise der Begriff von **„identity-based network effects“ (identitätsbasierte Netzwerkeffekte)**, siehe z. B. Colangelo und Maggiolino (2018). Hier liegt auch ein entscheidender Unterschied zu „sozialen Netzwerken“ im heutigen Sinne von „Social Media“ vor, welcher mit der Unterscheidung von offenen und geschlossenen Nutzerkreisen vergleichbar ist. Für die Nutzung digitaler Dienste mit geschlossenen Nutzerkreisen wie WhatsApp ist eher die Präsenz bestimmter Personen/Kontakte entscheidend (ACCC, 2020), während für offene Nutzerkreise auch die Präsenz einer absoluten Anzahl von Personen eine größere Rolle einnimmt.

Prinzipiell kann durch die individuelle Bedeutung bestimmter Kontakte auch der Wechsel auf andere Dienste erleichtert werden. Im Zweifel kann bereits das Wechseln eines einzelnen Nutzers „U“ von einem Anbieter „A“ zu Anbieter „B“ direkt dazu führen, dass die Kontakte des Nutzers „U“ ebenfalls zum Anbieter „B“ wechseln, um ihn weiterhin erreichen zu können. Bei identitätsagnostischen Netzwerkeffekten oder bei höheren Wechselkosten ist hingegen klassisch eine kritische Masse notwendig, um eine Adaption bzw. den Wechsel für weitere Nutzer lohnenswert zu machen (vgl. Rohlfs, 1974). Dennoch bleibt in beiden Fällen eine Problematik kollektiven Handelns bestehen, wie im folgenden Kapitel weiter diskutiert wird.

4.1.3.2 Multi-Homing und Wechselkosten

Jüngste Entwicklungen im Zusammenhang mit WhatsApp zeigen, dass Verbraucher gewillt sein können, alternative Dienste zu nutzen. Laut Medienangaben installierten mit der Umsetzung neuer Datenschutzrichtlinien und Nutzungsbedingungen seitens WhatsApp zu Beginn des Jahres 2021 Millionen von Nutzern alternative Dienste wie Telegram, Signal oder Threema (Taş et al., 2021). Die Daten der jährlichen Erhebung des WIK zeigen ebenso einen Anstieg in der Nutzung dieser Dienste (siehe Abbildung 4-5) wie die Verbraucherbefragung der Bundesnetzagentur (2022), die zudem starke Zuwächse bei Discord sowie den Videokonferenzdiensten Zoom und Microsoft Teams feststellt. Der Anteil der Nutzer von WhatsApp ging im Vergleich zu 2020 leicht zurück.

Abbildung 4-5: Nutzeranteile ausgewählter Online-Kommunikationsdienste



Quelle: WIK-Consult. Sonderauswertung der jährlichen Umfrage des WIK. 2020: N=3.090. 2021: N=3.178. Deutsche Bevölkerung ab 18+ Jahre. *bezogen auf direkte Nachrichten, die gesendet oder empfangen wurden (direct messages). **keine Referenzwerte für 2020 vorhanden.

Fallbeispiel Switching & Multi-Homing: Änderung der Datenschutzbestimmungen bei WhatsApp

Trotz einer gestiegenen (parallelen) Nutzung alternativer Dienste und bekundeter Wechselbereitschaft, verließ letztendlich nur ein sehr geringer Teil von Nutzern (0,5%) den Dienst WhatsApp tatsächlich. Griggio et al. (2022) untersuchten gezielt die Wechselbereitschaft und -aktivitäten von WhatsApp-Nutzern nach der Änderung der Datenschutzbestimmungen empirisch.

Griggio et al. (2022) führten zwei Befragungen im Abstand von 2 Monaten durch. Im Februar und Mai wurden 1525 WhatsApp-Nutzer in Mexiko, Spanien, Südafrika und dem Vereinigten Königreich zur ihren Wechselplänen befragt. Etwa 25% der Befragten gaben an, zumindest Teile ihrer Kommunikation von WhatsApp auf andere Apps verlagern zu wollen. Jedoch waren weniger als ein Viertel der Nutzer der Ansicht, dass sie zumindest in gewissem Maße bei ihrem Vorhaben erfolgreich waren, und fast die Hälfte war unzufrieden mit ihrer derzeitigen Situation. Bis Mai hatten 27 % ihre Nutzung anderer Apps erhöht, und nur 16 % nutzten WhatsApp weniger. Einer der

Gründe, warum die Befragten weiterhin an WhatsApp festhielten, war, dass nicht genügend ihrer Kontakte auf die alternativen Dienste mitgewechselt sind. Abgesehen von den Netzwerkeffekten, fiel es den Nutzern schwer, eine fundierte Wahl zwischen alternativen Apps zu treffen, die sich mitunter in den Datenschutzrichtlinien, im Design und ihren Funktionalitäten unterschieden. Durch diese Unterschiede entstehen ebenfalls Kosten, da sich die Nutzer mit den Richtlinien befassen, an die neue Oberfläche gewöhnen und möglicherweise an die verschiedenen Möglichkeiten der Kommunikation anpassen müssen. Zuletzt bringt für einige Befragte ein Wechsel auch den Verlust der Kontrolle über die Separation von Kontakten auf verschiedene Dienste mit sich. Insgesamt haben nur etwa 0,5% der Teilnehmer WhatsApp tatsächlich deinstalliert. Griggio et al. (2022) schließen daraus, dass es für Verbraucher einfach ist zusätzliche Dienste zu installieren und zu nutzen, einen Dienst tatsächlich vollständig zu verlassen ihnen jedoch weniger leicht fällt.

Einen weiteren möglichen Grund dafür stellt die Verbreitung von Gruppenchats z. B. innerhalb von Schulklassen oder Sportgruppen und anderen Vereinen dar. Dabei spielt auch das klassische „**collective action“ Problem (Problem des kollektiven Handelns)** beim Wechsel zwischen Netzwerken eine wichtige Rolle. Da in diesem Fall nicht nur einzelne Gesprächspartner, sondern direkt ganze Gruppen zum Wechsel überzeugt werden müssten, ist hier auch von **„kollektiven Wechselkosten“** die Rede (vgl. Shapiro und Varian, 1998a). Die bisherige Forschung zur Nutzung von Kommunikationsdiensten hat jedoch gezeigt, dass die meisten Verbraucher mehrere Dienste aus unterschiedlichen Gründen nutzen. Diese reichen vom Zugang zu verschiedenen Funktionen über Bequemlichkeit bis hin zur Möglichkeit, unterschiedliche soziale Gruppen zu erreichen. Dies deutet darauf hin, dass horizontale IOP aus dieser Hinsicht nicht erforderlich ist. Die jüngste Untersuchung des WIK bestätigt dies und zeigt, dass die Nutzung mehrerer Kommunikationsdienste durch Produktdifferenzierung, Innovation sowie einen heterogenen Kreis von Kontakten angeregt wird (Taş et al., 2021). Die Studie stellt weiter fest, dass die Anzahl der genutzten Kommunikationsdienste mit der Anzahl an sozialen Gruppen, mit der Verbraucher privat interagieren, ansteigt.

In den Kommunikationswissenschaften existieren mehrere Ansätze, die die Wahl sowie die Nutzung mehrerer Kommunikationskanäle erklären. In der Channel Complementarity Theory nach Dutta-Bergman (2004) wird beispielsweise postuliert, dass Individuen, die Kommunikationskanäle zur Befriedigung eines bestimmten zwischenmenschlichen oder instrumentellen Bedürfnisses auswählen, auch andere Kanäle nutzen, um dieselben Bedürfnisse zu erfüllen (Dutta-Bergman, 2004; Ruppel et al., 2017). Kommunikationskanäle werden damit zumeist auf eine komplementäre Weise genutzt.

Die Art der Beziehung mit den Kommunikationspartnern hat daher ebenfalls einen Einfluss auf die Nutzung von Kommunikationskanälen. Arnold und Schneider (2017) untersuchten die Wahl von Kommunikationsdiensten anhand semi-strukturierter Interviews mit Nutzern. Die Teilnehmer verbinden verschiedene Kommunikationsdienste mit bestimmten sozialen Kontaktgruppen. So betonten einige Teilnehmer, dass WhatsApp und Snapchat eher für enge Kontakte reserviert sind; über Facebook und / oder Facebook Messenger hingegen vermehrt mit Bekannten kommuniziert wird, zu denen die Teilnehmer keine enge Beziehung pflegen. Arnold et al. (2020) bestätigen diese Ergebnisse in einer umfangreichen empirischen Studie, die insgesamt 22 Online-Kommunikationsdienste, traditionelle ECS und E-Mail als Kommunikationskanäle miteinander vergleicht. Sie fanden dabei heraus, dass die Individuen proaktiv die Grenzen zwischen Kommunikationsdiensten nutzen, um ihre sozialen Kontakte je nach Beziehungsnähe aufzuteilen.

Im Social Media Kontext verdeutlichen Tandoc et al. (2019) ebenfalls, dass Nutzer sozialer Medien zum Zweck des Beziehungsmanagements mehrere Plattformen verwenden und zwischen diesen hin und her wechseln. Der Wechsel zwischen verschiedenen Plattformen ermöglicht Nutzern, ihre Netzwerke zu segmentieren und sozial abzugrenzen. Dies kann auch das Handling von Kontakten, Nachrichten und entsprechender Benachrichtigungen („Notifications“) erleichtern. Damit einhergehend oder alternativ können Dienste und damit Kanäle auch der thematischen Aufteilung dienen, z. B. entsprechend Beruf, Schule, Sport oder anderen Hobbies.

Quan-Haase und Collins (2008) und Nouwens et al. (2017) beschreiben zum einen den Wunsch der Verbraucher, selbst zu bestimmen, von wem und über welchen Dienst sie kontaktiert werden, und zum anderen den Aufwand, den sie betreiben, um die Kontrolle darüber zu behalten. Quan-Haase und Collins (2008) führten Interviews und Fokusgruppen mit Studenten in Kanada zum Thema Online-Präsenz und soziale Verfügbarkeit beim Instant Messaging. Einige Teilnehmer beschrieben, dass undifferenzierte und lange Kontaktlisten problematisch sein können, wenn die Person nicht für jeden Kontakt im gleichen Maße über den Instant Messenger erreichbar sein möchte. Ein paar der Teilnehmer lösten das Problem, indem sie neue Listen mit ausgewählten Kontakten erstellten. Andere wiederum blockierten oder löschten Kontakte, mit denen sie nicht über den Dienst interagieren wollten. Nouwens et al. (2017) verdeutlichen ebenfalls, dass Verbraucher ihre Kontakte für Kommunikationsdienste kontrollieren und monitoren und sich einzelne Verbraucher unwohl fühlen, wenn sie von Kontakten über einen Kommunikationskanal kontaktiert werden, der diesen nicht zugeordnet ist. Angesichts der Möglichkeit der IOP von Kommunikationsdiensten beschrieben die Teilnehmer der Studie von Arnold und Schneider (2017) das Gefühl, ihrer Privatsphäre beraubt zu werden. Die Teilnehmer gaben an, zu befürchteten, dass selbst Kontakte, zu denen eine lockere Beziehung gepflegt wird, plötzlich in die Bereiche eindringen könnten, die für engere Beziehungen vorbehalten sind.

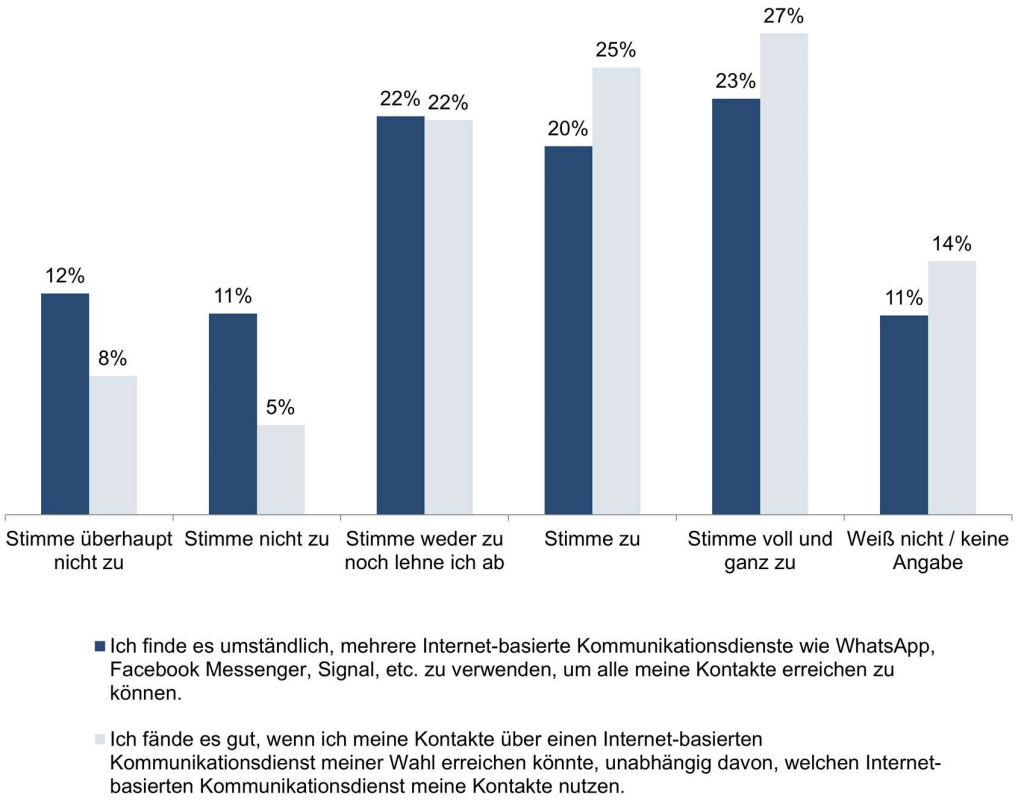
Es lässt sich allgemein schlussfolgern, dass der Grad von Multi-Homing am Markt somit stark davon abhängt, wie Nutzer soziale Gruppen voneinander abgrenzen und welche

Dienste sie für die Kommunikation mit den einzelnen Gruppen präferieren. Je unterschiedlicher die Einstellungen und Präferenzen eines Kommunikationspartners sind, desto höher ist tendenziell die Anzahl an Kommunikationsdiensten, die verwendet werden.

Ein anderer Grund für Multi-Homing kann der Zugang zu verschiedenen Funktionalitäten sein. Obwohl die meisten Online-Kommunikationsdienste und traditionelle ECS die gleichen Grundfunktionen gewährleisten, stellen einzelne Dienste auch einige Nischenfunktionen bereit, die für Konsumenten durchaus attraktiv sind. Taş et al. (2021) zeigen, dass den Befragten, die mindestens zwei Dienste verwenden und somit Multi-Homing betreiben, der Zugang zu einer großen Anzahl an verschiedenen Funktionen und unterschiedlichen Kommunikationsformen sowie die Auswahl an Bildern, Skins und Emoticons wichtiger ist als den Konsumenten, die nur einen Kommunikationsdienst verwenden.

Weil die Nutzung von Online-Kommunikationsdiensten selten mit monetären Kosten verbunden ist, ist auch die Hürde für Verbraucher, einen oder mehrere dieser Dienste zu nutzen, besonders gering. Nichtsdestotrotz ist Multi-Homing mit Kosten verbunden. Diese entstehen vor allem durch das Managen verschiedener Dienste. Laut den Ergebnissen der jährlichen Befragung des WIK zur Nutzung von Kommunikationsdiensten, die zuletzt Ende 2021 durchgeführt wurde, empfinden viele Befragte den Umgang mit mehreren internetbasierten Kommunikationsdienste, um die eigenen Kontakte zu erreichen, als umständlich (siehe Abbildung 4-6). Damit geht auch einher, dass Befragte es tendenziell bevorzugen würden, wenn Sie ihre Kontakte über einen internetbasierten Kommunikationsdienst ihrer Wahl kontaktieren könnten, unabhängig davon, welchen Dienst ihre Kontakte nutzen. Wenn sich die Kategorisierung sozialer Gruppen und die Präferenzen für die genutzten Dienste je Gruppe im Kontaktkreis stark unterschiedet, kann dies durchaus die Nutzung von internetbasierten Kommunikationsdiensten verkomplizieren. Insgesamt sind 43% der Meinung, dass die Nutzung mehrerer Online-Kommunikationsdienste umständlich ist, während etwa 52% IOP begrüßen würden, jedenfalls dann, wenn sie die kontaktierende Person sind.

Abbildung 4-6: Einstellung zu Multi-Homing



Quelle: WIK-Consult. Sonderauswertung der jährlichen Umfrage des WIK. 2021: N=3.178. Deutsche Bevölkerung ab 18+ Jahre. Basis: Nutzer ausgewählter Online-Kommunikationsdienste.

4.1.3.3 Überblick Funktionalität inkl. Aktuelle Entwicklung

Online-Kommunikationsdienste erlauben eine vielfältige und reichhaltige Kommunikation; nicht zuletzt durch die Vielzahl an unterschiedliche Funktionen, die diese Dienste bereithalten. In den vergangenen Jahren haben einzelne Dienste ein breites Repertoire an unterschiedlichen Funktionalitäten eingeführt. Insgesamt scheinen sich die Online-Kommunikationsdienste immer stärker zu umfassenden Plattformen zu entwickeln (Taş und Arnold, 2019). Bereits 2020 besaßen Dienste wie WeChat, Facebook Messenger und KakaoTalk deutlich mehr als 20 verschiedene Funktionen. WIK hat 2020 weltweit 180 internetbasierte Kommunikationsdienste untersucht. Abbildung 4-7 zeigt die Verteilung der identifizierten 35 Funktionen über die betrachteten Online-Kommunikationsdienste. Nahezu alle Dienste ermöglichten zu diesem Zeitpunkt das Versenden von Textnachrichten (98%). Funktionen, die audiovisuelle Kommunikation erlauben, waren ebenfalls weit verbreitet. Knapp 77% der Dienste erlaubten das Versenden von Bildern; 54% das Senden von Videos. Telefonie oder Videotelefonie wurde von etwa 46% bzw. 36% der Dienste ermöglicht. Neben diesen primären Kommunikationsfunktionen wurden von

einigen Diensten auch andere Funktionen ermöglicht. Etwa 13% der Dienste gingen Partnerschaften mit anderen Plattformen ein; es war zum Beispiel möglich, Ride- oder Carsharing Dienste über einzelne Online-Kommunikationsdienste zu buchen. Wiederum 5-7% der Dienste erlaubten das Tätigen von Zahlungen oder Geldtransfer. 6-7% der betrachteten Dienste integrierten die Funktion des Screen-Sharings oder die Sendung von selbstlöschenden Nachrichten in ihr Angebot. Im Durchschnitt hatten internetbasierte Kommunikationsdienste im Jahr 2020 etwa 10 Funktionen. Im Jahr 2016 hatte WIK-Consult in einer vergleichbaren Erhebung im Durschnitt nur 8 Funktionen erfasst (Arnold et al., 2017). Der steigende Trend scheint anzuhalten, wie beispielsweise neue Reaktions- sowie Businessfunktionen unter WhatsApp (WhatsApp, 2022), eine stärkere Integration der Messagingfunktion auf Instagram (Instagram, 2022) oder die Bestrebungen von Apple und Meta im privaten Zahlungsverkehr aufzeigen.

Abbildung 4-7: Funktionen von internetbasierten Kommunikationsdiensten weltweit

Lesehilfe: Die Schattierungen geben ein Indiz für den Anteil der betrachteten 180 internetbasierten Kommunikationsdienste, die jeweils eine Kombination der waagerecht und senkrecht aufgelisteten Funktionen zur Verfügung stellen. Je dunkler die Fläche, desto höher ist der Anteil der spezifischen Kombination von Funktionen. Die Diagonale gibt an, wie häufig die jeweilige einzelne Funktion in unserer Datenbank von internetbasierten Kommunikationsdienste angeboten wird.

Quelle: Eigene Darstellung; Daten stammen aus einem fortwährenden Monitoring des Marktes für internetbasierte Kommunikationsdienste (Stand: 2020).

Wie soeben beschrieben gehören Textnachrichten und Funktionen, die eine direkte Kommunikation ermöglichen, zum Standardrepertoire internetbasierter Kommunikations-

dienste. Bei den Konsumenten sind daneben auch das Versenden von Bild- und Sprachnachrichten besonders beliebt. Laut einer Umfrage, die Taş und Arnold (2019) veröffentlichten, nutzen diese Funktionen jeweils etwa 60-72% der Konsumenten in Deutschland.

Tabelle 4-1: Nutzungsanteile unterschiedlicher Funktionen

Funktionen – Gesamt	
Bildnachrichten	72,1%
Sprachnachrichten	60,8%
Empfangs- und Lesebestätigung	59,2%
Profilbild	58,4%
Gruppenchat	48,7%
Sprach- und/oder Videotelefonie	42,4%
Status, Stories, Day, Mood, Moments etc.	40,5%
„Zuletzt online"-Funktion	38,4%
Videobotschaften	35,4%

Quelle: Taş und Arnold (2019), S. 38.

4.1.3.4 Geschäftsmodelle

Nicht zuletzt durch verschiedene zugrundeliegende Firmenstrukturen unterscheiden sich verschiedene Messaging-Dienste stark in ihren Monetarisierungs- bzw. Geschäftsmodellen (Bundeskartellamt, 2021). Einige Dienste bzw. die entsprechenden Apps werden gegen direkte Einmal- oder regelmäßige Zahlungen verkauft (Threema, Element), während die Nutzung vieler anderer Dienste zunächst entgeltfrei ist. Hierbei gibt es wiederum grundlegende Unterschiede, so wird das Signal-System durch ein stiftungs- und spendenbasiertes Modell finanziert, während für andere Dienste verschiedene sekundäre direkte oder indirekte Einnahmen generiert werden sollen oder in Planung sind. Nicht nur in Bezug auf juristische Definitionen (vgl. Kapitel 4.1.1), die auf eine Leistungserbringung „*gewöhnlich* gegen Entgelt" abzielen, bleibt der Umgang mit anderen Formen der Finanzierung häufig unklar. In der Regel scheint ein Einbezug von Diensten mit Formen indirekter Einnahmen aber nötig, z. B. durch eine „Bezahlung" mit eigenen Daten der Verbraucher oder durch Synergien bzw. Quersubventionierungen mit anderen unternehmensinternen Diensten oder Hardware (vgl. auch Kapitel 4.1.3.5).

Von Meta wird aktuell unter anderem das Angebot einer Business-API für die Kommunikation zwischen Firmen und Endverbrauchern ausgeweitet (WhatsApp, 2022). Dies ist auch via Telegram möglich, findet allerdings bisher ebenso ohne eine Provisionsleistung für Telegram statt wie die Zahlungsfunktion die zwischen Nutzern und Unternehmen ermöglicht wird. Daneben findet sich auf Telegram mittlerweile die Möglichkeit, Werbung in öffentlichen Kanälen zu schalten (Telegram, 2022), außerdem sollen hier entsprechend eines Freemium-Modells, das beispielsweise auch Twitch oder Discord verfolgen, über das weiterhin kostenlose Basisangebot hinausgehende Features zum Kauf angeboten werden (Clover, 2022).

In der Einschätzung wettbewerblicher Konstellationen und der Bewertung möglicher Maßnahmen sollten entsprechend weder einzelne Dienste aufgrund ihrer (ggf. scheinbar fehlenden) Monetarisierungsstrategie übersehen werden, auf der anderen Seite müssen aber auch stets mögliche besondere Aspekte und Risiken jedes Geschäftsmodells in Betracht gezogen werden. Insbesondere Werbemodelle, die auf Aufmerksamkeit und/oder Daten von Nutzern basieren, bringen eine erhöhte Komplexität mit sich. Durch die Geschäftsseite der Werbenden kommt eine zusätzliche Partei ins Spiel, durch die spätestens dann eine Plattform im klassischen ökonomischen Sinne entsteht und zu Wechselwirkungen bzw. indirekten Netzwerkeffekten gegenüber der Nutzerseite führt. Außerdem sind aus der Literatur verschiedene kognitive Verzerrungen, z. B. im Kontext von Datenfreigabe (Kokolakis, 2017) oder dem „zero-price“ Effekt (Shampanier et al., 2007) bekannt, die zu einer erhöhten Vulnerabilität auf Nutzerseite führen können. Auch kann es zu sekundären Fehlanreizen auf gesellschaftlicher Ebene kommen, wenn z. B. Polarisierung und Desinformation zu gesteigerter Aufmerksamkeit (und damit ggf. Werbeeinnahmen) führen (Marsden et al., 2020).

4.1.3.5 Ökosysteme & vertikale Integration

Darüber hinaus können einzelne Dienste zwar primär einer Dienstekategorie (hier: Messenger) zugeordnet werden, sind aber eigentlich nur als eine Wertschöpfungsstufe in einem weitreichenderen vertikal integrierten Ökosystem anzusehen. Dieser Fall wird in Abbildung 4-8 verdeutlicht. Dabei zeigen die farblich hinterlegten Zellen die Wertschöpfungsstufen an, in welchen die jeweiligen Unternehmen aktiv sind. Im Fall von Messaging-Diensten konkurrieren beispielsweise Dienste welche primär auf derselben Stufe der Wertschöpfung vertreten sind (Firma B & C, z. B. Threema, Signal) auch mit Messaging-Diensten, die Teil einer vertikal Integrierten Wertschöpfung (Firma A, z. B. WeChat) sind.

Abbildung 4-8: Horizontale IOP (Stufe 3) mit einer vertikal integrierten Plattform (Firma A)

	Firma A	Firma B	Firma C
Stufe 3			
Stufe 2			
Stufe 1			

Insbesondere in Fällen in denen einzelne Marktteilnehmer, welche sich auf einer Wertschöpfungsstufe in horizontalem Wettbewerb befinden, weitere vertikale Verflechtungen haben, können sich komplexe Abhängigkeiten und damit neben der reinen Netzwerkgröße auch andere Hebel zur Ausübung von Marktmacht ergeben. Für Firmen gibt es in diesen Fällen die Möglichkeit Kollusion über die Grenzen einzelner Segmente oder Märkte hinaus zu stabilisieren und das eigene Level von IOP strategisch in Abhängigkeit

der Häufigkeit des Kontakts mit anderen Firmen zu wählen (Choi und Gerlach, 2013). Ein entsprechendes Beispiel wird in Abbildung 4-9 verdeutlicht. Im Fall von Messengern stehen auch mehrere Dienste von vertikal integrierten Anbietern (z. B. iMessage, Facebook Messenger) in Konkurrenz zueinander. Die Anbieter dieser Dienste haben daher auch Kontakt zu ihren Konkurrenten in anderen Teilen der Wertschöpfungskette und auf anderen Märkten.

Abbildung 4-9: Horizontale IOP (Stufe 3) mit Multi-Marktkontakt (Stufe 2) von Firmen A und B

	Firma A	Firma B	Firma C
Stufe 3			
Stufe 2			
Stufe 1			

Insbesondere im Falle der verbreitetsten Messaging-Dienste ist die häufig fehlende direkte Monetarisierung (vgl. Kapitel 4.1.3.4) durch die dahinterstehenden Multiprodukt-Ökosysteme bedingt. Im deutschen und englischsprachigen Raum stehen hier der Meta-Konzern mit den zugehörigen Messaging-Diensten bzw. -funktionen WhatsApp, Facebook Messenger und Instagram sowie iMessage aus dem Hause Apple im Vordergrund. So wurde z. B. Meta eine Verknüpfung der Daten von WhatsApp mit den entsprechenden Facebook- und Instagramkonten vorgeworfen (vgl. Bundeskartellamt, 2019), um die dort erfolgenden Werbeeinnahmen steigern zu können. Ein anders gelagertes Beispiel für eine Quersubventionierung stellt auch iMessage dar, das fest in das Betriebssystem von Apple verankert ist. Insbesondere im amerikanischen Markt wird neben einer einfachen und integrierten Handhabung über das Betriebssystem hinweg nicht zuletzt auch der exklusive Charakter des hauseigenen Messaging-Dienstes aktiv für die Kaufentscheidung zur iPhone-Hardware beworben (Higgins, 2022).

Auch wenn ein Messaging-Dienst durch die Beschränkung auf direkte Netzwerkeffekte für sich gesehen also nicht die klassische Definition einer Plattform im ökonomischen Sinne erfüllt, ist dieser Markt in der Praxis doch durch „echte“ Plattformen geprägt, da durch die Einbettung in Plattformökosysteme verschiedenartige Formen indirekter Netzwerkeffekte ebenfalls eine essenzielle Rolle einnehmen können.

Die Bewegung hin zur Prävalenz von Ökosystem-Messengern erfolgt dabei insbesondere international gesehen aus beiden Richtungen: ursprüngliche Single-Purpose Messenger werden durch hinzukommende Funktionalitäten, Monetarisierungsarten und Firmenausrichtungen selbst zu Plattformen und/oder Ökosystemen, während bestehende multi-sektoral agierende Ökosysteme ihr Portfolio um Messaging-Funktionen erweitern (RTR, 2020).

4.1.4 Status quo & Positionen zu Interoperabilität

Laut Julia Weiss, Sprecherin von Threema, besteht die Sorge, dass IOP die Position von dominanten Anbietern zementieren würde, anstatt Marktbestreitbarkeit herzustellen: „Wenn bestehende Nutzer des kostenlosen Messengers A mit schlechten Datenschutzpraktiken mit Nutzern des datenschutzbewussten, kostenpflichtigen Messengers B kommunizieren könnten, würden sie kein Geld für den Messenger B bezahlen und ihn damit seiner einzigen Einnahmequelle berauben" (Meaker, 2022). Auch Signal lehnte eine Zusammenarbeit bzw. IOP mit anderen Apps wie WhatsApp und iMessage zuletzt öffentlich ab und verwies auf eine mögliche Gefährdung der bestehenden Datenschutzstandards, unter anderem durch die entstehende Zugriffsmöglichkeit auf Metadaten (Reuter, 2022). In der Vergangenheit hat sich Signal bereits öffentlich gegen föderierte Systeme und für geschlossene, proprietäre Protokolle ausgesprochen (vgl. Marlinspike, 2016a).

Eine Reihe von Positionen sind in anonymisierter Form im Bericht des Bundeskartellamt (2021) zusammengefasst. Allgemein wird IOP als grundsätzlich erstrebenswertes Ziel anerkannt und auch auf eigene Bestrebungen hingewiesen, sei es die gemeinsame Entwicklung von Standards (z. B. MLS – Messaging Layer Security) oder zumindest interne Bestrebungen, IOP zwischen hauseigenen Diensten herzustellen (vgl. auch die von Meta angekündigte Verknüpfung der verschiedenen konzerneigenen Messaging-Dienste). Eine breite IOP-Verpflichtung bis hin zur Standardisierung wird aber größtenteils kritisch gesehen. Zu den genannten Risiken und Herausforderungen zählen mögliche negative Auswirkungen auf Differenzierungsmöglichkeiten und Innovation (vgl. auch Kapitel 3.3), Belastungen für kleinere Marktteilnehmer, wenn diese zu branchenweiten Vorgaben verpflichtet würden sowie die technische Umsetzbarkeit. Eine effektive breite IOP sei nur durch eine umfassende Standardisierung möglich, die aber wiederum eine eigene Reihe von Problemen mit sich bringen würde und extrem aufwendig sei. Einige Aspekte der technischen Umsetzbarkeit und der Standardisierung werden in den Kapiteln 4.2 und 4.3.1.1 aufgegriffen.

Laut einer Marktkonsultation in Großbritannien stehen Marktteilnehmer insbesondere IOP- und Datenverpflichtungen als Teil von sogenannten pro-kompetitiven Instrumenten durchaus positiv gegenüber (HM Government, 2022). Allerdings wird hierbei zunächst nicht weiter nach verschiedenen Arten und Abstufungen entsprechender Maßgaben aufgeschlüsselt.

Innerhalb der Branche zeigt sich insgesamt aber ein gemischtes Bild bezüglich verpflichtender IOP-Vorhaben im Messengerbereich. Insbesondere einer breiten IOP-Vorschrift auf horizontaler Ebene stehen viele Marktteilnehmer und -beobachter überwiegend kritisch gegenüber (s. z. B. Barczentewicz, 2022; Bundeskartellamt, 2021). Auf der anderen Seite gibt es auch eine Reihe von Stimmen, die gezielte IOP-Vorgaben nicht zuletzt auch für Messaging-Dienste als mögliches wichtiges Instrument zugunsten von Marktbestreitbarkeit und Wahlmöglichkeiten für Verbraucher ansehen. Dazu gehören neben For-

schenden (Crémer et al., 2019; Scott Morton und Kades, 2021) auch aktuelle Alternativanbieter wie Element und Beeper, die auf Basis des Matrix-Protokolls (Element (2022b), vgl. auch Kapitel 4.2.1 ff.) schon heute einen interoperablen Ansatz für Messaging-Dienste verfolgen, sowie Verbraucherorganisationen (Doctorow, 2019; EDRi, 2018) und auch Marktaufsichtsbehörden (ACCC, 2020; CMA, 2020).

4.2 Technische Grundlagen von Messaging-Diensten

Wie auch die zuvor dargestellten Positionen zeigen, liegt ein besonderes Augenmerk auf technischen und Datensicherheitsaspekten. Dabei wird häufig in Frage gestellt, ob die technischen Voraussetzungen für einen effizienten Funktions- und Datenaustausch im Sinne einer IOP für Messaging-Dienste überhaupt erreichbar sind. Die technische Komplexität von Messengern und insbesondere von einer von vielen Seiten angestrebten Ende-zu-Ende-Verschlüsselung scheinen sich daher zu einem neuralgischen Punkt für die Beurteilung und praktische Entwicklung von IOP-Anforderungen wie sie unter anderem im DMA zu finden sind zu entwickeln. Technische Voraussetzungen für einen effizienten Funktionalitäts- und Datenaustausch sowie die benötigten Daten für eine technisch praktikable und effiziente IOP-Implementierung bedingen sich dabei wechselseitig.

Am Markt gibt es aktuell eine Vielzahl von verschiedenen Messaging-Protokollen und Standardisierungsversuchen, von denen sich aber über die Jahre bisher keiner einheitlich durchsetzen konnte.

Rich Communication Services (RCS) ist ein Kommunikationsprotokoll zwischen Netzbetreibern und Smartphones, das die Standard-SMS-Dienste zum Senden und Empfangen von Nachrichten, nicht zuletzt auch als Fallback-Option für Online-Kommunikationsdienste, ersetzen sollte. Ursprünglich als Reaktion der Netzbetreiber auf die aufkommenden OTT-Messenger in separaten Applikationen mit Anbindung an Mobilrufnummer und Vertrag implementiert, ist es nach erfolglosen Versuchen seitens der meisten Netzbetreiber eingestellt worden und wurde inzwischen seitens Google als Netzbetreiber-unabhängiger Service in die Android Nachrichtenapp integriert (Bohn, 2019; Oestreich, 2018). RCS bietet neben der Übermittlung von Nachrichten über ein Datennetz auch Multimedia-Unterstützung, eine „schreibt gerade“-Anzeige („typing indicator“) und Gruppen-Chat-Funktionen. Aktuell nutzt Google eine RCS-Implementation für seine eigenen und Android-nativen Messaging-Apps und forderte zuletzt öffentlich Apple dazu auf, eine RCS-Unterstützung für iMessage zu implementieren. Trotz einseitiger Anstrengungen von Google, auf Basis des Signal-Protokolls eine Ende-zu-Ende-Verschlüsselung mit RCS für seinen Google Client zu implementieren (Google, 2022a)[28], wird RCS anderen möglichen Standards und Implementierungen gegenüber als unterlegen angesehen (CMA, 2021). Das Signal-Protokoll als möglicher Goldstandard für die Verschlüsselung bietet

[28] In der Standard-Implementierung von RCS ist keine Ende-zu-Ende-Verschlüsselung möglich oder vorgesehen, da es als Netzbetreiberdienst gilt und somit den „lawful interception“-Vorgaben unterliegt (Amnesty International, 2018).

die Grundlage für eine Reihe von Implementierungen und wird in Kapitel 4.2.4 näher beleuchtet. Die beiden freien Protokolle Matrix und XMPP stellen Beispiele für föderierte Systeme dar, die im folgenden Kapitel erläutert werden.

4.2.1 Architektur-Arten

Messaging-Dienste können zunächst hinsichtlich ihres Aufbaus in zentralisierte und dezentralisierte Architekturen[29] unterschieden werden, letztere wiederum in föderierte Systeme und Peer-to-Peer-Systeme.

Als **zentralisiert** sind solche Dienste zu definieren deren Funktionalität exklusiv von einem Anbieter bereitgestellt wird. Somit findet Kommunikation über zentralisierte Dienste immer über diesen Intermediär statt. Messaging-Dienste, die eine zentralisierte Architektur haben, wie beispielsweise WhatsApp, Facebook Messenger, Telegram und Signal, gehören zu den am meisten genutzten Messengern. Föderierte Systeme hingegen, hier in Form von **dezentralen** Messengern, bieten die Möglichkeit einen gleichartigen Dienst über mehrere Anbieter zu nutzen, ohne dabei auf die direkten Netzwerkeffekte zu verzichten. Matrix folgt als Messenger-Protokoll dem Ansatz einer auf mehrere Anbieter verteilten Kommunikationsmöglichkeit. Föderierte Systeme basierenauf einem standardisierten Protokoll und sind mit den klassischen Telekommunikationsdienstleistungen zu vergleichen, bei denen jeder Kunde einem Anbieter zugeordnet ist, über den er als Intermediär andere Nutzer erreichen kann. Dies gilt sowohl für Telefonanrufe als auch Kurznachrichten und bedingt zur reibungslosen Abwicklung einer eineindeutigen Telefonnummer zur Identifizierung. Auch die E-Mail als Kommunikationsmöglichkeit ist föderiert über die E-Mail-Provider aufgebaut und bietet über die Anbieterkennung ebenfalls eine eindeutige Identifizierung. An diesem Punkt setzt DeltaChat an, ein Messaging-Dienst, der auf der bestehenden E-Mail-Infrastruktur aufsetzt und so Messaging ermöglicht. Da dieser Dienst über das E-Mail-Protokoll IMAP realisiert wird, kommt er ohne separate Infrastruktur aus. Da IMAP als Protokoll jedoch für asynchrone Kommunikation konzipiert wurde, ergeben sich laut Grüner (2019) Problematiken hinsichtlich der Spam-Beschränkungen mancher Anbieter bei gehäuften Nachrichten innerhalb von kurzen Zeiträumen.

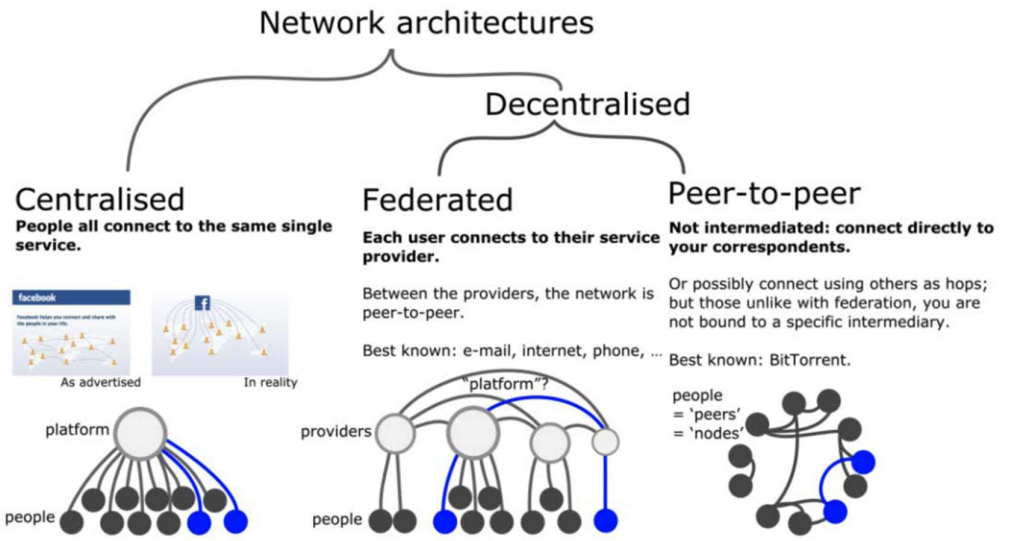
Ein dezentraler Messenger ohne vom Anbieter bereitgestellte Infrastruktur wird als Peer-to-Peer-Netzwerk realisiert. Während diese Methode insbesondere durch Filesharing-Netzwerke wie BitTorrent bekannt wurde, existieren im Anwendungsfall von Messaging-Diensten durch die zeitliche Asynchronität der Kommunikation besondere Schwierigkeiten. Insofern eine der Gesprächsparteien die Nachricht nicht unmittelbar in Empfang nehmen kann, steht bei dezentralen P2P-Netzwerken (Rechner-Rechner-Verbindung, engl. Peer-to-Peer) keine Infrastruktur zur temporären Speicherung zur Verfügung. Briar ist ein

29 Die Form der Architektur ist unabhängig von Infrastrukturen zu betrachten, so werden moderne digitale Dienste zwar im Sinne einer Lastverteilung oder geographischen Differenzierung dezentral vorgehalten, sind aber bezüglich der Erbringung der Dienste auf einen Dienstbetreiber zentralisiert.

solcher P2P-Messenger und baut zur Behebung dieses Problems auf eine selbstgehostete Mailboxstruktur (Briar, 2021). Diese Konzeption zeigt Ähnlichkeiten zu selbst-gehosteten E-Mail-Anwendungen, da auch in diesem Fall eine Client-seitige Synchronisierung mit permanent laufendem Server notwendig ist. Somit muss seitens des Nutzers eine eigene Infrastruktur bereitgestellt werden, insofern diese Funktionalität genutzt werden soll.

In Abbildung 4-10 werden, auf digitale Dienste generalisiert, die abnehmende Abhängigkeit von Nutzern gegenüber den Intermediären von zentralisierten über föderierte Systeme bis hin zur Abkehr von Intermediären in Form von P2P-Netzwerken visualisiert. Während sich bei zentralisierten Diensten alle Nutzer auf einen Intermediär konzentrieren, sind föderierte Systeme zweistufig aufgebaut. Neben der Interaktion mit dem eigenen Intermediär entsteht auf Ebene der Intermediäre ein Netzwerk der Intermediäre. Hierdurch entsteht ein „Netzwerk der Netzwerke“, womit allerdings interoperable Dienste via Standards oder Konverter notwendig werden.

Abbildung 4-10: Architektur-Arten von digitalen Netzwerken



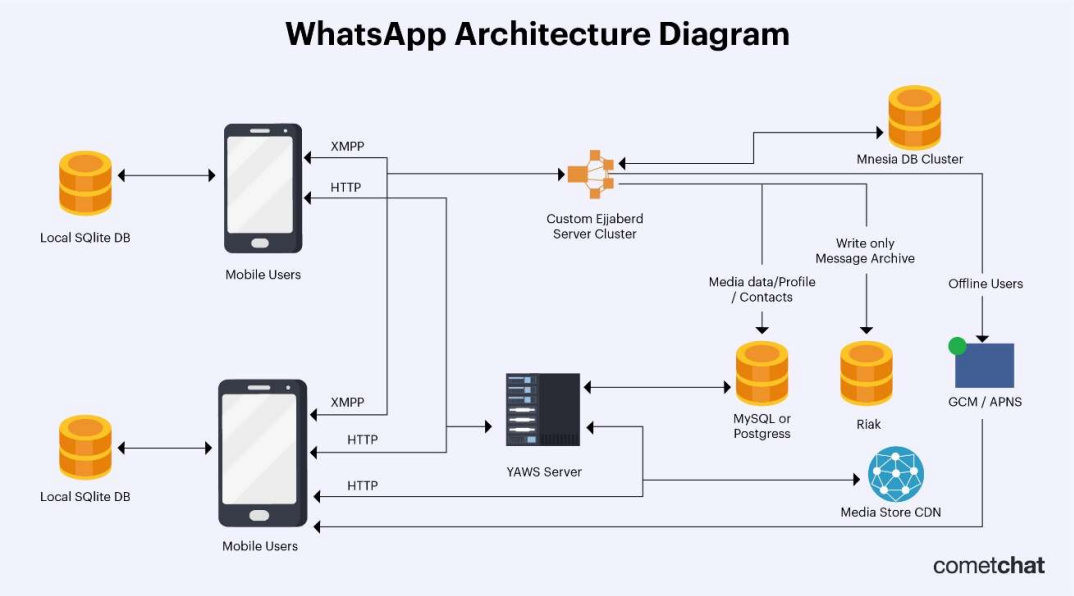
Quelle: Brown (2020, S. 8)

Neben der Art der Architektur unterscheiden sich die etablierten Messenger-Lösungen auch in der Ausgestaltung, weswegen exemplarisch an dieser Stelle der Aufbau von WhatsApp, Signal, Matrix und Briar dargestellt werden soll.

4.2.1.1 WhatsApp

WhatsApp wurde als Messenger 2009 entwickelt und ist seit der Übernahme 2014 Bestandteil des Meta-Ökosystems. Serverseitig basiert WhatsApp auf der Programmiersprache Erlang und nutzte FreeBSD als Betriebssystem. WhatsApp nutzt als Text-Kommunikationsprotokoll und für den Serverbetrieb angepasste Versionen von FunXMPP und ejabberd. Dabei ist anzumerken, dass sowohl FreeBSD als auch ejabberd und FunXMPP grundsätzlich Open Source sind, FunXMPP sogar eine Iteration eines standardisierten Kommunikationsprotokolls darstellt. Durch Änderungen von WhatsApp aus Gründen der Performance und vermutlich auch strategischen Überlegungen sind diese jedoch proprietär und somit nicht mehr ohne adversariales Reverse Engineering reproduzierbar. Diese einseitige Anpassung, aus der eine Inkompatibilität mit den ursprünglichen Standards entsteht, wird von Simcoe und Watson (2019) als strategische Entscheidung und Koordinationsproblem untersucht. Sie verweisen auf die strategische Abschirmung der eigenen Nutzergruppen durch die Implementation inkompatibler Kommunikationsprotokolle in den Anfängen des Instant Messagings. Dateien werden bei WhatsApp über das Protokoll HTTP und eine separate Server-Struktur versendet. Abbildung 4-11 stellt die WhatsApp zugrunde liegende Serverstruktur dar.

Abbildung 4-11: Schematische Darstellung der WhatsApp-Architektur



Quelle: Cressler (2021)

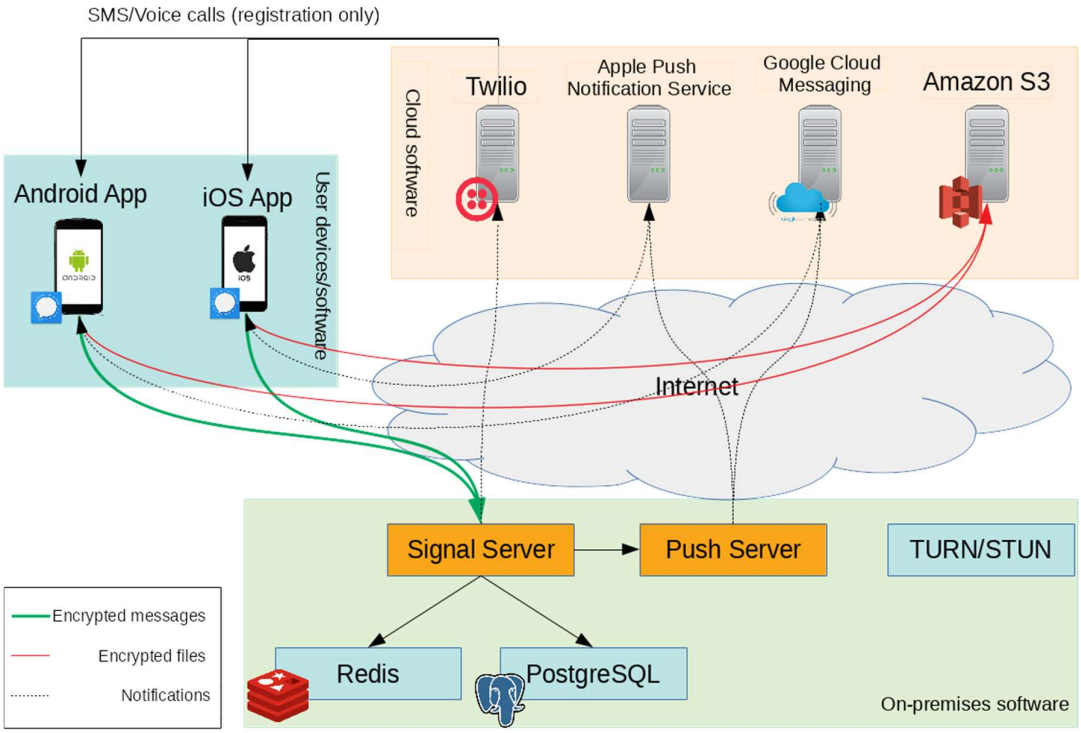
Cressler (2021) verdeutlicht damit die Trennung der Struktur für textbasierte Kommunikation und den Versand von Daten, was sich aus den unterschiedlichen Anforderungen der Teildienste hinsichtlich Speicherung und Senden ergibt. Laut Eugene Fooksman liegt

die Wahl einer stark Erlang-basierten Technologie mit ejabberd, Mnesia und YAWS in der Skalierbarkeit dieses Aufbaus (D'Incau, 2013).

4.2.1.2 Signal

In Abbildung 4-12 wird die grundsätzliche Infrastruktur von Signal dargestellt, aus der ebenfalls ein geteilter Infrastrukturaufbau ersichtlich wird. Um eine Verifizierung von Nutzern zu ermöglichen, nutzt Signal Twilio zur SMS-Verifizierung[30] neben den betriebssystembedingten Push-Servern von Apple und Google für App-Benachrichtigungen. Für die Zwischenspeicherung von noch zuzustellenden Inhalten verwendet Signal zudem die Cloud-Infrastruktur (S3) von Amazon Web Services.

Abbildung 4-12: Schematische Darstellung der Signal-Architektur



Quelle: Cocorada (2018)

Die TURN/STUN-Server-Komponente ist zur Vermittlung der IP-Adresse von Audio-/Videoanrufen erforderlich, insofern keine direkte Verbindung hergestellt werden kann[31] (Anturix, 2018). Zum Speichern von unstrukturierten Daten verwendet Signal Redis als

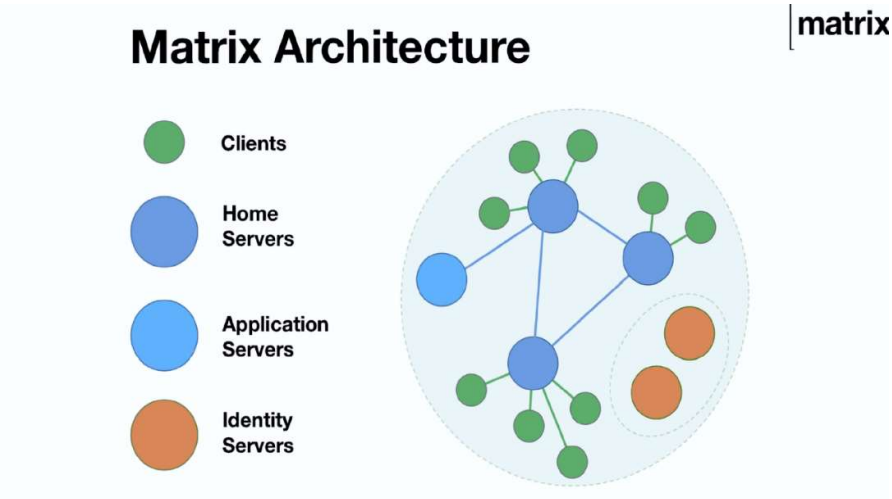
30 Hierzu: (Signal, 2021)
31 Laut dem Forumsbeitrag ist dies insbesondere notwendig, wenn sich das Mobiltelefon hinter einem NAT befindet. Dies ist üblicherweise im Kontext von geteilten öffentlichen IP4-Adressen (Carrier-Grade-NAT-IPv4-Adresse) der Fall.

nicht-relationale Datenbank und PostgreSQL für strukturierte Daten in einer relationalen Datenbank.[32] Durch die Veröffentlichung des Client- und Server-seitigen Quellcodes können die dargestellten Abhängigkeiten transparent eingesehen werden. Der Server und die Android-App sind in der Programmiersprache Java geschrieben und die iOS-App in Swift.

4.2.1.3 Matrix

Bei Matrix (Abbildung 4-13) handelt es sich durch die föderierte Struktur nicht um einen singulären Messaging-Dienst, sondern um ein Protokoll, das föderierte Messaging-Dienste ermöglicht. Dadurch ist die Struktur des Matrix-Systems in “Home-Server” strukturiert, welche von Nutzern, Gruppen oder Diensten betrieben werden und jeweils im Sinne eines E-Mail-Anbieters die digitale Infrastruktur liefern.

Abbildung 4-13: Schematische Darstellung der Matrix-Architektur



Quelle: Hodgson (2019)

Das gemeinsam verwendete Protokoll bietet hierbei die Möglichkeit die Netzwerkeffekte auch über den eigenen Home-Server hinaus zu realisieren. Der Logik von E-Mail folgend, entsprechen die vergebenen Matrix-IDs dem Muster “*@NAME:HOME-SERVER*” wodurch ein Zusammenhang zu Telefonnummern auch im Zuge von Registrationen vermeidbar wird. Um dennoch Identifikatoren außerhalb von Matrix mit den internen IDs zu

32 Detailliertere Informationen zu Datentypen und der Handhabung hinsichtlich Speicherung sind in Kapitel 3.6 zu finden.

verbinden, gibt es “Identity Server” die konzeptionell ähnlich dem Domain Name Resolver[33] eine Verbindung zwischen externem und internem Identifikator herstellen. Die Textnachrichten sind strukturierte Daten im JSON-Format und werden via HTTP und APIs zwischen den Instanzen ausgetauscht. Die APIs sind im Sinne dezentraler und nichtkoordinierter Update-Zyklen versioniert.

4.2.1.4 Briar

Briar hat entsprechend des dezentralen P2P-Ansatzes keine Infrastruktur, sondern basiert ausschließlich auf den Geräten auf denen Briar installiert ist. Um zwischen den Geräten eine Verbindung herzustellen und damit Kommunikation zu ermöglichen, nutzt Briar entweder die Funktechnologien WLAN und Bluetooth oder alternativ das Tor-Netzwerk. Eine Problematik von infrastrukturlosen Messengern ergibt sich, sobald ein Gesprächspartner nicht verbunden ist und keine Nachrichten zugestellt werden können. Während bei Gruppen die Mitglieder als “Hop” dienen können, die eine Nachricht bis zur Zustellung verwahren, ist dies bei bilateralen Gesprächen mit Kompromissen verbunden. Zur Lösung dieser Problematik gibt Briar zwei Ansätze an, einmal Nachrichten per “Multi-Hub” über die eigenen Kontakte zu senden oder die Nutzer eine Mailbox-Architektur selber bereitstellen zu lassen. Ersteres würde den Schutz der Metadaten dahingehend einschränken, dass zumindest die Kontakte erfahren, wann zwischen wem ein Kontakt stattfand. Eine individuell bereitgestellte Mailbox-Architektur erhöht den Aufwand für den Nutzer und sorgt für Ineffizienzen in der Infrastrukturbereitstellung. Für synchrone Kommunikation (z. B. Video-Chats) ist die Mailbox-Architektur zudem ungeeignet. Architekturbedingt ist der Funktionsumfang bei reinen P2P-Messengern daher eingeschränkt.

4.2.2 Quelloffenheit

Ein weiterer Aspekt der bei der Betrachtung des unterschiedlichen Aufbaus von Messaging-Diensten, zu berücksichtigen ist, ist die Quelloffenheit der Dienste. Im Kern stehen aus Sicht der Nutzer hierbei zwei Funktionen, die sich aus quelloffener Software ableiten lassen. Zum einen liefern Open-Source Programme eine Transparenz hinsichtlich der genauen Funktionsweise, welche externen Dienste kontaktiert werden und welche Verschlüsselung implementiert ist. Hieraus ergibt sich auch die Möglichkeit die Sammlung und Behandlung von Metadaten nachzuvollziehen. Zum anderen ermöglicht eine quelloffene Software, insofern nicht nur aus Transparenzgründen geschehen, die Infrastruktur eigenständig zu betreiben, womit die Autonomie der Nutzer gestärkt wird. Ist neben der reinen Quelloffenheit in der Veröffentlichungslizenz auch die Anpassung der Software vorgesehen, ist es den Nutzern neben dem reinen Betrieb einer eigenen Instanz auch

33 DNS-Server sind eine Art Adressbuch des Internets und dafür zuständig aus den sprachbasierten Internetadressen die zugeordnete(n) IP-Adresse(n) zu liefern.

möglich Anpassungen (unter Berücksichtigung des Standards) vorzunehmen oder weitere komplementäre Dienste anzubinden. Wie auch in Kapitel 3.6 teilweise erläutert, gibt es hier im Prinzip drei Klassifizierungen der Quelloffenheit:

- Proprietäre Systeme, die keinen Quellcode veröffentlichen und möglicherweise Sicherheitsaudits als Signal über die Qualität der Implementierung verwenden.
- Quelloffene Systeme, die nur aus Transparenzgründen den Quellcode veröffentlich, die Nutzung des Quellcodes aber untersagen.
- Open-Source Systeme, die in unterschiedlichen Graden die Nutzung und/oder Anpassung erlauben.

4.2.3 Datenschutz und -sicherheit

Die horizontale IOP zwischen denselben Arten von Anwendungen setzt ebenfalls voraus, dass bestimmte Nutzerdaten ausgetauscht werden, damit z. B. im Kontext von Messaging-Diensten Nachrichten und/oder Videoanrufe über mehrere Dienste hinweg funktionieren können. Hierbei sind nicht zwingend die eigentlichen Inhalte (ggf. Ende-zu-Ende-verschlüsselt), sondern vielmehr die anfallenden Metadaten relevant. Gegenwärtig haben sich die Verbraucher aus verschiedenen Gründen für bestimmte Messaging-Dienste entschieden, sei es aufgrund ihrer Funktionalität, ihrer Verbreitung, oder höherer Sicherheit und/oder einem besseren Datenschutzniveau. Diese Aspekte von Verbraucherinteressen, die sich mit horizontaler Differenzierung der Dienste abbilden, sind auch unter Souveränitätsaspekten bei der Ausgestaltung von IOP-Vorschriften zu berücksichtigen.

Dabei differenzieren sich Messaging-Dienste wie Threema oder Signal von anderen Diensten durch Aspekte der Sicherheit oder des Datenschutzes, wie eine Ende-zu-Ende-Verschlüsselung, keine Speicherung von personenbezogenen Daten nach der Zustellung auf eigenen Servern oder die generell ausbleibende Erhebung personenbezogener Daten. Horizontale IOP für Messaging-Dienste könnte die Sicherheitsstandards von Messaging-Diensten senken, da es schwierig ist, zwei unterschiedliche Verschlüsselungstechnologien und unterschiedliche Sicherheitsansätze vollständig und ohne Kompromisse in Einklang zu bringen.[34] Daher kann für die Kommunikation zwischen Messaging-Diensten als Kompromiss der kleinste gemeinsame Nenner auf niedrigeren Sicherheitsstufen nicht ausgeschlossen werden. Eine Befragung von Marktparteien durch das Bundeskartellamt bestätigt diese Vermutung insbesondere im Hinblick auf eine Ende-zu-Ende-Verschlüsselung da es unmöglich sei, diese „... unter IOP beizubehalten. Dazu müssten alle Anbieter der interoperablen Funktionen das gleiche Protokoll verwenden.“

34 Hierunter können die Speicherung der Kommunikation auf Servern, das Senden von Daten in die Cloud oder nur auf Servern im jeweiligen Land und das Erfordernis einer persönlichen Identifizierung für das Abonnement fallen.

(Bundeskartellamt 2021).[35] Auch von WIK-Consult befragte Experten teilten letztendlich die Einschätzung, dass es ohne vollständige Standardisierung bzw. Einigung auf einen einheitlichen Verschlüsselungsstandard keine Ende-zu-Ende-Verschlüsselung unter Messenger-IOP geben könne. Aspekte der Ende-zu-Ende-Verschlüsselung werden im folgenden Kapitel noch einmal gesondert aufgegriffen.

Einem kürzlich erschienenen Artikel zufolge haben große Messaging-Unternehmen wie Google und Apple bereits ihre Bedenken geäußert, dass IOP unnötige Datenschutz- und Sicherheitslücken schaffen könnten (Wooden, 2022).

Darüber hinaus können Anwendungen, die mit einem datenschutzorientierten Messaging-Dienst interoperabel sind, persönliche Nutzerdaten erfassen, die zwischen den Anwendungen ausgetauscht werden, um die Kommunikation zwischen ihnen zu ermöglichen. Insgesamt hätten die Nutzer eines Dienstes wie beispielsweise Threema also den Vorteil, dass sie mit Nutzern anderer Anwendungen wie WhatsApp kommunizieren (also die Netzwerkeffekte nutzen) könnten, müssten gleichzeitig aber ihre Präferenzen hinsichtlich der gewählten Sicherheit und der Nichterfassung personenbezogener Daten zurückstellen, die vermutlich bedeutsam für die Wahl des alternativen Messengers waren.

Praktisch kann der gleiche Vorteil von Netzwerkeffekten für einen Nutzer durch Multi-Homing über die gleichzeitige Nutzung eines weiteren Dienstes erreicht werden. Aus Sicht der datenschutzbewussteren Anbieter, z. B. Threema oder Signal, ist diese horizontale IOP ebenfalls nicht vorteilhaft, da ihr Alleinstellungsmerkmal verwässert wird. In einer entsprechenden Befragung des Bundeskartellamts resümiert ein Anbieter, der sich insbesondere an Nutzer wendet, die auf Datenschutz großen Wert legen, „...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). Die Messaging-Dienste mit weniger Sicherheit und/oder mehr Personen- und Nutzerdatenerhebung würden hingegen profitieren, da sie noch mehr Daten als bisher erheben könnten.

Unabhängig von der im Folgenden diskutierten Verschlüsselung der Inhalte fallen beim Versand von Nachrichten eine gewisse Mindestmenge an Metadaten an. Die Registrierung bei Messaging-Diensten geschieht größtenteils unter der Preisgabe von freiwilligen Daten zur eineindeutigen Identifizierung, wenngleich Dienste existieren, die dies nicht zur Voraussetzung machen.[36] Insbesondere Telefonnummern eignen sich als gemeinsamer Identifikator, da diese im lokalen Adressbuch des Mobiltelefons häufig vorliegen und somit eine vergleichsweise einfache „Contact Discovery“ vorgenommen werden kann. „Contact Discovery“ ist ein relevanter Bestandteil der Usability von Messaging-Diensten,

35 Siehe V Ermittlungsergebnisse, 1. Interoperabilität, d) Auswirkungen von Interoperabilität, cc. Datensicherheit, Seite 64.

36 Auch wenn einige Dienste die Angabe der Telefonnummer als zwingende Voraussetzung deklarieren, besteht in der Akzeptanz dieser Voraussetzung eine freiwillige Entscheidung des Nutzers dies als Bestandteil der Nutzungsbedingungen zu akzeptieren.

da dies eine Voraussetzung ist, um die möglichen Gesprächspartner auf Basis des eigenen Adressbuchs zu erfassen. Hier besteht ein Zielkonflikt zwischen der Nutzbarkeit alle möglichen Kontakte zu erkennen, also dem sozialen Graphen eines Nutzers, und dem Datenschutz. Die Komplexität einer datenschutzfreundlichen technischen Umsetzung von „Contact Discovery“ wird im Kapitel 4.2.4 erläutert. Neben der Telefonnummer bietet sich die E-Mail-Adresse als alternative Möglichkeit an Nutzer zu identifizieren und eine Account-Wiederherstellung zu ermöglichen. Weitere freiwillige Daten, die vom Nutzer geteilt werden können, bestehen aus dem Vor- und Nachnamen oder alternativ eines Benutzernamens. Je nach Dienst bietet sich die Möglichkeit eines persönlichen Profilbildes, der Angabe von Geburtsdatum, Geschlecht oder Nationalität. Diese Angaben sind üblicherweise nicht verpflichtend. Insofern das Adressbuch des Gerätes geteilt wird, ist auch dies eine freiwillige Angabe des Nutzers, wenngleich je nach Handhabung des Datenschutzes seitens des Dienstes nicht zwingend alle Kontakte im Adressbuch damit einverstanden sind. Im Falle einer vollumfänglichen IOP wäre eine transparente Darstellung der Handhabung von Metadaten notwendig, sowie eine Abgrenzung, welche Metadaten von den Diensten der Kontakte gespeichert werden dürfen. Ist diese Abgrenzung unklar, besteht die Möglichkeit, dass die Metadaten von Nutzern datenschutzfreundlicherer Dienste über den Kontakt zu Nutzern anderer Dienste dennoch gespeichert werden.

Ein weiterer Teil der Daten, welche gesammelt werden können, fallen bei der Nutzung der App an und sind als beobachtbare Daten kategorisierbar. Dies sind zum einen Geräte- und Konfigurationsdateien und oder Standortdaten, also passiv erzeugte Daten. Unter beobachtbare Daten, welche aktiv durch die Nutzung anfallen, sind Gruppenmitgliedschaften und Nutzungsverhalten zu fassen. Insbesondere die Nutzungsdaten, wie Häufigkeit und Dauer der Nutzung, Zeitpunkte der Nutzung und Kontaktaufnahmen zu anderen Nutzern geben dem Anbieter Hinweise auf den Aufmerksamkeitsstrom und den „Social Graph“ seiner Nutzer. Das BSI (2021) hat die Klassifizierung von Metadaten in folgender Tabelle 4-2 zusammengefasst.

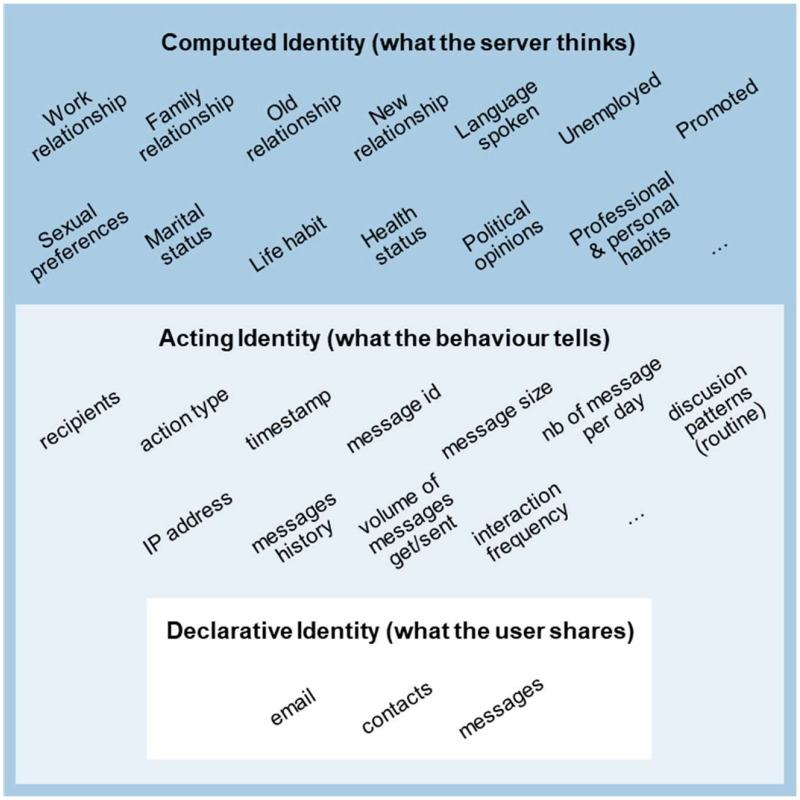
Tabelle 4-2: Klassifizierung von Metadaten moderner Messenger

Persönliche Daten: *Freiwillige Daten*	Profilbilder, Vor- bzw. Nachname des Nutzers, Benutzername oder Pseudonym (z. B. Nickname), Geburtsdatum, Alter, Geschlecht, Nationalität, E-Mail-Adresse, Telefonnummer, Kontoinformationen
Geräte- / Konfigurationsdaten: *Beobachtbare Daten*	IP-Adresse, Betriebssystem, Netzbetreiber, Gerätetyp, Geräte IDs, Benutzerkonten, Passwörter, Zertifikate, installierte Apps, Regions- und Spracheinstellungen
Standort- / Bewegungsdaten: *Beobachtbare Daten*	Aufenthaltsorte, Aufenthaltszeitpunkte, Aufenthaltsdauer, Bewegungsprofile
Kontakte / Daten Dritter: *Freiwillige Daten*	Kontaktverzeichnis, Adressbücher
Gruppenmitgliedschaften: *Beobachtbare Daten*	Teilnehmer oder Host in Chatgruppen, Telefonkonferenzen, Videokonferenzen
Nutzungsverhalten: *Beobachtbare Daten*	Häufigkeit und Dauer der Nutzung einer Messenger-App, Online-/Offline-Status, Browserchronik, Nutzung verschiedener Endgeräte, Zeitpunkte / Dauer / Teilnehmer eines Austauschs per Textnachricht / Telefonat / Videotelefonat

Quelle: BSI (2021); Einordnung der Freiwilligkeit/Beobachtbarkeit nach Crémer et al. (2019)

Eine der in Kapitel 4.1.3.4 dargestellten Monetarisierungsmöglichkeiten ist die indirekte Finanzierung über Werbung in anderen Diensten oder auf Plattformen. Um einen Nutzen aus den Informationen zu generieren, die im Zuge der Registrierung und bei der Verwendung angefallen sind, müssen diese verbunden und Personen zugeordnet werden. Pujol et al. (2019) definiert diese als unterschiedliche Grade der digitalen Identität und ordnet sie in deklarierte, darstellende und deduzierte Identitäten ein. Unter der deklarierten Identität fassen die Autoren die freiwillig geteilten Informationen zusammen. Dazu gehören entsprechend obiger Tabelle alle Informationen (Persönliche Daten, Kontakte/Daten Dritter), die der Nutzer freiwillig teilt. Die darstellende Identität erweitert dies um die beobachteten Informationen (Geräte- /Konfigurationsdaten, Standort- /Bewegungsdaten, Gruppenmitgliedschaften, Nutzungsverhalten). Bestandteil der Wertschöpfung ist jedoch die deduzierte Identität, also die Identität die aus den Modellen entsteht, die auf Basis der vorangegangenen Daten Erwartungen über die Eigenschaften und Charakterzüge der Nutzer bildet. Dazu gehört im Besonderen der soziale Graph der Nutzer, angereichert durch die Information der Häufigkeit von Kontaktaufnahmen. Auf Basis dieser ist es möglich ein iterativ angenähertes Abbild der Nutzer auf Basis dieser deduzierten Informationen zu bilden, welche für Kontaktvorschläge in sozialen Netzwerken und für die Personalisierung von Werbung bei Verbundprodukten genutzt werden können. Abbildung 4-14 visualisiert die Schnittmenge der graduellen Ausprägung von digitalen Identitäten.

Abbildung 4-14: Grade der digitalen Identitäten im Kontext von Messaging-Diensten

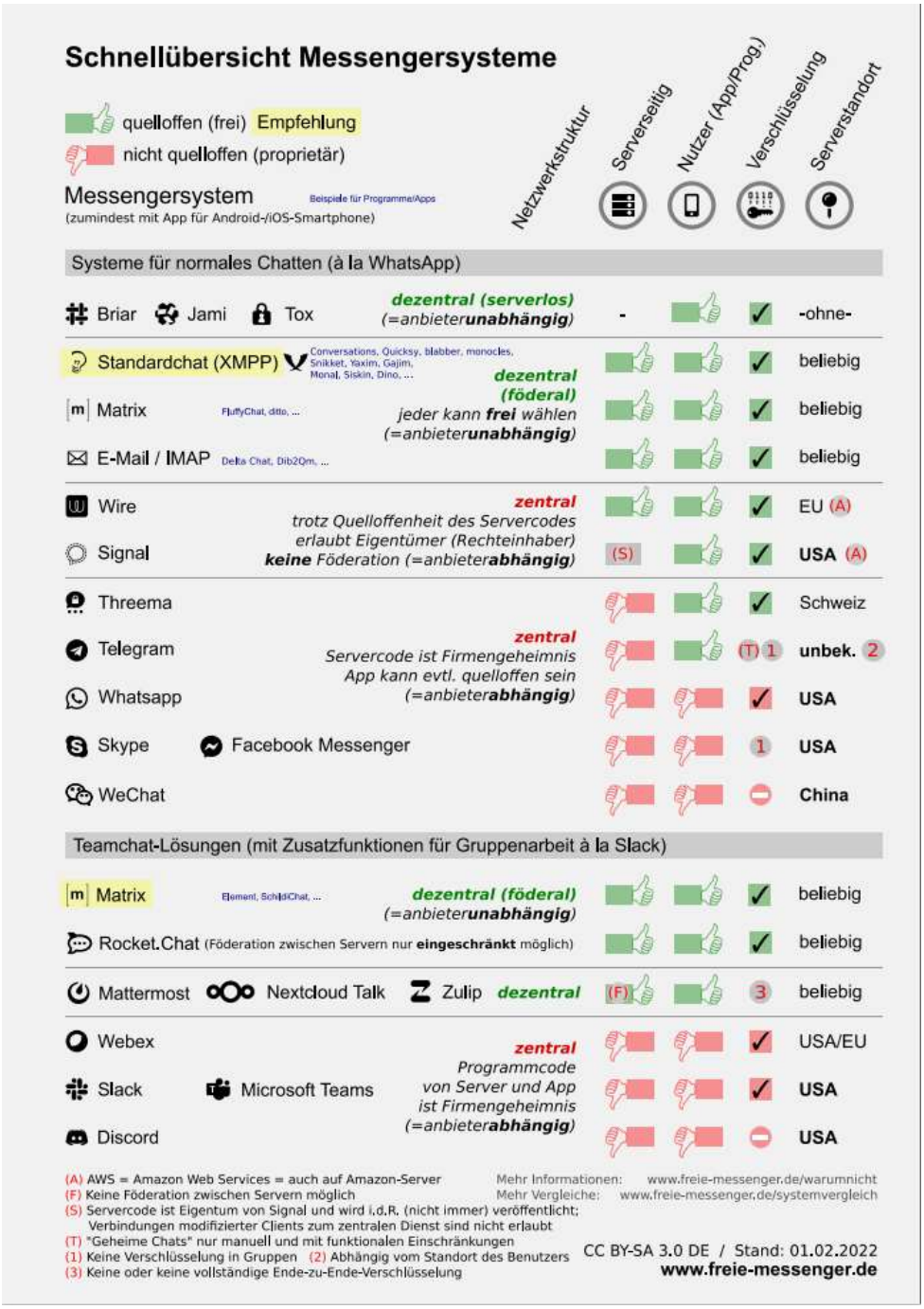


Quelle: Pujol et al. (2019, S. 180)

4.2.4 Ende-zu-Ende-Verschlüsselung

Eine besondere Rolle im Kontext von Datenschutz- und Datensicherheit spielt die Ende-zu-Ende-Verschlüsselung (auch: E2E bzw. E2EE – end-to-end-encryption) von Nachrichten (vgl. auch Kapitel 4.4 zur aktuellen Diskussion im Rahmen des DMA).

Abbildung 4-15: Vergleich unter Sicherheitsaspekten ausgewählter Messaging-Dienste



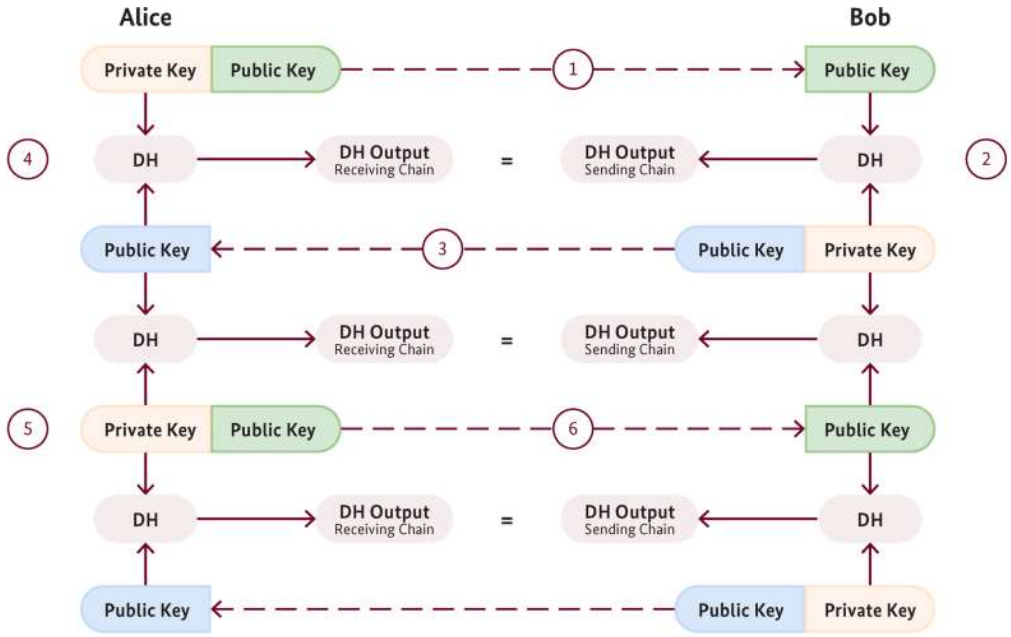
Quelle: Gekeler (2022)

Durch multiple Enthüllungen unter anderem von Edward Snowden ist bei vielen Nutzern ein erhöhtes Sicherheitsbewusstsein zu bemerken. Auf Druck der Nutzer und öffentlicher Berichterstattung implementierte WhatsApp im April 2016 die Ende-zu-Ende-Verschlüsselung des Signal-Protokolls und sorgte damit innerhalb kurzer Frist dafür, dass ein Großteil der Kommunikation über diesen Dienst verschlüsselt war (Marlinspike, 2016b). Das Signal-Protokoll gilt als Weiterentwicklung von den vorherigen Verschlüsselungen Pretty Good Privacy (PGP) für E-Mail und Off-the-Record Messaging (OTR) und vereint essenzielle Funktionen moderner Kommunikationsverschlüsselung. Eine Verschlüsselung muss in erster Hinsicht dafür sorgen, dass die Inhalte der *Confidentiality* (Vertraulichkeit) unterliegen. Ist diese Eigenschaft gegeben, können neben den intendierten Empfängern weder Dritte noch Betreiber des Dienstes den Inhalt nachvollziehen. Aus diesem Grund bietet eine Ende-zu-Ende Verschlüsselung ein höheres Niveau an Datenschutz als bei einer Transportverschlüsselung wie TLS (Transport Layer Security) gewährleistet werden kann. Ferner muss eine Verschlüsselung auch sicherstellen können, dass eine *Authenticity* (Authentizität) und *Integrity* (Integrität) der Nachricht sichergestellt ist, also alle Empfänger der Nachricht zweifelsfrei den Absender identifizieren können und dass Nachrichten auch unmanipuliert, wie vom jeweiligen Absender versendet, erhalten werden (Unger et al., 2015). Weitergehende Sicherheitsfunktionen beziehen sich auf den Fall der Schlüssel-Kompromittierung und sind als *Forward Secrecy* (vorwärts gerichtete Sicherheit) und *Post-Compromise Security* (Sicherheit nach einer Kompromittierung) definiert. Forward Secrecy stellt sicher, dass im Falle der Kenntnis der Haupt- oder Langzeitschlüssel keine Inhalte nachträglich entschlüsselt werden können. Dies wird durch unabhängige Sitzungsschlüssel erreicht, von denen im Zeitpunkt t_0 kein Rückschluss auf vergangene Schlüssel aus der Zeitperiode t_{-1} möglich ist (Rösler et al., 2018). Ein noch höheres Niveau an Sicherheit kann mit Post-Compromise Security erreicht werden, die eine „selbstheilende" Wirkung der Verschlüsselung garantiert. Dies wird erreicht, indem eine Verschlüsselung, die zum Zeitpunkt t_0 kompromittiert wird, auch keine Rückschlüsse auf zukünftige Schlüssel in t_1 zulässt.

Diese oben dargestellten sicheren Eigenschaften werden für Messenger üblicherweise mit asymmetrischen Double Ratchet Diffie-Hellman-Schlüsseln gelöst. Diffie-Hellman-Schlüssel sind das Ergebnis eines mathematischen Verfahrens, bei dem wechselseitig aus der Kombination der privaten und öffentlichen Schlüssel ein identischer Schlüssel generiert wird. Dieses gemeinsame Diffie-Hellman-Geheimnis ist nur den beiden Parteien bekannt und lässt keine Rückschlüsse auf die jeweiligen privaten Schlüssel zu, die ursprünglich zur Generierung verwendet wurden. Ist dieser Prozess beidseitig iterativ aufgebaut wird von einer „Double Ratchet", also einer doppelten Ratsche gesprochen. Diese wird jeweils „weitergedreht", um ein neues gemeinsames Geheimnis zu generieren. In Abbildung 4-16 wird die Herleitung einer asymmetrischen Ratsche vereinfacht dargestellt. Als Grundvoraussetzung besitzen beide Gesprächsbeteiligten jeweils einen öffentlichen und einen privaten Schlüssel. Dies kann in einem Beispiel verdeutlicht werden. Alice sendet mit der ersten Nachricht Bob ihren öffentlichen Schlüssel, wodurch dieser (zusammen mit seinem privaten Schlüssel) ein Diffie-Hellman-Geheimnis errechnen

kann. Im nächsten Schritt sendet Bob mit seiner Nachricht ebenfalls seinen öffentlichen Schlüssel an Alice, so dass auch diese (zusammen mit ihrem privaten Schlüssel) das Diffie-Hellman-Geheimnis errechnen kann. In diesem Diffie-Hellman-Geheimnis sind abgeleitete Informationen der privaten Schlüssel beider Gesprächsparteien, welche ausschließlich lokal auf den Geräten verbleiben und somit auch vom Dienstebetreiber nicht eingesehen werden können. Dadurch kann auch der Dienstebetreiber durch das Beobachten der ausgetauschten öffentlichen Informationen nicht den gemeinsamen Schlüssel von Alice und Bob errechnen. Mathematisch wird dies durch modulare Arithmetik oder elliptische Kurven, im Fall des Signal-Protokoll durch die elliptische Kurve Curve25519, gewährleistet (Bernstein, 2006). Diese elliptischen Kurven sind mathematisch als Einwegfunktionen zu verstehen, bei denen die Berechnung einfach ist, die Umkehrung der Funktion jedoch nur mit sehr großem Rechenaufwand möglich. Durch ein einmalig generiertes Diffie-Hellman-Geheimnis wird die Eigenschaft der Confidentiality erreicht. Um jedoch auch vergangene und zukünftige Nachrichten zu schützen, sehen Double Ratchet-Protokolle vor in regelmäßigen Abständen (beim Signal-Protokoll mit jeder Nachricht) nach einer, nur Alice und Bob bekannten Funktion, ein neues Schlüsselpaar zu generieren. Dies wird mit zwei Ratschen verglichen, die einmalig mit jeder Nachricht weiterrotiert werden. Ein Indikator in der verschlüsselten Nachricht teilt beiden Parteien mit an welcher Stelle der „Ratsche“ sich die jeweilige Partei befindet, so dass auch bei nicht empfangenen Nachrichten keine Asymmetrie entsteht.

Abbildung 4-16: Vereinfachte Darstellung der Double-Ratchet-Verschlüsselung



1. Alice sendet eine Nachricht zusammen mit ihrem Public Key an Bob
2. Bob berechnet mit Alices Public Key und seinem Private Key ein gemeinsames Diffie-Hellman-Geheimnis (DH)
3. Bob sendet seinen Public Key zusammen mit seiner nächsten Nachricht an Alice
4. Alice berechnet mit Bobs Public Key und ihrem Private Key das gemeinsame Diffie-Hellman-Geheimnis
5. Alice generiert ein neues Schlüsselpaar
6. Alice sendet eine Nachricht zusammen mit ihrem neuen Public Key an Bob (usw.)

Quelle: BSI (2021, S. 8)

Der nötige Koordinierungsaufwand zwischen den beiden Parteien muss von Seiten des verwendeten Dienstes geleistet werden, der den Beteiligten Parteien die Rahmenparameter des Protokolls erläutern muss. Ohne diese Abstimmung wäre es nicht möglich eine Nachricht derart zu verschlüsseln, dass der Inhalt für Dritte nicht einsehbar wäre und beide Parteien sich auch auf eine gemeinsame Verschlüsselung „einigen“. Dies hat auch Implikationen für die IOP, insofern die Verschlüsselung der Nachrichten garantiert werden soll.

Die genaue Implementierung der Ende-zu-Ende-Verschlüsselung unterscheidet sich zwischen Messaging-Diensten, wenngleich sich bestimmte Tendenzen herausarbeiten lassen. So beschreiben Ermoshina und Musiani (2019) einen fortlaufenden Prozess der teilweisen Quasi-Standardisierung des Signal-Protokolls, welches zwar von einem Großteil der Dienste in mitunter leichter Anpassung verwendet wird, aber im Gegensatz zu PGP keine offizielle Standardisierungsprozedur durchlaufen hat.

Tabelle 4-3: Übersicht verwendeter Verschlüsselungsprotokolle ausgewählter Messaging-Dienste

Dienst	Ende-zu-Ende-Verschlüsselung bilateral:	Ende-zu-Ende-Verschlüsselung Gruppe:
Discord	N	N
Element (Matrix)	Olm (Signal-basiert)	Megolm (Signal-basiert)
FB Messenger	Proprietär (Signal-basiert)	N
Google Chat (Hangouts)	N	N
iMessage	Proprietär	Proprietär
Instagram DM	Proprietär (Signal-basiert)	N
Kik	N	N
Signal	Signal-Protokoll	Signal-Protokoll
Skype	Proprietär (Signal-basiert)	N
Slack	N	N
SMS (trad. TK)	*N*	*N*
Snapchat	N (Nur Bilder)	N
Telegram	Proprietär (MTProto 2.0)	N
Threema	NaCl	NaCl
Viber	Proprietär	Proprietär
WeChat	N	N
WhatsApp	Proprietär (Signal-basiert)	Proprietär (Signal-basiert)
wickr	Proprietär (Quellcode einsehbar)	Proprietär (Quellcode einsehbar)
Wire	Proteus (Signal-basiert)	Proteus (Signal-basiert)

Quelle: WIK-Consult

Tabelle 4-3 zeigt, dass, insofern eine Verschlüsselung der Nachrichten gewährleistet ist, diese häufig vom Signal-Protokoll abgeleitet wurde. Dazu gehören im Besonderen die Produkte des Meta-Konzerns (WhatsApp, Facebook Messenger und Instagram), der Microsoft-Dienst Skype und die Derivate Olm (Matrix-Protokoll) und Proteus (Wire). Insbesondere bei Facebook Messenger, Instagram und Skype ist die Verschlüsselung nur für bilaterale Kommunikation möglich und muss seitens des Nutzers eingeschaltet werden.[37] Telegram hat die Verschlüsselung proprietär ähnlich dem oben beschriebenen Konzept aufgebaut und nennt sie MTProto. Auch diese Ende-zu-Ende-Verschlüsselung muss seitens des Kunden aktiviert werden. Threemas Verschlüsselung hingegen basiert auf der NaCl-Bibliothek und ist standardmäßig für alle Chats aktiviert. Laut einem Artikel

37 Beim Facebook Messenger heißt diese Funktion „Geheime Unterhaltung“, bei Instagram ist sie unter der Funktion „Ende-zu-Ende-verschlüsselten Chat beginnen“ zu finden und Skype nennt diese Funktion „Private Unterhaltung“.

von Spektrum wird NaCl als sehr sicher eingeschätzt, bietet im Gegensatz zum Signalprotokoll aber keine Post-Compromise-Secrecy, weswegen das Signal-Protokoll als „state-of-the-art“ gilt (Wolfangel, 2021).

Die Verschlüsselung in Gruppen, insofern implementiert, basiert aktuell auf einer bilateralen Verschlüsselung zwischen jedem Mitglied der Gruppe mit jeweils allen anderen Mitgliedern nach den obigen Prinzipien. Dies hat einen überproportionalen Anstieg an notwendigen Schlüsselaustauschverfahren mit jedem weiteren Mitglied in der Gruppe zur Folge, weswegen die Gruppen in beispielsweise WhatsApp auf 512 Mitglieder und in Signal auf 1000 Mitglieder beschränkt sind. An dieser Stelle setzt das neue MLS-Protokoll an, was eine effiziente Skalierung ohne Kompromisse der Sicherheit erreichen soll. Der Name dieses, sich noch in der Entwicklung befindlichen, Verschlüsselungs-Protokolls orientiert sich an dem Protokoll TLS, welches eine Transportverschlüsselung ist und insbesondere bei HTTPS-Verbindungen im Browser Verwendung findet. Dennoch existieren Gegensätze zu TLS, wo bilateral Verschlüsselungen zwischen Server und Clients ausgehandelt werden, da bei Gruppen in Messengern mehr Parteien beteiligt sind und die Dauer einer Session sich mitunter über mehrere Jahre erstreckt. Ferner berücksichtigt TLS als Protokoll eine direkte und synchrone Verschlüsselung, bei der beide Parteien online sein müssen, wohingegen Verschlüsselungen in Messaging-Diensten auch unter Asynchronität funktionieren müssen. Aus diesen Gründen sind Gruppen-Verschlüsselungen in MLS in einer Baumstruktur namens TreeKEM angeordnet, so dass beim Ausscheiden eines Gruppenmitglieds der entsprechende Strang in der Baumstruktur die Verschlüsselung aktualisiert. Das genaue Verfahren ist von Bhargavan et al. (2018) in einem Vorschlag für den MLS-Standard detaillierter beschrieben worden.

Im Gegensatz zu Signal, deren Protokoll bewusst nicht föderiert aufgebaut ist (Marlinspike, 2016a), zeigen die Beispiele Matrix und E-Mail aber, dass auch die Identitäts- und Schlüsselverwaltung grundsätzlich dezentral umzusetzen ist, wie auch von WIK-Consult befragte Experten bestätigen. Zwar würde sich die bisherige breite Anwendung des Signal-Protokolls auch als Anknüpfungspunkt für weitere Standardisierungsansätze anbieten. Zu berücksichtigen für etwaige Implementationen hinsichtlich der IOP zwischen Messengern ist aber, dass im Signal-Protokoll ein zentraler Identifizierungsserver vorgesehen ist, der für die öffentlichen Schlüssel und ein Bundle aus One-Time-Keys für das erstmalige Aushandeln von Verschlüsselungen erforderlich ist (Marlinspike und Perrin, 2016). Dementsprechend müssen bei einer solchen Implementation von IOP Möglichkeiten zum Zugang zu diesen Identitätsservern berücksichtigt werden.

Neben den Inhalten verschlüsselt das Signal-Protokoll auch den Header. Die Telefonnumern der Kontakte werden ge„hashed“[38] , sodass zwar ein Abgleich[39] stattfinden kann, jedoch der Prozess der „Contact Discovery“ nicht unmittelbar zur Reduktion des Datenschutzes für Dritte führt (Marlinspike, 2017). Hinter dem Abgleich von Telefonnummern steht für Messaging-Dienste zugleich die Möglichkeit mit sozialen Graphen die Interaktion von Nutzern nachzuvollziehen. Gerade im Kontext von Ökosystemen können mit Identifikatoren wie Telefonnummern Rückschlüsse auf die Interaktionen über Dienste hinweg gezogen werden. Für die im Folgenden diskutierten IOP-Ansätze stellt die Ende-zu-Ende-Verschlüsselung in ihrer technischen Komplexität eine besondere Hürde dar. Wie von WIK-Consult befragte Verschlüsselungsexperten bestätigen, kann es eine echte Ende-zu-Ende-Verschlüsselung zwischen interoperablen Messengern letztendlich nur unter vollständiger Standardisierung bzw. einer jeweiligen Einigung auf einen gemeinsamen Verschlüsselungsstandard geben. Da es sich um bisher meist proprietär entwickelte Systeme handelt, die zueinander inkompatible Verschlüsselungsverfahren verwenden, wäre der nötige Einigungs- und Implementierungsaufwand extrem hoch und würde laut einem der Experten einer Neuentwicklung einer interoperablen Messaging-Plattform gleichkommen.

4.3 Interoperabilitätsansätze & -verpflichtungen

4.3.1 Verschiedene Arten & Ansätze von Interoperabilität

4.3.1.1 Standardisierung als Protokoll-Interoperabilität

Die technisch robusteste Lösung wäre die gemeinsame Einigung auf einen Standard, indem die notwendige Verschlüsselung, die Semantik und technischen Details im Rahmen eines branchenübergreifenden Einigungsprozesses definiert werden. Dafür müsste der Leistungsumfang des Standards mit den zu berücksichtigen Funktionalitäten verhandelt werden. Dies alles müsste in einem Prozess definiert werden wodurch anschließend eine „Protokoll-IOP“, wie in Kapitel 2.1 erläutert, erreicht werden könnte.

Aus der obigen Erörterung zur Verschlüsselung ergibt sich ebenfalls, dass insofern die Nachrichten Ende-zu-Ende verschlüsselt sein sollen, eine Notwendigkeit zur Koordinie-

38 Eine Hash-Funktion verschlüsselt den Inhalt mithilfe einer Einwegfunktion, die gegeben der gleichen Input-Parameter die gleichen Werte als Output hat. Aus der Nummer „1234567890“ wird beispielsweise durch die SHA256-Funktion der Python-Bibliothek „hashlib“ unabhängig der verwendeten Instanz der hexadezimale Hash “c775e7b757ede630cd0aa1113bd102661ab38829ca52a6422ab782862f268646“. Aus diesem Hash ist ohne Kenntnis der Nummer kein Rückschluss auf diese möglich, will jedoch eine weitere Person diese Nummer abgleichen, sendet sie diesen Hash an den Server und findet den Kontakt mit dieser Nummer.

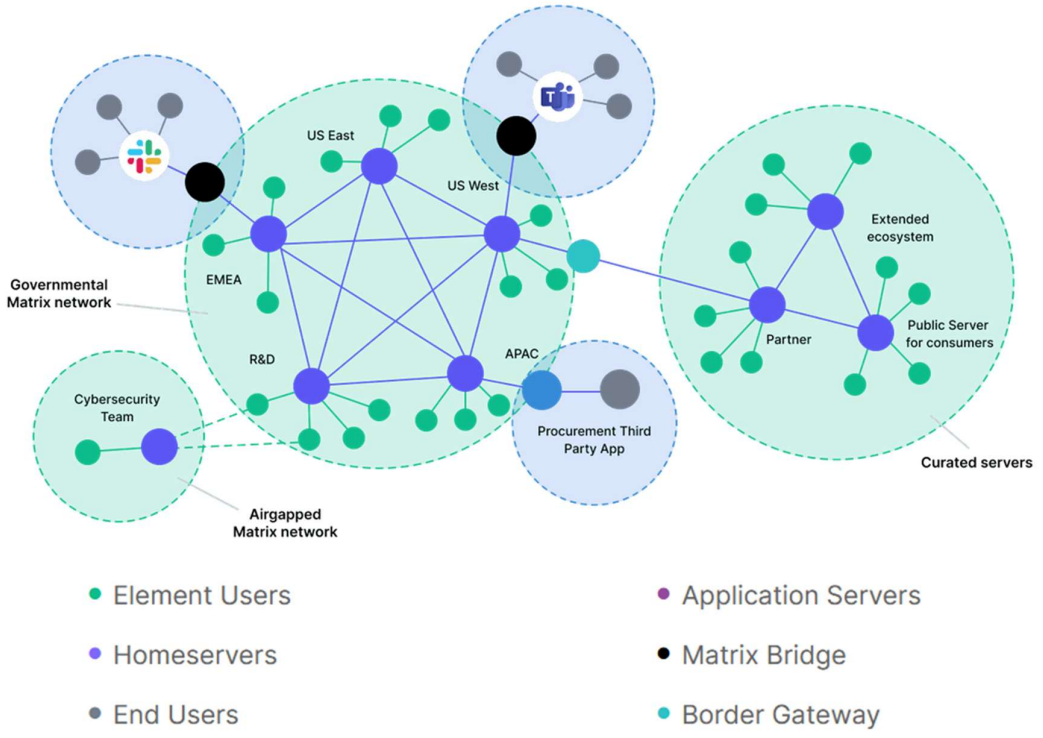
39 Seit 2017 ermöglicht Signal diesen Prozess in einer verschlüsselten Enklave auf dem Server laufen zu lassen, so dass dieser Prozess vollständig getrennt von der Datenbank der registrierten Nutzer von Signal abläuft.

rung auf ein Verschlüsselungsprotokoll entsteht. In Tabelle 4-3 zeigt sich eine weite Verbreitung von Protokollen, die auf dem Signal-Protokoll basieren. Sowohl WhatsApp, Facebook Messenger als auch Instagram haben dieses Protokoll unter Mitarbeit von Signal implementiert, wenngleich ohne Quellcode keine Nachvollziehbarkeit besteht (Marlinspike, 2016b). Andere Messenger bauen auf Forks und Weiterentwicklungen des Signal-Protokolls auf, wie Wire und Matrix. Ermoshina und Musiani (2019) schlussfolgern daraus eine de-facto Standardisierung für den Bereich der Ende-zu-Ende-Verschlüsselung. Dabei ist jedoch anzumerken, dass aufgrund der technischen Komplexität der Verschlüsselung, anders als bei Datei-Formaten wie PDF oder DOCX, auf keine IOP als Nebenprodukt zu schließen ist. Sie beschreiben hierzu einen Prozess der „quasi-standardisation“, der einer asymmetrischen Standardisierung folgt. Dieser Prozess basiert auf einem funktionierenden Code, der erst im Folgenden durch die Implementierung zum „Quasi-Standard“ wird. Diese Tendenz zur Standardisierung folgt der Logik von Entwicklern, dass mit einem Standardisierungsprozess der „Silo-Effekt“ reduziert werde und eine Referenzimplementierung ermöglicht wird. Allerdings beschreiben Ermoshina und Musiani auch eine zunehmende Unzufriedenheit der Entwickler gegenüber Standardisierungsprozessen. Laut Interviews steckt hinter der Kritik die Behäbigkeit von Standardisierungs-Komitees wie IETF und W3C. Aus diesem Grund sei Signals Ansatz erst der Weg über das Programmieren der Funktionalität hin zu einer Dokumentation, worauf potenziell dann eine Standardisierung aufbauen könnte. Einen ähnlichen Ansatz gibt auch der Matrix-Entwickler wieder, der den Dienst erst „stable“[40] bekommen möchte, bevor ein Standardisierungsprozess in Frage käme (Ermoshina und Musiani, 2019). Ebenfalls in diesem Rahmen sei der sich aktuell noch in Entwicklung befindliche Standard MLS zu nennen, welcher eine bessere Skalierbarkeit für Gruppen bezweckt.

Da Matrix von seiner Grundkonzeption dem Prinzip der Föderierung folgt, würde sich dieses Konzept für einen Standard zur IOP grundsätzlich eignen. In Abbildung 4-17 ist ein Beispiel für ein föderiertes Netzwerk dargestellt, welches sich in diesem Sinne auch auf interoperable Netzwerke unterschiedlicher Dienste-Anbieter übertragen ließe. Als blau Punkte wären hierbei die unterschiedlichen „Home-Server“ als die interoperablen Dienste zu verstehen, welche alle auf Basis eines Protokolls miteinander kommunizieren können.

40 In der Entwicklung von Software gibt es eine gestufte Beschreibung des Programmzustands, welcher von Alpha als erste funktionierende Version, über Beta als Testversion hin zu Stable respektive Final zu verstehen ist. In nicht finalen Programmen können sich für die Standardisierung wesentliche Parameter noch ändern, so dass durch eine vorzeitige Standardisierung entweder die Autonomie der Entwickler eingeschränkt wird oder der Standard iterativ angepasst werden müsste.

Abbildung 4-17: IOP föderierter Systeme im Matrix-Protokoll



Quelle: Element (2022a)

Eine Problematik hierbei könnten jedoch die Vereinheitlichung der Identitätsserver darstellen, welche aktuell in föderierten Matrix-Systemen eine Verbindung zwischen Drittanbieter-Identitäten (Telefonnummer, E-Mail-Adresse) und der Matrix-inhärenten ID herstellen. Dieser Prozess wäre für eine sogenannte „Contact Discovery“ notwendig, bei der erkennbar wird, welche Kontakte im lokalen Adressbuch über welchen Dienst erreichbar sind. Da diese Datenbank persönliche Daten enthält, wäre zu koordinieren, ob und inwiefern der Zugriff von den unterschiedlichen Diensten auf diese Identitäts-Datenbank reglementiert werden kann. Alex Stamos, Direktor des Stanford Internet Observatory und ehemaliger CSO bei Facebook, wird in einem Artikel des Nachrichtenportals TheVerge wie folgt zitiert: „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.“ [„Es gibt keine Möglichkeit der Ende-zu-Ende-Verschlüsselung ohne das zugrunde liegende Vertrauen allen Anbietern gegenüber hinsichtlich des Identitätsmanagements… Wenn das Ziel darin besteht, dass alle Nachrichtensysteme die Benutzer der anderen genau gleichbehandeln, dann ist dies ein Alptraum in Sachen Datenschutz und Sicherheit.“] (Faife, 2022).

4.3.1.2 Schnittstellen und API-Zugang

Während Konverter die üblichen Schnittstellen des Dienstes nutzen, bieten im Umfeld der C2B-Kommunikation („consumer-to-business“) viele Dienste Schnittstellen an, um über diese im größeren Umfang mit ihren Kunden in Kontakt zu treten. Dedizierte API-Endpoints sind, wie in Kapitel 3.6.1 erläutert, durch Authentifizierung im kommerziellen Rahmen geeignet, da eine Zuordnung stattfinden kann. Da eine Schnittstelle jedoch üblicherweise über die Transportverschlüsselung TLS hinaus keine Verschlüsselung des Inhaltes aushandelt, unterliegen in diesem Fall die Nachrichten nicht der Ende-zu-Ende-Verschlüsselung. Die WhatsApp Business API löst diesen Umstand damit, dass der die API nutzende Kunde die Software im Unternehmensnetzwerk betreibt, womit die Nachricht zwischen API-Endpoint und Empfänger verschlüsselt bleibt. In Abbildung 4-18 ist zu sehen, wie beispielhaft eine reine Textnachricht über die API versendet wird. Neben der Option „text“ lassen sich auch komplexere interaktive Nachrichten, Sprachnachrichten, Videos und Dateien versenden. Die Möglichkeiten, die WhatsApp Business bietet, sind in einem umfangreichen Developer-Portal erläutert.

Abbildung 4-18: Beispiel aus der Dokumentation der WhatsApp Business API

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

Quelle: Facebook (2022)

Ferner weist WhatsApp in seinem Whitepaper zur Verschlüsselung daraufhin, dass sobald ein zwischengeschalteter Mittler die Software betreibt oder der Cloud-Service ohne eigene Server genutzt wird, eine Ende-zu-Ende-Verschlüsselung nur zwischen dieser Software oder Cloudinstanz und dem Empfänger der Nachricht Wirkung entfaltet (WhatsApp, 2021). Im Whitepaper findet sich dazu folgende Formulierung: „WhatsApp does not consider chats with organizations who choose to use Facebook to operate their API endpoint to be end-to-end encrypted.“ [„WhatsApp betrachtet Chats mit Organisationen, die Facebook mit dem Betrieb der API-Endpoints beauftragen, nicht als Ende-zu-Ende-verschlüsselt.“] (WhatsApp, 2021, S. 26).

Im OECD Bericht (2021) zum Wettbewerb auf digitalen Märkten wird die Möglichkeit der „Personal Information Management Systems“ (PIMS) zur Verwaltung der personenbezo-

genen Daten genannt, welche als Treuhänder auftreten können (OECD, 2021). Grundsätzlich wäre ein digitaler Treuhänder auch in der Lage die Funktion eines Intermediärs zu übernehmen, jedoch dürften sich Unterschiede in den Anforderungen zwischen der Verwaltung von Identitäten und der Bereitstellung eines permanent laufenden Messaging-Dienstes mit vielen ausgetauschten Nachrichten ergeben.

Unter Berücksichtigung des Vorschlags von individuellen Schnittstellen im Non-Paper der Europäischen Kommission (2022a) ist zu berücksichtigen, dass grundsätzlich das Risiko von entstehenden Sicherheitslücken und Angriffsstellen zum Missbrauch geschaffen werden können. Ein vormals unter Designaspekten geschlossen konzipiertes System nachträglich für Schnittstellen zu öffnen ist von erhöhter Komplexität gegenüber ursprünglich offen konzipierten Systemen. Im Falle von Cambridge Analytica und Facebook ist ferner festzuhalten, dass auch bestehende Schnittstellen durch missbräuchliche oder unsachgemäße Verwendung Datenschutzrisiken für die Nutzer zur Folge haben können.

4.3.1.3 Bridges

Wie in Kapitel 2.1.2 bereits erläutert, sind Adapter und Konverter eine Möglichkeit, um zwischen inkompatiblen Produkten oder Diensten Kompatibilität herzustellen. Im Falle von Messaging-Diensten handelt es sich hierbei um einen „Übersetzer“ vom Datenmodell des Messengers A zum Datenmodell des Messengers B, der die etwaigen Unterschiede der Datenmodelle angleicht. Bennaceur et al. (2012) nennen diesen Prozess eine Aggregation disparater Systeme mithilfe von Mediatoren. Obwohl es sich aus ökonomischer Sicht bei Messaging-Diensten um eine, in den oben erörterten Grundfunktionen, relativ homogene Dienstleistung handelt, ist die technische Realisierung sehr unterschiedlich, wie in den vorangegangenen Kapiteln erörtert wurde. So bedingt ein Prozess der Konvertierung sowohl die technische als auch die semantische „Übersetzung“. Unter technischen Unterschieden können Dateiformate verstanden werden, mit semantischen Unterschieden sind Daten, die über die eigentliche Nachricht hinausgehen also Metadaten, und die Art der Deklarierung und Erläuterung gemeint. Durch diesen Übersetzungsprozess von einem Datenmodell in ein anderes ist es unabdingbar, dass die ursprüngliche Nachricht unverschlüsselt bereitgestellt oder vor der Umwandlung entschlüsselt wird, was das Konzept der Ende-zu-Ende-Verschlüsselung verletzt. Laut von WIK-Consult befragten Experten kann diese daher nur bei Nutzung des gleichen Standards gewährleistet werden (vgl. auch Kapitel 4.2.4). Da die meisten Messenger nicht derart konzipiert sind auf der Gegenseite mit einem Konverter zu „kommunizieren“, ist es zudem erforderlich, dass dieser Konverter als „Puppet“ konzipiert ist. Der Konverter ahmt somit die andere Seite nach und verhält sich entsprechend so, als wäre der Konverter eine andere Instanz dieses Messengers. Hieraus ergibt sich eine Fragilität bei Änderungen, die dann, insofern keine Quelloffenheit besteht, seitens des Konverters nachempfunden werden muss. Dabei sind je nach Komplexität des zu „übersetzenden“ Dienstes nicht alle Funktionalitäten kompatibel zu gestalten. Ferner muss für jeden anderen Messenger, der kontaktiert werden soll, ein separater Konverter programmiert und auch aktuell gehalten werden. Dieser

Aufwand steigt mit der Diversität und Komplexität insbesondere der angebotenen Features der Messenger (z. B. Austausch von Bild-, Audio- oder Videodateien sowie Audio-/Videocalls) an. Im Bereich der Messenger sind Konverter eine gängige Lösung zur Bereitstellung von adversarialer IOP, bisweilen aufgrund fehlender direkter „Usability“ eher adversarialer Kompatibilität.

Die Entwicklung von Matrix steht im Kontext von dezentralisierten Messenger-Anbietern, weswegen für Dienste, die nicht auf dem Matrix-Protokoll basieren, mit sogenannten „Bridges“ (partielle) Kompatibilität über Konverter hergestellt werden muss. Diese werden ebenfalls Open-Source zur Implementierung bereitgestellt und umfassen aktuell jeweils eigene „Bridges“ für unter anderem Facebook Messenger, iMessage, WeChat, Instagram, Signal und WhatsApp (Matrix, 2022). Hinsichtlich der oben erläuterten, mitunter eingeschränkten „Usability“, ist an dieser Stelle die Implementierung von iMessage zu Matrix zu nennen. So ist zur Herstellung der Funktionalität ein separater Mac-Computer oder eine modifizierte iOS-Firmware notwendig, auf der ein separater Server läuft, der auf die lokale Nachrichten-Datenbank zugreift und die Nachrichten versendet. Auch für diese Bridge weist Matrix aus, dass die Verschlüsselung ausschließlich zwischen Endnutzer 1 und Bridge besteht. Neben den öffentlich bereitgestellten und von der Matrix-Community gepflegten Bridges bietet Element (ehemals Riot) ein kommerzielles SaaS-Angebot für Endkunden und Firmen an. Die Bridges sind zum einen umfangreicher und eine nahtlose Integration wird beworben (Element, 2022b). Eine ähnliche Dienstleistung auf Matrix-Basis bietet Beeper an, welches dadurch ebenfalls die Problematik unvollständig kompatibler Bridges teilt (Beeper, 2022).

Aufgrund der Tatsache, dass die Bridges für den Gesprächspartner nicht als solche erkennbar sind, sieht Kuketz (2020) datenschutzrechtliche Bedenken. Gerade da der Schutz von Metadaten sehr heterogen behandelt wird und Bestandteil der Produktdifferenzierung ist, können sich hier Unterschiede ergeben. So weist Kuketz darauf hin, dass wenn ein Nutzer von Messenger A über eine Bridge einen Nutzer bei Messenger B kontaktiert, dieser Nutzer B keine Einwilligung zur Datenverarbeitung von Messenger A gegeben hat. Da jedoch zumindest die Metadaten in Bezug auf diesen Kommunikationsaustausch auch von Messenger A erhoben werden können, sei dies datenschutzrechtlich bedenklich, schlussfolgert Kuketz.

Ein weiteres Hindernis bei dem Betrieb dieser Bridges sind die Nutzungsbedingungen der Messaging-Dienste. So findet sich beispielsweise in den Nutzungsbedingungen von WhatsApp ein Absatz der sowohl Reverse Engineering als auch abgeleitete Dienste verbietet. Insofern dürfte die Nutzung von Bridges unter rechtlichen Aspekten ohne IOP-Verpflichtung kritisch sein. Bislang gibt es keine Berichte zu Versuchen der aktiven rechtlichen Unterbindung dieser Bridges. Wohl aber gibt es Berichte über den Versuch von WhatsApp modifizierte Apps aus den App-Stores entfernen zu lassen (Johannsen, 2015).

4.3.1.4 Multi-Messenger als Aggregationsdienst

Aggregationsdienste haben insbesondere im Bereich von Preisvergleichsportalen an Relevanz gewonnen und bieten in der anfänglichen Form die Möglichkeit auf einer grafischen Oberfläche die Preise zu vergleichen und nach der Entscheidung auf die separate Seite des Anbieters weitergeleitet zu werden. Suchmaschinen reduzieren unter diesem Aspekt die Suchkosten der Nutzer. Ein ähnliches Konzept verfolgt die Applikation DM Me, welche lokal auf dem Gerät vorhandene Messenger in einer Oberfläche vereint. Da das Gerät und damit der Nutzer selbst der jeweilige Endpunkt der Verschlüsselung ist, kann mit dieser Umsetzung das Problem der verletzten Ende-zu-Ende-Verschlüsselung umgangen werden.

Auch hier sollen implizite „Suchkosten“ durch die Frage welcher Kontakt über welchen Dienst üblicherweise kontaktiert wird reduziert werden, indem eine gemeinsame einheitliche Nutzeroberfläche geschaffen wird. Unter technischen Aspekten findet hier jedoch durch eine separate Applikation keine Verbindung zwischen den Diensten statt, womit auch keine Kompatibilität hergestellt wird und es sich technisch nicht um echte IOP handelt. Die niedrige Verbreitung dieser Dienste lässt vermuten, dass durch nur ein geringer Mehrwert geschaffen wird. Inwiefern diesem Umstand durch Vorgaben zur Öffnung von Schnittstellen entgegen gewirkt werden kann ist unklar. Trotz der in Kapitel 4.3.1.3 beschriebenen Probleme beim Einsatz von Bridges, die zur Aggregation verwendet werden, lassen sich derartige Dienste gewissermaßen als Messenger sehen, die Multi-Homing vereinfachen und somit in dieser Hinsicht positiv zu bewerten sind.

4.3.2 Aktuelle Vorschläge

Im Fokus der folgenden Analyse stehen vor allem die im Rahmen des DMA diskutierten und vorgesehen IOP-Regelungen. Neben den in Kapitel 3.1.2.1 genannten Ansätzen in Deutschland finden aber auch auf internationaler Ebene verstärkt ähnliche Forderungen nach IOP-Verpflichtungen oder zumindest Verboten der unverhältnismäßigen Verhinderung von IOP statt, auch im Bereich von Messaging-Diensten (ACCC, 2020; CMA, 2020), ACCESS Act (H.R. 3849), die allerdings meist noch nicht klar ausspezifiziert wurden. Somit stellt der DMA insbesondere für Messaging-Dienste bzw. NI-ICS den aktuell relevanten Ansatz einer konkreten Ausgestaltung dar.

Laut DMA sollen IOP-Verpflichtungen in Bezug auf NI-ICS vor allem die Marktbestreitbarkeit erhöhen, indem sie das Überwinden von starken Netzwerkeffekten ermöglichen (vgl. auch Kapitel 3.2.1). In Bezug auf die adressierten, meist als Multiprodukt-Ökosystem agierenden, Gatekeeper werden auch die durch entsprechende Integrations- und Verbundvorteile in besonderer Weise erhöhten Wechselkosten für Endnutzer und damit erhöhten Markteintrittsbarrieren für alternative Anbieter genannt (vgl. auch Kapitel 4.1.3.5).

Laut internen Dokumenten wurden zunächst verschiedene Optionen diskutiert (Europäische Kommission, 2022a). Neben einer IOP-Verpflichtung für Social Media

Dienste der Gatekeeper wurde auch von einer vollständigen Standardisierungsmaßgabe auf Messengerebene zunächst Abstand genommen. Stattdessen findet sich in der finalen Fassung ein vergleichsweise milder Ansatz, der gleichzeitig eine möglichst volle Wahlfreiheit für Endnutzer und alternative Anbieter, Differenzierungsmöglichkeiten und ein hohes Maß an Datenschutz erhalten soll. Es handelt sich um eine asymmetrische Verpflichtung, in der ernannte Gatekeeper anderen Anbietern einen entgeltfreien Zugang zu von ihnen betriebenen NI-ICS gewähren müssen. Dies muss allerdings nur auf aktive Anfrage eines anderen Anbieters erfolgen, so dass für diese ein eventueller Anschluss auf vollständiger Freiwilligkeit basiert.

Außerdem ist die Zugangsverpflichtung auf eine Basisfunktionalität beschränkt, die gestaffelt im Laufe der Zeit erweitert wird. Zunächst gilt diese nur zwischen Einzelnutzern für Textnachrichten, Sprachnachrichten, Austausch von Dateien, insbesondere Fotos und Videos. Zwei Jahre nach einer Einordnung als Gatekeeper soll selbige Funktionalität dann auch für Gruppenchats gewährleistet werden, nach vier Jahren kommen außerdem Sprach- und Videoanrufe hinzu.

Der Gesetzestext legt einen hohen Wert auf den Erhalt von Datensicherheit und Datenschutz. Dazu gehört ein Datensparsamkeitsgebot, in dem die Sammlung und der Austausch von Daten ausschließlich auf das nötige Niveau zur Gewährleistung einer effektiven IOP zu beschränken ist. Das gleiche Schutzniveau, welches für eigene Nutzer angeboten wird, muss auch für die IOP mit externen Anbietern gelten. Dazu gehört explizit auch der Erhalt einer etwaigen Ende-zu-Ende-Verschlüsselung.

Um die etwaigen Anfragen für Drittanbieter zu erleichtern, sollen Gatekeeper außerdem Referenzangebote zur Verfügung stellen, die insbesondere die nötigen technischen Anforderungen und Details für einen IOP-Anschluss erläutern. Auch hier sind explizit die Themen Sicherheit und Ende-zu-Ende-Verschlüsselung genannt. Selbige können auch eine Ausnahmeverlängerung der Zugangsfrist bedingen, während der jeweilige Zugang normalerweise innerhalb von drei Monaten nach Anfrage gewährt sein soll. Allgemein sind aber Verhaltensweisen untersagt, die die IOP aufweichen oder für Anfragende erschweren sollen wie diskriminierende Bedingungen oder unberechtigte technische Maßnahmen und Urheberrechtsforderungen.

Neben der freiwilligen Entscheidung für alternative Anbieter wird auch der Erhalt der Wahlfreiheit für Nutzer hervorgehoben. Endnutzer sowohl des Gatekeepers als auch des anfragenden Anbieters sollen frei in ihrer Entscheidung bleiben können, die Funktionen interoperabel zu nutzen, also z. B. für Nutzer des jeweilig anderen Anbieters tatsächlich erreichbar (und auffindbar) zu sein.

Eine weitere nicht abschließend geklärte Frage im allgemeinen Fall von IOP-Verpflichtungen stellt zudem die Art und Bepreisung des Zugangs dar, während der DMA für den Zugang zu NI-ICS-Funktionen einen entgeltfreien Zugang fordert. Zur Frage einer angemessenen Bezahlung wird im generellen Kontext von obligatorischem Zugang zu

digitalen Plattformen häufig der „FRAND“-Mechanismus als Möglichkeit diskutiert (Matos und Torres-Sarmiento, 2022), der bisher vor allem im Bereich von Patentzahlungen Anwendung findet. Insbesondere für den Fall asymmetrischer Verpflichtungen gegenüber „dominanten“ Anbietern wird teilweise auch ein kostenfreier Zugang gefordert bzw. vorgesehen (Heim und Nikolic, 2019), so auch in der im Folgenden diskutierten Regelung für Gatekeeper im DMA.

Inwiefern die insgesamt eher milden Regelungen möglichen Bedenken gegenüber der im Messengerbereich vorliegenden Form von insbesondere horizontaler IOP (vgl. unter anderem Kapitel 3.3 & 4.1.4) zuvorkommen, aber auch eigene Probleme mit sich bringen, wird im folgenden Kapitel diskutiert.

4.4 Bewertung und Handlungsempfehlungen

4.4.1 Ökonomische und technische Bewertung

Nicht zuletzt im Vorfeld möglicher IOP-Anforderungen im DMA wurden eine Reihe von Bedenken gegen eine IOP-Vorschrift für Messaging-Dienste im Speziellen und für horizontale Anforderungen im Allgemeineren aufgeworfen (vgl. Kapitel 3).

Hier wurde vor allem vor zu umfassenden Regelungen, sowohl in Bezug auf den Adressatenkreis als auch auf den Funktionalitätsumfang, gewarnt, die Möglichkeiten zur Ausdifferenzierung und Abgrenzung und damit auch Innovationsanreize schwächen könnten. Die Besorgnis über zu geringe Möglichkeiten zur Produktdifferenzierung wird unter anderem von der Monopolkommission (2021) in ihrem 12. Sektorgutachten zum Telekommunikationsmarkt als ein Hauptargument gegen eine verbindliche horizontale IOP-Verpflichtung im Markt für Messaging- und Videodiensten geteilt. Sie bezieht sich in ihrer Analyse auf eine Befragung des Bundeskartellamt (2021) von 44 Unternehmen der Branche. Hieraus geht hervor, dass der bestehende Wettbewerb auf horizontaler Ebene bereits als intensiv wahrgenommen wird und differenzierte Produktfunktionalitäten wie z. B. Handheben, Emojis im Konferenzchat, Inhalte teilen, Einspielen visueller Hintergründe etc. wichtige Wettbewerbsfaktoren sind. Durch eine Homogenisierung der Dienste durch horizontale IOP wären Kunden weniger geneigt zwischen den verschiedenen Anbietern zu wechseln.

Da sich der Beschluss des DMA zunächst lediglich auf die Basisfunktionalität des reinen Austauschs von Nachrichten und Dateien beschränkt, wird hier eine größere Möglichkeit zur Ausdifferenzierung über diverse Zusatzfunktionen erhalten. Dies führt allerdings auch zu einem Konflikt mit dem ursprünglichen Ziel der Reduzierung von firmenspezifischen Netzwerkeffekten, da diese im Rahmen dieser Zusatzfunktionen dadurch erhalten bleiben. Andererseits wird der Innovationsanreiz, sich durch exklusive Funktionalitäten abzuheben bzw. im Vergleich zu konkurrierenden Anbietern nicht ins Hintertreffen zu geraten, erhalten. Ein Beispiel aus der Vergangenheit sind hier möglicherweise die Ende-zu-Ende-

Verschlüsselung bei WhatsApp sowie Emoji-Reaktionen für Nachrichten, die Dienste wie Signal oder Beeper bereits über längere Zeit anbieten und erst in einem aktuellen Update von WhatsApp eingeführt wurden. Inwiefern solche und andere Funktionen im Laufe der Zeit möglicherweise ebenfalls zu „Basisfunktionalitäten“ werden können, bleibt allerdings gerade im dynamischen Entwicklungsverlauf von Messaging-Diensten eine nicht eindeutig zu beantwortende Frage.

Auch bei der zeitlichen Staffelung besteht das Risiko, dass die Planung von der dynamischen Marktentwicklung überholt wird und später nötige Anpassungen umso aufwendiger werden. Dadurch kann die Entwicklung ineffizient verlaufen, wenn am Anfang ein technisches Fundament geschaffen wird, das später bestimmte Funktionserweiterungen gar nicht erlaubt. Gerade solche komplexen Systeme bergen dann die Gefahr, dass teuer nachgebessert oder der Unterbau erneuert werden muss.

Andererseits können durch IOP aber auch Innovationen im Kernbereich des Funktionsumfangs erschwert werden. Beispielsweise würde die Einführung eines höheren Verschlüsselungsniveaus oder selbstlöschender Nachrichten eine Aktualisierung der IOP-Schnittstelle erfordern und könnte demnach nicht dezentral von den interoperablen Messengern durchgeführt werden. So besteht bereits im Status quo eine fehlende Einigkeit auf die Definition von echten Basisfunktionalitäten. So impliziert z. B. die Internet Society (2022), dass nicht nur eine Ende-zu-Ende-Verschlüsselung eine solche Basisfunktionalität darstellen sollte, sondern weist darauf hin, dass auch über die detaillierte technische Ausgestaltung dieser eine Einigung notwendig wäre, um IOP herzustellen. Konkret wird dort das Beispiel genannt, ob ausstehende Nachrichten noch übermittelt werden, wenn sich auf halbem Weg der Authentifizierungsschlüssel des Gesprächspartners ändert. Da dies z. B. von Signal und WhatsApp unterschiedlich gehandhabt wird, könne nicht von einer einheitlichen „Basisfunktionalität“ gesprochen werden und IOP nicht erreicht werden, ohne hier eine Einigung zu erzielen. Diese würde allerdings erfordern, dass eine von beiden Entwicklerseiten ihren ja eigentlich präferierten Ansatz in der Abwägung zwischen Sicherheit und Usability aufgeben müsste (Internet Society, 2022).

Verpflichtende IOP-Standards könnten auch als strategische Marktzutrittsschranke zweckentfremdet werden und bereits etablierte Anbieter damit sogar vor Eintritten innovativer Wettbewerber schützen. Erste Indizien für diese Gefahr sind in der Befragung von 44 Anbietern von Messaging- und Videodiensten des Bundeskartellamt (2021) zu finden. Hier wird angemahnt, dass „[b]esonders 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, S. 93). Im Festlegungsprozess des Standards ist somit zu bewerten, wie realistisch Markteintritte sind, um somit das Aufbauen von Marktzutrittsschranken zu vermeiden. Dieser Aspekt wird zwar im DMA entschärft durch die asymmetrische Verpflichtung ausschließlich für Gatekeeper und die Freiwilligkeit für alternative Marktteilnehmer sowie durch den vorläufigen Verzicht auf eine Standardisierung im engeren Sinne.

Gerade in Bezug auf eine effektive Ende-zu-Ende-Verschlüsselung wird eine vollständige (de-jure oder de-facto) Standardisierung aber auf der anderen Seite als notwendig erachtet, um eine sichere Verschlüsselung unter IOP zu gewährleisten, wie auch die Einschätzung der von WIK-Consult befragten Experten für Verschlüsselungstechnologien zeigen (vgl. Kapitel 4.2 und 4.3). Dieser Implementierungsansatz würde also bei konsequenter Durchsetzung eine Einführung von IOP für zuvor Ende-zu-Ende-verschlüsselte Funktionen unmöglich machen oder alternativ bestehende Sicherheitsniveaus gefährden. Eine Neuevaluation und die spätere Festlegung von Standards wird sich allerdings im DMA vorbehalten und wäre dann den entsprechenden Risiken unterworfen, die Standardisierungsprozesse im Allgemeinen aufweisen können (vgl. auch Kapitel 3.7).

Zunächst ist aber laut Andreas Schwab, Berichterstatter des Europaparlaments, vorgesehen, dass die Gatekeeper APIs für Konkurrenten anbieten, um interoperable Messaging-Funktionen ermöglichen zu können (Europäische Kommission, 2022a; Lomas, 2022). In dieser asymmetrischen Ausgestaltung sind andere Anbieter also weder verpflichtet, sich gegenüber Gatekeepern, noch einander gegenseitig zu öffnen. Lediglich die Gatekeeper sind verpflichtet, eine bilaterale Verbindung zum ggf. Anfragenden herzustellen. Die einfachste Option werden höchstwahrscheinlich öffentliche Versionen von Schnittstellen (APIs) und entsprechender Funktionalität sein, die Gatekeeper bereits in ihren eigenen Systemen verwenden. Wie oben erwähnt, ist diese technische Implementierung von IOP aber nicht vereinbar mit zuvor Ende-zu-Ende-verschlüsselten Funktionalitäten. Eine freiwillige Einigung auf offene technische Standards wie z. B. Matrix oder MLS wäre grundsätzlich möglich, ist aber aktuell nicht zu erwarten. Dies bedeutet auch, dass interessierte Wettbewerber im Zweifel eine Reihe von unterschiedlichen APIs und zugehörigen Messaging-Protokollen pro Gatekeeper unterstützen müssten und die Nutzer ggf. Einschränkungen bei der Sicherheit hinnehmen müssten.

In Anbetracht der potenziellen Ineffizienzen durch die zeitliche Staffelung der Herstellung von IOP für bestimmte Funktionalitäten und durch den potenziell nötigen gleichzeitigen Einsatz diverser Protokolle, lässt sich auch hier festhalten, dass die dadurch kumulierten Kosten, sowohl bei Anbietern als auch im Monitoring, vermutlich die Kosten einer systematischen vollständigen Standardisierung sogar übersteigen könnten. Aber auch in diesem Prozess wäre eine zuverlässige Planung und Berücksichtigung von zukünftig zu inkludierenden Features nötig, um keine Fehlentwicklungen in dem pfadabhängigen Ablauf zu erzeugen, welcher darüber hinaus mit den üblichen Problemen von Standardisierungsprozessen behaftet ist (vgl. Kapitel 2.1.3 und 3.7.2). Sowohl Gatekeeper als auch konkurrierende Anbieter müssen bei einer möglichen Implementierung von IOP gewährleisten, dass alle Verbraucher auch im Fall einer grundsätzlichen Anbindung weiterhin frei in Ihrer Entscheidung bleiben, von Nutzern des jeweils anderen Dienstes kontaktiert werden zu können. Dies begegnet auch der Sorge, dass Zugriff auf (Meta-)Daten von Kunden anderer Services die Gatekeeper-Positionen noch stärken könnte. Dies soll zusätzlich durch den gleichzeitigen „ban on personal data combination“ (Art. 5(2)(b)) verhindert werden, durch den z. B. für die Nutzung für gezielte Werbung die ausdrückliche Zustimmung der Nutzer für eine solche Verwendung erforderlich ist. In der praktischen

Umsetzung könnten diese Aspekte allerdings in ihrer logistischen und technischen Komplexität zu schwer überschaubaren Konstellationen für Nutzer führen, die schlimmstenfalls sogar von der Nutzung kleinerer, alternativer Dienste abschrecken könnte.

Horizontale IOP könnte theoretisch dazu beitragen, die Marktkonzentration bei Messaging-Diensten zu verringern. Untersuchungen zeigen jedoch, dass die Verbraucher in Deutschland trotz Netzwerkeffekten mehrere Dienste gleichzeitig nutzen (s. z. B. Bundesnetzagentur, 2020, sowie Kapitel 4.1). Dies ist auf Produktdifferenzierung, Innovationen, geringe Kosten von Multi-Homing und einen heterogenen Kreis von Kontakten zurückzuführen, was darauf hindeutet, dass IOP nicht erforderlich ist bzw. wie oben beschrieben, sogar zu einem negativen Effekt führen könnte. Teile der Netzwerkeffekte können seitens eines Nutzers durch Multi-Homing über die gleichzeitige Nutzung mehrerer Dienste realisiert werden. Aus Sicht von Anbietern, die ihre Dienste hinsichtlich Datenschutz oder anhand erweiterter Sicherheitsfunktionen differenzieren, ist diese horizontale IOP mitunter nicht vorteilhaft, da Alleinstellungsmerkmale nicht erhalten bleiben (vgl. auch Bundeskartellamt, 2021).

Grundsätzlich macht IOP es zwar einfacher, zu kleineren Anbietern zu wechseln, senkt aber gleichzeitig den Anreiz dafür, dies tatsächlich zu tun (vgl. Bourreau et al., 2022). Entscheidet sich ein „verhandlungsmächtiger“ Kontakt, nur noch Anbieter B zu nutzen, müssten ohne IOP alle seine Kontakte, die ihn noch erreichen wollen, ebenfalls den Dienst von Anbieter B installieren und für diese Kommunikation auch nutzen. Im interoperablen Fall können alle Kontakte problemlos ausschließlich bei Anbieter A verbleiben und können dennoch weiterhin mit ihrem Kontakt bzw. Nutzern von Anbieter B kommunizieren. Auf der anderen Seite wird es denjenigen, die zu Anbieter B wechseln, auch leichter gemacht, den Anbieter A vollständig zu deinstallieren, da sie weiterhin dessen Nutzer kontaktieren können. So hat (partielle) IOP grundsätzlich sowohl einen pro-kompetitiven Effekt (durch Reduktion der firmenspezifischen Netzwerkeffekte) als auch einen anti-kompetitiven Effekt (durch Reduktion von Multi-Homing) und es ist ex-ante unklar welcher der Effekte schlussendlich dominiert (vgl. Bourreau et al., 2022).

4.4.2 Juristische Bewertung

Die im DMA vorgesehenen Regelungen zur IOP von Messaging-Diensten sind erkennbar darauf ausgerichtet, einen sachgerechten Ausgleich zwischen unterschiedlichen Regelungszielen zu erreichen. Insbesondere soll ein hohes Datenschutzniveau gewährleistet und Bedenken hinsichtlich der Datensicherheit Rechnung getragen werden. Dies kommt etwa in Art. 7(3) DMA zum Ausdruck, der betont, dass das Sicherheitsniveau, einschließlich einer etwaigen Ende-zu-Ende-Verschlüsselung, das der Gatekeeper seinen eigenen Nutzern bietet, bei den interoperablen Diensten beibehalten werden muss. Bei konsequenter Durchsetzung würde dies aufgrund der diskutierten technischen Unvereinbarkeit von IOP und Ende-zu-Ende-Verschlüsselung implizieren, dass die IOP für zuvor bereits Ende-zu-Ende-verschlüsselte Dienste bzw. Funktionen nicht hergestellt werden kann

bzw. von Seiten des Gatekeepers nicht hergestellt werden muss, sofern der sich anschließende Anbieter nicht vollständig das Protokoll bzw. den Standard des Gatekeepers implementiert.

Die Regelung lässt sich dahingehend verstehen, dass die Beibehaltung des Sicherheitsniveaus eine Voraussetzung für die Öffnung des Messaging-Dienstes gegenüber anderen Anbietern ist. Diese Auslegung wird durch Art. 7(4) DMA gestützt. Danach hat der Gatekeeper in dem von ihm zu veröffentlichten Referenzangebot die technischen Details und allgemeinen Bedingungen für Ermöglichung von IOP zu veröffentlichen "einschließlich der erforderlichen Einzelheiten zum Sicherheitsniveau und zur Ende-zu-Ende-Verschlüsselung". Somit kommt eine Einräumung von IOP nur gegenüber solchen Anbietern in Betracht, die in der Lage sind, diese Anforderungen zu erfüllen. Dieser Vorbehalt könnte von Gatekeepern dazu genutzt werden, um die Einräumung von IOP unter Berufung auf Sicherheitsbedenken zu erschweren. Allerdings stellt Erwägungsgrund 64 DMA klar, dass der Inhalt des Referenzangebotes durch die EU-Kommission (gegebenenfalls in Abstimmung mit BEREC) daraufhin überprüft werden kann, ob er den Vorgaben des DMA zur Ermöglichung von IOP genügt.

Klärungsbedürftig ist in diesem Zusammenhang insbesondere die Frage, welche Anforderungen an die "Beibehaltung" des Sicherheitsniveaus zu stellen sind. Soweit der Gatekeeper für seine Nutzer eine Ende-zu-Ende-Verschlüsselung vorsieht, wird man als Mindestanforderung verlangen können, dass auch der andere Anbieter eine entsprechende Verschlüsselung gewährleistet. Zu weitgehend dürfte es allerdings sein, in technischer Hinsicht identische Sicherheitsvorkehrungen zu verlangen. Im Sinne einer effektiven IOP dürften vielmehr äquivalente Maßnahmen zur Gewährleistung von Datensicherheit ausreichend sein.

Art. 7(5) DMA sieht vor, dass der Gatekeeper nach Veröffentlichung des Referenzangebotes verpflichtet ist, einem „zumutbaren Antrag" ("reasonable request") auf IOP binnen einer Frist von drei Monaten nachzukommen. Hier stellt sich die Frage, welche Anforderungen an einen "zumutbaren Antrag" zu stellen sind. Bei enger Auslegung könnte Art. 7(5) DMA als Schikaneverbot verstanden werden. Demnach dürften nur solche Anträge als "unzumutbar" unbeachtet bleiben, die offenkundig missbräuchlich sind. Denkbar wäre es aber auch, bei der Bewertung der Zumutbarkeit ökonomische Aspekte einfließen zu lassen, etwa die Frage, ob die IOP im konkreten Fall nur mit unverhältnismäßigen Kosten hergestellt werden kann. Im Interesse einer effektiven IOP erscheint eine enge Auslegung von Art. 7(5) vorzugswürdig.

Wie oben bereits näher ausgeführt, dürfte sich die Gewährleistung des erforderlichen Sicherheitsniveaus, einschließlich der Ende-zu-Ende-Verschlüsselung, aus technischer Hinsicht als komplexe Herausforderung darstellen. Es erscheint daher sachgerecht, dass Art. 7(6) DMA der EU-Kommission die Möglichkeit einräumt, die in Art. 7(2) bis (5) genannten Fristen für die Ermöglichung von IOP zu verlängern, sofern der betreffende Ga-

tekeeper nachweist, dass dies für die Gewährleistung des erforderlichen Sicherheitsniveaus notwendig ist. Einige der von WIK-Consult befragten Experten für Verschlüsselungstechnologien schätzen den Implementierungs- bzw. Entwicklungsaufwand für die Nutzung eines einheitlichen Standards mit bis zu 5 Jahren ein.

Art. 7(7) DMA verlangt, dass die Nutzer des Gatekeepers und des anderen Anbieters frei entscheiden können ("bleibt freigestellt"), ob sie von der IOP der Basisfunktionalitäten Gebrauch machen. Die nach Art. 7(5) DMA zwischen den Messaging-Diensten ermöglichte IOP darf den jeweiligen Nutzern dementsprechend nicht aufgezwungen werden. Art. 7(7) DMA enthält keine näheren Vorgaben dazu, wie die Entscheidungsfreiheit der Nutzer sichergestellt werden soll. Insbesondere stellt sich die Frage, ob die Anbieter ein Opt-in-Modell vorsehen müssen oder ob auch ein Opt-out-Modell den Anforderungen des Art. 7(7) DMA genügt.

Da die Herstellung von IOP mit der Verarbeitung personenbezogener Daten durch den jeweils anderen Anbieter verbunden ist, dürfte schon aus datenschutzrechtlichen Gründen ein Opt-in-Modell erforderlich sein, auch wenn dadurch ebenfalls erhebliche Herausforderungen bei der praktischen Umsetzung aus Nutzerperspektive abzusehen sind, z. B. beim Handling von Gruppenfunktionalitäten oder für Einwilligungsanforderungen bei ggf. nach und nach im Laufe der Zeit hinzukommenden Messaging-Diensten. Für die datenschutzrechtlich vorrangige Sicht spricht aber auch der in Art. 7(8) DMA enthaltene Hinweis, dass die Sammlung und der Austausch von Daten für die Zwecke der IOP in vollem Umfang den Vorgaben der DSGVO und der ePrivacy-Richtlinie genügen müssen. Die Entscheidung für oder gegen die IOP muss daher den Anforderungen an eine "freiwillige" Entscheidung im Sinne von Art. 7 DSGVO genügen. Soweit die IOP mehrere Basisfunktionalitäten erfasst, müsste auch eine differenzierte An- und Abwahl einzelner Funktionalitäten ermöglicht werden. Entscheidet sich der Nutzer für die Nutzung der interoperablen Basisfunktionalitäten, sind die Sammlung und der Austausch der Daten strikt auf das für die Herstellung von IOP erforderliche Maß zu beschränken (Art. 7(8) DMA). Dies entspricht dem in Art. 5(1)(c) DSGVO verankerten Grundsatz der Datenminimierung.

Art. 7(9) DMA ergänzt die genannten Regelungen um eine allgemeine Vorbehaltsklausel. Danach sind Gatekeeper nicht daran gehindert, Maßnahmen zu ergreifen um sicherzustellen, dass Drittanbieter den Datenschutz, die Integrität und die Sicherheit der Messaging-Dienste nicht gefährden. Voraussetzung ist, dass es sich um Maßnahmen handelt, die "unbedingt erforderlich und angemessen" sind. Die Vorbehaltsklausel dürfte es etwa ermöglichen, die zunächst eingeräumte IOP wieder einzuschränken, wenn begründete Zweifel an der Gewährleistung von Datenschutz und Datensicherheit durch den Drittanbieter auftreten. Ein Verfahren für eine solche Suspendierung der IOP regelt Art. 7(9) nicht, sondern verlangt lediglich, dass die Maßnahmen ordnungsgemäß „hinreichend begründet" werden. Aus Gründen der Verhältnismäßigkeit wird man aber verlangen können, dass der Gatekeeper bei auftretenden Sicherheitsproblemen zunächst eine

Abhilfe seitens des Drittanbieters verlangt. Eine dauerhafte Beendigung der IOP kommt nur als ultima ratio in Betracht.

4.4.3 Handlungsempfehlungen

Aufgrund der langen Reihe an Risiken von horizontalen IOP-Verpflichtungen ist es grundsätzlich zu begrüßen, dass der DMA einen vorsichtigen Ansatz im Bereich der Messaging-Dienste verfolgt. Nicht zuletzt durch die nun vorgesehenen IOP-Verpflichtungen im finalen Beschluss des DMA steht der Aspekt der Ende-zu-Ende-Verschlüsselung im Mittelpunkt der Diskussionen und scheint häufig einen Scheidepunkt in der finalen Bewertung entsprechender Maßgaben darzustellen. Die IOP-Anforderung für Messaging-Dienste hat in der Branche ernsthafte Bedenken hervorgerufen, ob diese die Ende-zu-Ende-Verschlüsselung, die einige Messaging-Dienste eingeführt haben, sowie andere Sicherheits- und Anti-Spam-Maßnahmen untergraben würde.

Wie oben beschrieben, trifft der vorerst finale Beschluss des DMA nur noch gemäßigte Vorgaben, indem er unter anderem auf symmetrische Vorgaben und enge Standardisierung zunächst verzichtet und eine besondere Priorität auf den Erhalt eines hohen Sicherheitsniveaus und Wahlfreiheit der Nutzer legt. Hierbei ist zunächst festzuhalten, dass aus technischer Sicht keine klare oder einheitliche Definition vorherrscht, welche Aspekte und Angriffsmodelle tatsächlich unter dem Begriff „Sicherheitsniveau“ („level of security“) verstanden werden, z. B. können hierunter neben der Inhalteverschlüsselung die Nutzerauthentifizierung, (mangelndes) Vertrauen in schlüsselverwaltende Stellen oder das Anfallen von Metadaten fallen. Potentielle „Angreifer“ variieren dabei von Arbeitgebern, Ex-Partnern, über Konzerne hin zu eigenen oder fremden Regierungen (Muffett, 2022).

Dies gilt auch für die „Ende-zu-Ende-Verschlüsselung“ selbst. Je nach Anwendung und deren Nutzenversprechen, Nutzer(basis) und Infrastruktur können teils stark unterschiedliche „Enden“, Angriffs- und Angreifermodelle relevant sein, die auch unterschiedliche Abwägungen auf technischer Ebene implizieren (vgl. Burgess, 2022; Muffett, 2022). So sind einheitliche technische Lösungen zwar auf einer abstrakten Ebene grundsätzlich denkbar, stoßen aber im Detail und der praktischen Implementierung an ihre Grenzen, wie auch von WIK-Consult befragte Experten bestätigen. Entsprechende Kompromisse und eine Erweiterung der beteiligten Parteien und Akteure implizieren daher letztendlich auch eine Erweiterung möglicher Angriffspunkte und bedingen damit im Zweifel ein Absinken von Sicherheitsniveaus.

Gerade für den Erhalt etwaiger Ende-zu-Ende-Verschlüsselungen in Verbindung mit einem sicheren Schlüsselaustausch scheint die Kombination ohne eine (de jure oder de facto) Einigung auf einen bestehenden oder neuen Standard technisch in der praktischen Implementierung nahezu ausgeschlossen zu sein. Bei IOP-Vorschriften, die eine Standardisierung nicht explizit vorsehen bzw. ohne Koordination auf einen einheitlichen Standard eingeführt werden, sei eine Erhaltung einer Ende-zu-Ende-Verschlüsselung letzt-

endlich nicht gewährleistet, wie auch die von WIK-Consult befragten Experten für Verschlüsselungstechnologien bestätigen. Die Implementierungskosten für eine solche einheitliche Lösung wären hoch, der Aufwand sei laut einem der Experten in diesem Falle vergleichbar mit einer Neuentwicklung einer gemeinsamen interoperablen Messenger-Plattform und belaufe sich auf ca. 5 Jahre. Laut einem anderen Experten könne eine Standardisierung inklusive Verschlüsselung auf dem Basisniveau von bilateralen Nachrichten im besten denkbaren Fall in 2-3 Jahren erreicht werden. Selbst dies setzt aber voraus, dass die beteiligten Marktakteure grundsätzlich den Willen haben, sich auf einen gemeinsamen Standard zu einigen.

Einige Aspekte der grundlegenden technischen Herausforderung bei der Ende-zu-Ende-Verschlüsselung, insbesondere für die Implementierung in einem interoperablen Umfeld, wurden bereits in Kapitel 4.2.4 diskutiert. Auch die Internet Society (2022) äußert sich kritisch bezüglich einer grundsätzlichen Vereinbarkeit von Messenger-IOP und der Ende-zu-Ende-Verschlüsselung. Alternativ müssten alternative Anbieter bzw. Entrants vollständig die Standards von Gatekeepern annehmen und würden dadurch weiter hinein in die Abhängigkeit von proprietären Systemen gezwungen. Auch aus dem in Kapitel 4.3.1.2 diskutierten Whitepaper von WhatsApp (2021) geht hervor, dass die Ende-zu-Ende-Verschlüsselung über Schnittstellen selbst innerhalb eines Konzerns zumindest nicht trivial ist. Dieser Eindruck wird verstärkt durch die Medienberichte nach denen Meta mit der angekündigten Integration seiner Dienste und der konzerninternen IOP aufgrund der Komplexität des technischen Ausbaus nur bedingt Fortschritte erzielt (Ahmed, 2021).

Auch aktive Befürworter von IOP-Vorschriften für Messaging-Dienste erkennen die Wichtigkeit, aber auch die Schwierigkeit bei der Vereinbarung von Messenger-IOP und einer bestmöglichen Verschlüsselung an und räumen ein, dass eine adäquate, insbesondere verschlüsselungsgerechte Implementierung um „Jahre“ länger brauchen könne, als aktuell im DMA vorgesehen (vgl. z. B. Stoltz et al., 2022). Denkbar wäre alternativ auch ein proaktiver, informierter Verzicht auf eine Ende-zu-Ende-Verschlüsselung von Nutzerseite (Le Pape, 2022). Im Hinblick auf die bereits im Kontext der DSGVO und Cookie Bannern beobachteten Probleme um inflationär gegebene Einwilligungen wäre hier allerdings ein Absinken des durchschnittlichen Sicherheitsniveaus für Nutzer zu befürchten (Utz et al., 2019).

Entsprechend könnten die Fristen und der vorgesehene Zeitrahmen zu eng gefasst sein, insbesondere für Gruppennachrichten, deren Verschlüsselung bereits im nicht interoperablen Fall mit zusätzlichen Hürden bei der Skalierung verbunden ist (vgl. Kapitel 4.2.4). Artikel 7(6) trägt dieser Unsicherheit bereits teilweise Rechnung und sollte zunächst großzügig genutzt werden. Der Fokus auf Verbraucheraspekte wie den Erhalt der Verschlüsselung und Datensparsamkeit sollte dabei auch in der praktischen Umsetzung und Verfolgung aufrechterhalten werden. Hierbei besteht allerdings die Schwierigkeit, zwischen validen technischen Abwehrargumenten und möglichen Umgehungsstrategien zu unterscheiden. Zur Beurteilung, inwiefern eine verschlüsselungs- und datenschutzgerechte Implementierung von IOP tatsächlich technisch möglich und in angemessenem Rahmen

implementierbar ist, sollten daher verschiedene zentrale und unabhängige Organisationen einbezogen werden. Ebenso sollten die an anderen Stellen des DMA geforderten Transparenz- und Berichtspflichten für diesen Bereich ebenfalls konkretisiert werden.

Neben den APIs, die von den Messaging-Diensten selbst angeboten werden, gibt es zudem Intermediäre wie beispielsweise Tyntec, welche aggregiert den Zugang zu mehreren APIs bereitstellen. Über diese können dann etwaige Endkunden über ihren jeweilig präferierten Dienst kontaktiert werden (Tyntec, 2022). Auch hier ist jedoch zu berücksichtigen, dass die Nachrichten ausschließlich über Transportverschlüsselung verfügen, der Dienstleister entsprechend ebenfalls die Nachrichten unverschlüsselt einsehen kann.

Auch der Anspruch, die Entscheidungsfreiheit von Nutzern nicht durch verpflichtende IOP-Maßgaben einzuschränken, sollte in der Praxis beibehalten werden (vgl. persönliche digitale Souveränität). Die Kontrolle für Nutzer darüber, wer sie wann und wie kontaktieren darf und welche Daten innerhalb und außerhalb des genutzten Dienstes verwendet werden, sollte dabei klar und in verständlicher Weise ermöglicht werden. Um dies zu gewährleisten, sollten für Verbraucher Opt-in-Lösungen eingefordert werden (vgl. auch Internet Society, 2022) . Außerdem können bzgl. Datenabflüssen und der Weiterverwendung von Daten Kontroll- und Transparenzmechanismen nötig sein, sofern dies nicht auf technischem Wege „by design“ lösbar ist.

Zwar enthält der DMA eine Vorbehaltsklausel und fordert „zumutbare“ Anträge von Drittanbietern ein (vgl. Kapitel 4.4.2), allerdings könnte eine Verdeutlichung bzw. sogar regulatorische Prüf- und Auswahlverfahren nötig sein, um Missbrauch effektiv zu verhindern (vgl. u. a. Barczentewicz, 2022). Prinzipiell denkbar wären hier Anbieter von Spam- und Massennachrichten, die eine IOP-Anfrage als Schlupfloch nutzen könnten und ggf. unter wechselnden Namen und Firmenkonstrukten erneute Anfragen stellen könnten. Auch auf Nutzerebene kann die Identifizierung von Spam-Akteuren in dezentralen Systemen erschwert werden, wie das Beispiel des E-Mail-Ökosystems zeigt.

Insgesamt besteht die Gefahr der IOP-Maßgaben des DMA möglicherweise eher darin, dass die Regelungen in der Praxis wegen mangelnder Nachfrage durch Konkurrenzdienste und der mangelnden adäquaten technischen Implementierungsmöglichkeit vorerst nicht die erwarteten praktischen Implikationen haben könnten. Hingegen steht eine zu starke Vereinheitlichung von Diensten oder ein Absinken des allgemeinen Sicherheitsniveaus zunächst nicht zu befürchten, sofern die Priorisierung z. B. der Ende-zu-Ende-Verschlüsselung auch in der praktischen Umsetzung beibehalten wird. Diese Regelungen zum gleichzeitigen Erhalt von Datenschutz und Datensicherheit sollten in der Praxis im Zweifel tatsächlich vorranging gegenüber einem IOP-Ziel selbst beachtet werden. Auch bestehende Regelungen wie die DSGVO dürfen dabei nicht beeinträchtigt werden.

Ein weiterer wohl nicht beabsichtigter Effekt könnte darin bestehen, dass kleinere konkurrierende Anbieter die Möglichkeit zur IOP nicht aufgreifen (vgl. das aktiv bekundete fehlende Interesse von den Anbietern Signal und Threema, Kapitel 4.1.4), sondern von

Gatekeepern auch untereinander aktiviert werden könnte. Ob diese Möglichkeit intendiert oder möglich wäre, bleibt unklar und die möglichen Auswirkungen komplex. So könnten z. B. Meta oder Alphabet den Zugang zu Apples iMessage einfordern, was einerseits Apples Wettbewerbsposition und Exklusivität schwächen würde, aber auch unter anderem datenbezogene Bedenken gegenüber Meta und Alphabet verstärken könnte.

Multi-Messenger können zwar nicht unter einem IOP-Ansatz im engeren Sinne subsumiert werden, können aber dazu dienen, die Kosten von Multi-Homing durch eine integrierte Benutzeroberfläche weiter zu senken, ohne die Datensicherheit der Nutzer durch eine Aufweichung der Ende-zu-Ende Verschlüsselung einzuschränken, wenn die Entschlüsselung direkt auf den Endnutzer-Geräten umgesetzt wird. Dass diese Applikationen in Zukunft durch IOP-Vorschriften mit entsprechenden Dokumentationen, sowie dem Ausschluss der Verhinderung entsprechender Zugriffsmöglichkeiten breiter ermöglicht werden, erscheint als ein zielführender praktischer Lösungsansatz.

5 Schlussfolgerungen und Ausblick

Die Studie bietet einen Überblick über die komplexen Fragestellungen, die das Konzept der IOP und eine mögliche Verpflichtung zu solcher aufwirft, insbesondere im Kontext der heutigen Internet- und Plattformökonomie und Online-Kommunikationsdiensten. Dabei werden mögliche Auswirkungen von IOP-Vorschriften für Wettbewerb und Innovation sowie für digitale Souveränität dargestellt und die potenzielle Notwendigkeit solcher Vorschriften untersucht. Im Fokus stehen dabei insbesondere digitale Dienste aus dem Bereich der Kommunikationsdienste sowie der Plattformökonomie.

5.1 Interoperabilitätskonzepte

Bereits beim Begriffsverständnis und hinsichtlich der verschiedenen Konzepte von IOP aus technischer, rechtlicher und ökonomischer Perspektive ergibt sich ein breites, teils uneinheitliches Bild. Insbesondere im ökonomischen und rechtlichen Kontext werden der Begriff der IOP und verwandte Konzepte wie Kompatibilität und Portabilität in einem Atemzug oder sogar explizit synonym verwendet. Andere Definitionen heben neben einer Austauschfähigkeit von Daten und Informationen zwischen Systemen auch konkreter deren Nutzbarkeit und eine damit einhergehende Schnittmenge von Funktionalität hervor. Die sich etablierende Unterteilung in Daten-IOP und Protokoll-IOP zielt auf diese verschiedenen Verständnisse ab. Von partieller IOP, bei der nur einzelne oder eine Teilmenge aller Funktionalitäten für Nutzer anderer Anwendungen oder Systeme nutzbar sind bis hin zu “vollständiger Protokoll-IOP" mit einem tieferen Level an Integration und Standardisierung stellt sich die IOP dabei häufig als Kontinuum dar.

Als abgrenzende Arbeitsdefinition zwischen Kompatibilität und IOP wurde in der Studie das folgende Verständnis entwickelt. Kompatibilität wird hier als die störungsfreie Arbeit und konsistente Austauschfähigkeit von Komponenten, Anwendungen und Systemen insbesondere innerhalb einer Umgebung verstanden. Unter IOP wird die Zusammenarbeit und Kombinierbarkeit von Komponenten, Anwendungen und Systemen verstanden, welche sich auch in unterschiedlichen Umgebungen befinden können. Unter einer Umgebung kann im Kontext digitaler Märkte der technische Einflussbereich oder das Ökosystem eines Unternehmens verstanden werden.

Des Weiteren geht IOP über die punktuelle, meist einseitige, (Daten-)Portabilität hinaus und grenzt sich von dieser durch einen kontinuierlichen, meist wechselseitigen, Datenaustausch ab. Neben dieser wechsel- bzw. zweiseitigen IOP finden sich aber auch einseitige Formen von IOP, wie z. B. sogenannte adversariale IOP durch Reverse Engineering oder das Teilen von externen Medieninhalten auf Social Media Plattformen.

In einem technischen Kontext werden für die Unterscheidung in einseitige und zweiseitige IOP auch die Begrifflichkeiten asymmetrische und symmetrische IOP verwendet. Der Begriff asymmetrischer Regelungen findet ebenfalls im juristischen Sinne Anwendung.

So stellt z. B. die im DMA vorgesehene IOP-Verpflichtung für sogenannte „Gatekeeper“ eine solche asymmetrische Verpflichtung dar, während eine symmetrische Regelung alle Marktteilnehmer direkt betreffen würde.

Wenn eine Plattform (komplementären) Drittanbietern auf vor- und nachgelagerten Wertschöpfungsstufen Zugang gewährt, spricht man von vertikaler IOP. Hier ist festzuhalten, dass im Fall von vertikalem Wettbewerb keine symmetrische IOP möglich ist, da hier der Zugang zu einem essenziellen Teil der Wertschöpfung unter Kontrolle eines Unternehmens im Vordergrund steht. Bei gleichartigen (substitutiven) Diensten, die sich in direktem Wettbewerb zueinander befinden, spricht man von horizontaler IOP. Im Fall horizontaler Wettbewerbsverhältnisse ist zu klären, ob eine IOP-Verpflichtung nur für bestimmte Unternehmen gelten soll, welche eine starke Marktposition innehaben (z. B. Finanzkraft, Anzahl Nutzer etc.), oder gleichermaßen für alle Anbieter eines bestimmten Diensttyps (vgl. auch Tabelle 3-3).

Entsprechend der Wettbewerbssituation (horizontal oder vertikal) sind jeweils unterschiedliche ökonomische Effekte in der Beurteilung zu berücksichtigen bzw. zu gewichten. Allerdings lässt sich auch festhalten, dass gerade im Kontext von Plattformen und der Herausbildung von Multi-Produkt-Ökosystemen die Grenzen zwischen horizontalen und vertikalen Firmenbeziehungen immer stärker verschwimmen. Dabei haben vordergründig horizontal konkurrierende Dienste häufig auch verschiedenste Arten von vertikalen Beziehungen, womit der Wettbewerb auf anderen Marktstufen eine wichtige Rolle spielen kann.

5.2 Interoperabilität und Interoperabilitätsverpflichtungen in der Plattformökonomie

Die grundlegende erwünschte Wirkung von IOP aus einer Wohlfahrtsperspektive ist das Auflösen firmenspezifischer Netzwerkeffekte auf horizontaler und auch vertikaler Ebene, sodass resultierende Nutzengewinne aus der Größe des Netzwerks den Konsumenten aller interoperablen Dienste zugutekommen. Für Verbraucher sollen erleichterte Anbieterwechsel ermöglicht, Wahlmöglichkeiten auf horizontaler und vertikaler Ebene durch Innovation geschaffen und der Preis- und Qualitätswettbewerb intensiviert werden. Dabei kann IOP Wettbewerb *im* Markt etablieren und dem Kippen von Märkten vorbeugen bzw. eine vorhandene Marktkonzentration abschwächen. Allerdings schränkt die Möglichkeit und das tatsächliche Niveau von Multi-Homing (der parallelen Nutzung verschiedener gleichartiger Dienste durch Anwender) die Relevanz und Notwendigkeit von IOP-Vorgaben ein, da Anwender auch auf diesem Weg von unterschiedlichen Funktionalitäten und dem Zugang zu unterschiedlichen Anwendern profitieren können.

Die digitale Souveränität für Verbraucher in Form eines selbstbestimmten Handels kann durch IOP gestärkt werden, wenn dadurch Lock-in-Effekte reduziert werden und die

Wahlfreiheit gestärkt wird. Wahlmöglichkeiten können aber durch horizontalen Wettbewerb und Substitutionsmöglichkeiten, sowie durch modulare Wahlmöglichkeiten auf vertikaler Ebene gegeben sein, die einen Mix-and-Match-Ansatz, also die Kombination von komplementären Produkten und Diensten verschiedener Anbieter auf verschiedenen Wertschöpfungsstufen, ermöglichen.

Die besondere Relevanz von Daten stellt eine Besonderheit von Plattformdiensten und -ökosystemen dar, die durch datengetriebene Lerneffekte geprägt sind. Dabei verwenden Firmen Nutzerdaten für Produktverbesserungen und/oder gestiegene Vermarktungschancen, sowohl bei der kontinuierlichen Nutzung innerhalb eines Dienstes als auch insbesondere bei der Verknüpfung über verschiedene Dienste, Produkte, Marktstufen und Kontexte hinweg. Daher nimmt die Freigabe und Verwendung eigener (persönlicher) Daten eine immer größere Rolle für Nutzer ein. Für ein selbstbestimmtes Handeln sind hier größtmögliche Transparenz und Kontrolle darüber notwendig, welche Daten wann und von wem gesammelt, genutzt oder weitergegeben werden. Eine IOP und damit das Zusammenwirken von mehr Akteuren kann dies grundsätzlich erschweren. Die transparente und ausdrückliche Einholung einer Zustimmung, wenn Daten an andere Dienste weitergegeben werden, kann dies zwar erreichen, erhöht aber auch die Komplexität für Verbraucher. In einem interoperablen Netzwerk haben Anbieter ggf. Zugriff auf Metadaten (Angaben zu Absender und Empfänger der Information, Zeitpunkt der Interaktion, Standort der Nutzer etc.), zu denen die Nutzer in keiner direkten Geschäftsbeziehung stehen. Damit kann sich im interoperablen Umfeld der Umfang der Datenverarbeitung durch Dritte der unmittelbaren Kontrolle durch die Nutzer entziehen.

Aber auch die klassischen direkten und indirekten Netzwerkeffekte spielen weiterhin eine fundamentale und wachsende Rolle im Kontext von mehrseitigen Plattformen und auch einseitigen Kommunikationsnetzwerken. Diese stellen in der Regel das Kernargument für eine mögliche Einführung von IOP-Verpflichtungen dar. Auch wenn Netzwerkeffekte den Effekt des Marktkippens („Market tipping“) und damit für sich gesehen eine Monopolisierungstendenz bewirken können, und einige Firmen sogar immer größere in sich geschlossene Ökosysteme („walled gardens“) anzustreben scheinen, ist es unklar, ob dies (ursächlich) zu Marktkonzentration führt und ob diese im konkreten Fall tatsächlich schädlich für Wohlfahrt und/oder Konsumentenrente ist. So müssen für eine Gesamtbeurteilung möglicher IOP-Pflichten eine Reihe weiterer, ggf. moderierender oder gegenläufiger, Faktoren berücksichtigt werden.

Gerade bei digitalen Diensten können die unmittelbaren Kosten des Multi-Homings häufig gering (beispielsweise Installieren einer weiteren Applikation auf dem bestehenden Smartphone) und vorrangig nicht-monetärer Natur sein (z. B. Registrierungs-, Lern- und andere Transaktionskosten). Da IOP den Anreiz zum Multi-Homing deutlich abschwächen kann, ist aus dieser Perspektive Vorsicht für entsprechende IOP-Verpflichtungen geboten. Wenn durch IOP aber substanzielle Kosten von Multi-Homing vermieden werden können, kann dies durchaus wohlfahrtsfördernd sein. Ein Multi-Homing zwischen

verschiedenen mobilen Betriebssystemen findet üblicherweise z. B. nicht statt, da dafür teure Hardware, hier in Form eines weiteren Smartphones, nötig wäre.

Wird ein zu starkes Maß an Standardisierung für die IOP benötigt, kann IOP im horizontalen Wettbewerb die Produktvielfalt und innovative Differenzierungsmöglichkeiten einschränken, auch zu Lasten von Verbrauchern und innovativen Unternehmen. Eine zu starke Homogenisierung von Funktionalitäten kann dazu führen, dass Kunden sogar weniger geneigt sind, den Anbieter zu wechseln und letztendlich der Konsumentennutzen durch eine geringere Produktvielfalt sinkt. Für die Definition von Kernfunktionen, die ggf. interoperabel gestaltet werden sollen, resultiert dabei ein Zielkonflikt. Wird die Innovation in Produktdimensionen gelenkt, die für Nutzer nicht attraktiv sind, besteht das besagte Problem der Homogenisierung. Wird die Innovation in für Nutzer relevante Produktdimensionen gelenkt, die Nachfragewirkungen induzieren, wird ggf. das Ziel einer Reduktion von firmenspezifischen Netzwerkeffekten konterkariert und auch die vorherige Definition “relevanter” Kernfunktionen in Frage gestellt.

Auf vertikaler Ebene kann IOP aber Planungssicherheit und Nachfragepotenzial auf vor- und nachgelagerten Märkten schaffen und somit Innovationen komplementärer Anbieter fördern. Hier besteht allerdings gerade im Hinblick auf die Plattformökonomie das Problem der Verbreitung von vertikal integrierten Diensten und Produkten. Zunächst freiwillig bereitgestellte IOP kann hier strategisch und diskriminierend genutzt werden, um Wettbewerber auf nachgelagerten Märkten zu schädigen, z. B. indem zunächst in frühen Wachstumsphasen von Plattformen Attraktivität durch die Öffnung gegenüber Komplementoren und Nutzerkreisen anderer Dienste generiert wird. Je nach Marktanteilen und der etwaigen Integration eigener Angebote werden Schnittstellen dann teilweise im späteren Verlauf wieder geschlossen oder nur einseitig angeboten, um z. B. eine strategische Steuerung des Aufmerksamkeitsflusses zu erreichen. Auch kann es gerade unter IOP dazu kommen, dass (dominante) Plattformen bzw. Anbieter die interoperablen Produkte oder Funktionen externer Firmen kopieren und in ihr eigenes Angebot integrieren („Sherlocking“), so dass sich kleinere Firmen ggf. nicht im Markt differenzieren und halten können und die Dominanzposition letztendlich sogar gestärkt wird. Grundsätzlich spricht ein hohes Ausmaß an verfügbarer freiwilliger IOP aber tendenziell gegen eine ex-ante Verpflichtung, während ein hohes Level an adversarialer IOP oder sogar aktive Verhinderungsversuche solcher ein Anzeichen für einen nötigen Eingriff darstellen können.

Außerdem zu beachten sind anfallende Kosten für die Einführung von IOP, unter anderem Anpassungs- Verhandlungs- und Pflegekosten, die insbesondere den Markteintritt für kleine Unternehmen sogar erschweren statt erleichtern können. Auch der Prozess einer Standardisierung kann kleine und insbesondere potenzielle Anbieter benachteiligen, wenn dieser durch bestehende, (markt-)mächtige Firmen geprägt wird und kann sogar Kollusionsgefahren und “Patent Hold-up" bewirken, wenn Firmen eigene Technologien und Patente gegen Lizenzzahlungen in Standarddefinition einbringen können. Neben den Incumbents sollten auch weitere Stakeholder wie potenzielle Wettbewerber, Verbraucherorganisationen und unabhängige technologische Expertise einbezogen werden.

Darüber hinaus ergeben sich bei Zugangsverpflichtungen auch regulatorische Kosten des Monitorings und der Durchsetzung der Verpflichtungen, da davon ausgegangen werden muss, dass das Zugangsverpflichtungen strategisch unterlaufen werden, z.B. durch bewusste technische Störung der IOP-Schnittstellen.

5.3 Interoperabilität bei nummernunabhängigen interpersonellen Telekommunikationsdiensten

Die Studie hat sich weiterhin insbesondere mit dem Marktsegment der Online-Kommunikationsdienste und einer IOP-Verpflichtung in diesem Bereich beschäftigt. Der Fokus liegt auf Online-Kommunikationsdiensten, die entsprechend der diskutierten Prüfkriterien ein relativ homogenes Produkt darstellen, deren Anbieter vordergründig in horizontalem Wettbewerb stehen. Hierbei findet sich insbesondere im deutschen und europäischen Markt eine starke Marktkonzentration auf den Meta-Konzern, der die Messaging-Dienste WhatsApp, Facebook Messenger sowie Instagram Messages unter sich vereint und somit auch in verschiedenen Abstufungen eine vertikale Integration mit den sozialen Netzwerken Facebook und Instagram bzw. dem Meta-Konzern insgesamt vorliegt.

Auch im weiteren Marktsegment findet sich ein diverses Feld an unterschiedlichen Anbindungs- und Monetarisierungsformen. Telegram beispielsweise testet weiterhin verschiedene Ansätze wie z. B. ein Freemium-Modell. Einige kleinere Dienste bzw. die entsprechenden Apps werden gegen direkte Einmal- oder regelmäßige Zahlungen angeboten (Threema, Element). Nicht nur in Bezug auf juristische Definitionen von NI-ICS, die auf eine Leistungserbringung „*gewöhnlich* gegen Entgelt“ abzielen, bleibt der Umgang mit anderen Formen der Finanzierung häufig unklar. Während der Meta-Konzern insgesamt seine Einnahmen hauptsächlich aus Werbeeinnahmen generiert, steht hinter Signal ein non-profit/spendenbasierter Ansatz. Im Fall von iMessage werden durch den Dienst selbst ebenfalls keine Einnahmen generiert, er dient aber zur Steigerung der Attraktivität und Exklusivität des Apple-Ökosystems, das durch Einnahmen im Hardware- und Service-Bereich geprägt ist. Daher ist ein Einbezug von Diensten mit Formen indirekter Einnahmen und eine Abschätzung der damit jeweils verbundenen Anreize und Wettbewerbswirkungen nötig. Während gerade für Anbieter mit direkter Monetarisierung die Differenzierungsmöglichkeit essenziell ist und die Exklusivität von iMessage durch Erzeugung eines Kunden-Lock-Ins und firmenspezifischen Netzwerkeffekten vor allem im vorgelagerten Wettbewerb zwischen Betriebs- und Hardwaresystemen relevant ist, können Modelle, die auf Aufmerksamkeit und/oder Daten von Nutzern basieren, durch IOP mit anderen Diensten und dabei entstehende Metadaten sogar profitieren.

Auch wenn ein Messaging-Dienst durch die Beschränkung auf direkte Netzwerkeffekte für sich gesehen nicht die klassische Definition einer Plattform im ökonomischen Sinne erfüllt, ist dieser Markt in der Praxis doch durch „echte“ Plattformen geprägt, da durch die Einbettung in Plattformökosysteme verschiedenartige Formen indirekter Netzwerkeffekte ebenfalls eine essenzielle Rolle einnehmen können. Die Bewegung hin zur Prävalenz

von Ökosystem-Messengern erfolgt dabei insbesondere international gesehen aus zwei Richtungen: Einerseits werden ursprüngliche Single-Purpose Messenger durch hinzukommende Funktionalitäten, Monetarisierungsarten und Firmenausrichtungen selbst zu Plattformen und/oder Ökosystemen. Andererseits erweitern bestehende multi-sektoral agierende Ökosysteme ihr Portfolio um Messengerfunktionen.

In Bezug auf die Einstufung einzelner Dienste als NI-ICS (sei es als Verpflichteter oder als Anspruchnehmer) muss in der Verwaltungspraxis teilweise noch Rechtsklarheit geschaffen werden. So stellt z. B. Telegram einen Grenzfall zwischen Individual- und Massenkommunikation dar, dessen Kanal- und offene Gruppenfunktionen als „öffentlich“ im Rahmen des DSA einzustufen ist. Bilaterale Kommunikation und private Gruppen stellen hingegen klassische Messenger-Funktionen dar.

Auch die Grenzen zwischen offenen (Massenkommunikation, z. B. soziale Medien) und geschlossenen (Individualkommunikation) Nutzergruppen verschwimmen dabei häufig. Sowohl bei sozialen Netzwerken als auch bei Messaging-Diensten lassen sich Funktionalitäten beobachten, welche geschlossene Nutzergruppen ermöglichen. Umgekehrt ist auch zwischen einzelnen Nutzern in sozialen Netzwerken der Austausch von Direktnachrichten möglich. Auch die Kriterien eines interaktiven Austauschs bzw. einer Antwortmöglichkeit und die Beschränkung auf eine endliche Zahl von Personen aus der NI-ICS Definition des EECC führen nicht immer zu einer klaren Zuordnung, wie das Beispiel Telegram zeigt. Von der rechtlichen Definition z. B. im Rahmen des EECC ist außerdem die Kommunikation ausgeschlossen, die nur eine „untergeordnete Nebenfunktion“ darstellt und untrennbar mit einem anderen Dienst verbunden ist. Neben eindeutigen Fällen wie der Chatfunktion eines Online-Spiels kann es aber auch hier zu Grenzfällen oder perspektivisch zu Umgehungsmöglichkeiten kommen, z. B. im Fall von Instagram Messages. Wie die Nutzungszahlen zeigen, wird die Funktion z. B. in Deutschland sogar häufiger genutzt als viele dedizierte Messenger.

In Bezug auf das Multi-Homing stellt sich im Markt ein differenziertes Bild dar. Multi-Homing ist aufgrund der häufig gratis oder zu geringen Kosten nutzbaren Dienste relativ einfach möglich und auf Diensteebene nutzen z. B. in Deutschland ca. 75% der Nutzer mindestens zwei Online-Kommunikationsdienste, während im Durchschnitt sogar knapp vier Dienste verwendet werden. Auf Unternehmensebene reduzieren sich diese Zahlen auf immerhin noch 61% der Nutzer und knapp drei Dienste im Durchschnitt. Die Dominanz des Meta-Konzerns, der die Dienste WhatsApp, Facebook Messenger und Instagram (Messages) unter sich vereint, zeigt sich auch darin, dass 80% der Nutzer in Deutschland mindestens einen dieser drei Dienste verwenden. Dienste anderer Unternehmen nutzen jeweils nur bis zu 30% Befragten (Microsoft-Dienste), oder weit weniger (sonstige Dienste). Empirische Ergebnisse nach den Änderungen der Datenschutzbestimmungen von WhatsApp zeigen außerdem, dass alternative Dienste zwar verstärkt installiert und zunächst auch genutzt wurden, aber nur 0,5% der Nutzer WhatsApp tatsächlich verließen und die Applikation deinstallierten.

Dennoch lässt sich festhalten, dass Multi-Homing in Form des Ausprobierens und der parallelen Nutzung mehrerer Dienste in diesem Markt einerseits relativ einfach möglich und damit auch entsprechend bei einer Mehrheit der Nutzer verbreitet ist. Anbieter wie Signal konnten in den Markt einsteigen und ihre Nutzungszahlen in relevantem Ausmaß steigern. Zudem erlaubt eine hohe installierte Basis an Multi-Homing ein noch schnelleres Wechseln der Kunden von einem Messenger auf einen anderen und diszipliniert so die Marktmacht des dominanten Unternehmens. Da IOP den Anreiz zum Multi-Homing reduzieren kann, könnte es hier schlimmstenfalls zu einer Hemmung von Exploration und Verbreitung von neuen Diensten kommen sowie zu einer geringeren Disziplinierung von Marktmacht. Auch wenn WhatsApp bzw. die Dienste von Meta (nicht zuletzt durch deren Akquisitionsstrategie) weiterhin mit Abstand am stärksten verbreitet sind, besteht (potenzieller) Wettbewerbsdruck, der vermutlich unter anderem dazu beigetragen hat, dass WhatsApp die Ende-zu-Ende-Verschlüsselung eingeführt hat. Letztlich steht im Fokus aller IOP-Vorschriften ein potenzielles Marktversagen im Sinne eines funktionierenden Wettbewerbs im Markt, welches durch die Herstellung von IOP überwunden werden könnte. Sollten wie im Fall von Messaging-Diensten das Niveau von Multi-Homing vergleichsweise hoch und die Kosten von Multi-Homing gering sein, ist grundsätzlich von einem verhältnismäßig geringen Wohlfahrtsverlust für Verbraucher auszugehen, wenn ein anbieterübergreifender, interoperabler Austausch nicht möglich ist. Zudem bewahrt Multi-Homing den Wettbewerb um den Markt.

Vor allem im Vorfeld des DMA gab es verschiedene entsprechende Bedenken gegenüber einer angedachten IOP-Verpflichtung. Insbesondere einer symmetrischen, alle Unternehmen betreffenden, Verpflichtung standen Marktteilnehmer und Beobachter kritisch gegenüber, da diese zur besagten zu starken Homogenisierung führen würde. Hier wurde insbesondere befürchtet, dass alternative, datenschutzbewusste Anbieter dabei ihre Differenzierungsmöglichkeit verlieren könnten und in Bezug auf das allgemeine Sicherheits- und Datenschutzniveau ein zu “kleinster-gemeinsamer-Nenner” getroffen werden würde. Diesen Bedenken kommt der aktuelle Beschluss des DMA zunächst durch eine asymmetrische Verpflichtung ausschließlich gegenüber dominanten Anbietern entgegen, so dass alle anderen Anbieter frei und unabhängig in ihrer Teilnahmeentscheidung und damit der Ausgestaltung ihrer Funktionalität bleiben. So verkündeten Signal und Threema bereits, nicht von der IOP-Anbindung an Dienste wie WhatsApp und iMessage Gebrauch zu machen.

Da sich der Beschluss des DMA zunächst lediglich auf die Basisfunktionalität des reinen Austauschs von Nachrichten und Dateien beschränkt, wird auch hier eine größere Möglichkeit zur Ausdifferenzierung über diverse Zusatzfunktionen erhalten. Dies führt allerdings auch zu einem Konflikt mit dem ursprünglichen Ziel der Reduzierung von firmenspezifischen Netzwerkeffekte, da diese im Rahmen dieser Zusatzfunktionen dadurch erhalten bleiben. Andererseits wird der Innovationsanreiz, sich durch exklusive Funktionalitäten abzuheben bzw. im Vergleich zu konkurrierenden Anbietern nicht ins Hintertreffen zu geraten, konserviert.

Auch wenn eine umfassendere Standardisierung ebenfalls eine zuverlässige Planung und Berücksichtigung noch zu inkludierender Funktionen über die Zeit erfordern würde, wären die Kosten durch eine stückweise und gestaffelte Implementierung durch Ineffizienzen bei der Entwicklung bei später notwendigen Anpassungen möglicherweise langfristig höher.

Auf Nutzerseite soll ebenfalls die Entscheidungsfreiheit, ggf. je nach Anbieter interoperable Funktionen zu nutzen oder nicht, gewährleistet werden. Die Kontrolle für Nutzer darüber, wer sie wann und wie kontaktieren darf und welche Daten innerhalb und außerhalb des genutzten Dienstes verwendet werden, sollte dabei klar und in verständlicher Weise ermöglicht werden. Nach der juristischen Bewertung dürfte schon aus (datenschutz-)rechtlichen Gründen ein Opt-in-Modell erforderlich sein, was aber bisher nicht explizit verlangt wird. Im Falle einer resultierenden Opt-in-Verpflichtung wird die Zielerreichung von IOP nochmals geschmälert, da nicht alle Nutzer von der Möglichkeit Gebrauch machen werden und daher abermals firmenspezifische Netzwerkeffekte verbleiben. Außerdem sind erhebliche Herausforderungen bei der praktischen Umsetzung bzw. für die Komplexität aus Nutzerperspektive abzusehen, z. B. beim Handling von Gruppenfunktionalitäten oder für Einwilligungsanforderungen bei ggf. nach und nach im Laufe der Zeit hinzukommenden Anbietern.

Zwar legt der Beschluss im Wortlaut großen Wert auf den Erhalt von bestehenden Datenschutz- und -sicherheitsniveaus und einer ggf. bestehenden Ende-zu-Ende-Verschlüsselung, die auch im Fall eines interoperablen Anschlusses erhalten werden soll und deren Erhalt Vorrang haben sollte. Dabei wird in der anhaltenden Diskussion aber häufig in Frage gestellt, ob die technischen Voraussetzungen für einen effizienten Funktions- und Datenaustausch im Sinne einer IOP für Messaging-Dienste überhaupt erreichbar sind. Die technische Komplexität von Messengern und insbesondere von einer von vielen Seiten angestrebten Ende-zu-Ende-Verschlüsselung scheinen sich daher zu einem neuralgischen Punkt zu entwickeln. Die vorgesehene Implementierung im DMA anhand von APIs dürfte dabei trotz anders lautender Kommentare nicht ausreichend sein, um dabei gleichzeitig IOP, echte Ende-zu-Ende-Verschlüsselung sowie sichere Identitäts- und Schlüsselverwaltung zu gewährleisten. Die Komplexität all dieser Unterfangen steigt neben der Kernfunktion von 1:1 Textnachrichten im abzudeckenden Funktionsumfang (Gruppenchats, Dateianhänge, Audio-/Videocalls etc.). Zudem ist der Begriff des “Sicherheitsniveaus” sehr umfassend und weder in der Theorie noch in der Praxis hinreichend präzise definiert. Ein Öffnen von Schnittstellen und die Herstellung von IOP zu Dritten impliziert allgemein ein Absenken des Sicherheitsniveaus, da so zusätzliche Möglichkeiten für Angriffsvektoren entstehen und beteiligten Dritten vertraut werden muss (z. B. in Bezug auf die Nutzer-Authentifizierung und den Schlüsselaustausch).

Es ist daher fraglich, ob der im DMA verfolgte Ansatz, IOP zu etablieren, ohne das Datenschutz- und Sicherheitsniveau gegenüber dem Status Quo abzusenken, überhaupt umsetzbar ist. Nach Experteneinschätzungen kann eine Ende-zu-Ende-Verschlüsselung

nur durch vollständige (de jure oder de facto) Standardisierung erreicht werden, was insbesondere den geplanten Schnittstellen/API-Ansatz ausschließt. Die Etablierung einer solchen standardisierten interoperablen Umgebung könnte laut einem der von WIK-Consult befragten Experten wiederum ca. 5 Jahre benötigen. Ein weiterer befragter Experte nennt 2-3 Jahre als bestmöglichen Fall für eine standardisierte Verschlüsselungseinigung für einfache bilaterale Textnachrichten. Die technische Komplexität und die Anforderungen für eine Standardisierung, aber auch an die Rechenkapazitäten, steigen zudem deutlich, wenn nicht nur Textnachrichten, sondern auch Echtzeit-Audio- und Videoanrufe verschlüsselt werden sollen.

Eine kurzfristigere Lösung könnte prinzipiell über die verpflichtende Einführung eines bestehenden Standards (für Gatekeeper) erfolgen, mit entsprechend hohem Implementierungsaufwand für die betreffenden Gatekeeper. Aufgrund der besagten Diversität an verschiedenartigen Standards, Protokollen, Anwendungsgebieten, Nutzenversprechen und Angriffsmodellen wäre aber auch hier ein Marktinteresse, zumindest von bestehenden Anbietern, fraglich. Eine vollständige Standardisierung (unter Beteiligung der Gatekeeper und Entrants) mit dem Ziel auch bestehende proprietäre Features (welche derzeit nicht von offenen Standards abgedeckt werden) oder zukünftige Features von beiden Parteien abzudecken ist ein extrem aufwändiges und langwieriges Verfahren zu welchem im Anschluss noch einmal die Implementierungskosten hinzukommen würden.

Alternativ zu einer formalen Standardisierung oder freiwilligen Nutzung eines einheitlichen Standards müssten konkurrierende Anbieter direkt die bestehenden Protokolle der Gatekeeper übernehmen, die damit zu de facto Industriestandards erhoben werden würden. Es ist allerdings zu bezweifeln, dass ein solches Vorgehen Wettbewerb und Innovation begünstigt bzw. solche Systeme für kleine Anbieter überhaupt attraktiv sind. Signal und Threema haben entsprechenden Systemen bereits eine Absage erteilt. Damit besteht die Gefahr, dass solche Vorhaben in IOP-Systemen münden, welche unter hohen zeitlichen und finanziellen Kosten entwickelt werden müssen, aber letztlich am Markt nicht angenommen werden. Darüber hinaus werden Weiterentwicklungen des Standards, z.B. hinsichtlich der Vermeidung zukünftiger Sicherheitslücken, erschwert bzw. verzögert, wenn daran alle Unternehmen mitwirken, die den Standard implementieren.

Die erhoffte Wirkung der IOP würde letztendlich nur diese Kunden betreffen, deren genutzte Anbieter zunächst das Angebot der IOP wahrnehmen möchten und sie danach als Kunde selbst jeweils ihre Einwilligung erteilen würden. Die faktischen positiven Auswirkungen sind daher als erheblich begrenzter einzuschätzen und erzeugen durch die zunehmende Fragmentierung und komplexere Usability auch neue Kosten für Verbraucher.

Anhand des Beispiels von anbieterübergreifenden Gruppen wird insgesamt eine mögliche Impraktikabilität sowohl aus rechtlicher Einwilligungs- als auch aus technischer Hinsicht bzw. in deren Kombination deutlich. Angenommen, ein Alternativanbieter „C“ implementiert jeweils Referenzangebote der Gatekeeper „A“ und „B“, zwischen denen selbst allerdings weiterhin keine IOP herrscht. Möchte ein Nutzer in einer Gruppe von Nutzern

des Anbieters „C“ nun einen Nutzer des Anbieters „A“ einladen, müssten zunächst alle anderen Gruppenteilnehmer des Anbieters „C“ sowie der einzuladende Nutzer von „A“ individuell zustimmen, dass sie gegenüber dem jeweils anderen Anbieter angesprochen werden dürfen und die interoperable Funktion nutzen möchten. Unter diesen Bedingungen könnten also sowohl gemischte Gruppen aus Nutzern von „A“ und „C“ sowie analog aus Nutzern von „A“ und „B“ gebildet werden.

Inwiefern Nutzer von „A“ und „B“ dabei aber gleichzeitig zusammengebracht werden können oder sollen, bleibt allerdings unklar. Könnte ein Nutzer von „A“ innerhalb dieser Gruppe Nutzer von „B“ einladen? Innerhalb einer hypothetischen Gruppe mit Nutzern aus „A“, „B“ und „C“ würde de facto IOP zwischen diesen Nutzern herrschen, die aber de jure zwischen Anbietern „A“ und „B“ nicht besteht und daher keine entsprechende Einwilligung vorliegen kann. Eine damit notwendige Weiterleitung („Relay“-Funktion) zur praktischen Ermöglichung der Gruppenkommunikation durch Anbieter „C“ ist nicht vorgesehen und würde die Ende-zu-Ende-Verschlüsselung verletzen, wenn dabei zwischen verschiedenen Protokollen von „A“ und „B“ übersetzt werden müsste. Neben der Inhalteverschlüsselung im engeren Sinne wird insbesondere im multilateralen (Gruppen-)Kontext die Problematik der anbieterübergreifenden Nutzeridentifizierung und -authentifizierung sowie Contact Discovery deutlich (vgl. Kapitel 4.2 und 4.3). Hier ist aus Perspektive (der Nutzer) einzelner Anbieter grundsätzlich das Vertrauen in das korrekte Handling weiterer Parteien nötig und die jeweilige Einwilligungssituation insbesondere über mehr als zwei Anbieter hinweg unklar.

In der Gesamtabwägung bleibt es daher fraglich, wie eine IOP-Verpflichtung bei Messaging-Diensten und der im DMA verfolgte Ansatz zielführend umgesetzt werden können. Die neuen IOP-Verpflichtungen des DMA stehen auch in einem Spannungsverhältnis zu den wesentlich restriktiveren Regelungen des § 21 Abs. 2 TKG (vgl. Kapitel 3.1.2.1). Die größere Vorsicht im TKG bzw. EECC scheint im Vergleich auch unsere Erkenntnisse zu horizontaler IOP widerzuspiegeln. In Anbetracht der beschriebenen Risiken ist daher bei einer praktischen Umsetzung eine enge regulatorische Begleitung notwendig.

Der Fokus des DMA auf Verbraucheraspekte wie den Erhalt der Verschlüsselung und Datensparsamkeit sollte grundsätzlich auch in der praktischen Umsetzung und Verfolgung aufrechterhalten werden. Hierbei besteht allerdings die Schwierigkeit, zwischen validen technischen Abwehrargumenten und möglichen Umgehungsstrategien zu unterscheiden. Zur Beurteilung, inwiefern eine verschlüsselungs- und datenschutzgerechte Implementierung von IOP tatsächlich technisch möglich und in angemessenem Rahmen implementierbar ist, sollten daher verschiedene zentrale und unabhängige Organisationen einbezogen werden. Ebenso sollten die an anderen Stellen des DMA geforderten Transparenz- und Berichtspflichten möglicherweise für diesen Bereich ebenfalls konkretisiert werden.

Insbesondere zum im Vorfeld gängigsten Beispiel einer umfassenden IOP zwischen direkt konkurrierenden Diensten wie WhatsApp und Signal wird es voraussichtlich in absehbarer Zeit nicht kommen. Wahrscheinlicher ist hier die Nutzung durch Aggregationsdienste wie Beeper, die sich auch als Zwischenstufe zwischen rein horizontaler und rein vertikaler Ebene bezeichnen ließen, da sie als vertikaler Komplementär auftreten, der horizontale IOP ermöglicht. Dass Beeper bereits sein Interesse an einer Wahrnehmung der IOP-Möglichkeit bekundet hat, zeigt, dass auch die Marktakzeptanz weniger aus Richtung von direkten Rivalen auf der rein horizontalen Ebene stammt, sondern Modelle mit vertikalen Aspekten vielversprechender sein könnten. Hier bleibt abzuwarten, inwieweit der Marktfindungsprozess neuartige populäre Lösungen hervorbringen könnte. Theoretisch möglich wäre auch eine IOP zwischen Gatekeeper-Diensten. So werden sowohl WhatsApp als auch iMessage Referenzangebote veröffentlichen müssen, es ist allerdings fraglich, ob auf dieser Basis zueinander IOP umgesetzt werden würde. Wenn es dazu einen konkreten Anreiz geben würde, hätten die Unternehmen dies auch bereits ohne gesetzliche Verpflichtung umsetzen können. Einseitiges Interesse an einer Anbindung gegenüber iMessage hat allerdings Alphabet/Google bereits in der Vergangenheit bekundet und könnte hier einen neuen Versuch starten, für Android-Kunden einfache Konnektivität zu iMessage-Nutzern zu ermöglichen. Es ist unklar, inwiefern die Wahrnehmung einer IOP-Verpflichtung *zwischen* Gatekeepern tatsächlich durch den DMA intendiert ist, da dies die Vormachtstellung einiger Gatekeeper sogar noch stärken könnte.

Allgemein scheinen von Seiten der Gatekeeper, insbesondere im Hinblick auf WhatsApp und Facebook Messenger als größte potenzielle Ziele für IOP-Anfragen, zwei unterschiedliche Herangehensweisen möglich. Eine Möglichkeit besteht im (indirekten) Widerstand, u. a. durch eine nur minimale und formaljuristische Erfüllung der Vorgaben oder z. B. durch eine überkomplexe und unübersichtliche Gestaltung der geforderten Referenzangebote. Ein ähnliches entsprechendes Verhalten lässt sich aktuell im Rahmen des Rechtsstreits zwischen Apple und der niederländischen Marktaufsichtsbehörde ACM beobachten (vgl. ACM, 2019). Hier könnte auch die Möglichkeit bestehen, dass verschiedene Gatekeeper (explizit oder implizit) kolludieren und ihre jeweiligen Referenzangebote gezielt möglichst technisch unterschiedlich gestalten, um den Implementierungsaufwand für Konkurrenten und Entrants zu erhöhen.

Im Gegensatz dazu ist aber auch eine “Umarmungsstrategie“ denkbar, z. B. mit dem Ziel, möglichst viele neue (Meta-)Daten sammeln zu können. Als Extremform könnte neben dem Referenzangebot sogar eine fertige Implementierung als „White Label“-Lösungen angeboten werden, bei denen der Messaging-Dienst technisch auf der Infrastruktur des Gatekeepers aufbauen würde und lediglich das Branding bzw. die Benutzeroberfläche und die Vermarktung durch den alternativen Anbieter erfolgt. Entsprechende Lösungen sind z. B. im Bereich von Mobilfunktarifen oder Cloud-Anbietern verbreitet. Einer solchen Entwicklung sollte entgegengewirkt werden, da hier kein echter Infrastrukturwettbewerb stattfindet und allenfalls die Vormachtstellung einiger Gatekeeper über die verwendeten Technologien und über Daten gestärkt werden würde.

Als pragmatischer Mittelweg wäre laut einem der befragten Experten eine zentrale Koordinierungsstelle für Referenzangebote denkbar. Dabei könnte durch teilweise oder ganzheitliche Vorgaben, wie die Referenzangebote technisch zu gestalten sind, der Implementierungs- und Koordinierungsaufwand gesenkt werden, der durch eine Vielzahl von unterschiedlichen, jeweils nur für einen Anbieter geltenden Referenzangeboten entstehen würde. Insbesondere wenn gleichzeitig IOP mit mehreren Anbietern hergestellt werden soll, skalieren bilaterale Einigungen schlecht, da sich die Kombinationsmöglichkeiten verschiedener Angebote und ggf. verschiedener genutzter Protokolle potenzieren.

Für anfragende Unternehmen wäre der Implementierungsaufwand geringer, wenn beispielsweise alle Referenzangebote zumindest auf dem gleichen Standard wie z. B. dem Signal- oder Matrixprotokoll oder einem neu zu entwickelnden basieren müssten. Allerdings zeigt die aktuelle Entwicklung im Bereich der Verwendung des Signal-Protokolls, dass sich selbst aus der gleichen Basis entstandene Entwicklungen in essenziellen Details unterscheiden können, so dass ein Einigungs- und Anpassungsaufwand nicht gänzlich entfällt. Eine zentrale Vermittlungsstelle könnte z. B. die Referenzangebote steuern oder im Extremfall ein einheitliches Verschlüsselungs- oder Schlüsselaustauschverfahren einfordern, das zusätzlich zu den proprietären Angeboten als Fallback-Option implementiert werden muss. Auch dieser Ansatz wäre aber grundsätzlich mit den bereits benannten Problemen bei der Einigung auf eine einheitliche Lösung und bei der praktischen Implementierung und Betrieb verbunden. Hier stellt sich die Frage, wer im Zweifel ein solches einheitliches Verfahren bestimmt und die Vertrauenswürdigkeit der beteiligten Akteure bestätigt. Dieser Prozess könnte z. B. durch eine öffentliche Konsultation unterstützt werden.

Literaturverzeichnis

ACCC (2020). Digital Platform Services Inquiry - Online Messaging. Abgerufen von: 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. Abgerufen von: https://www.acm.nl/en/publications/acm-launches-investigation-abuse-dominance-apple-its-app-store. Abgerufen am: 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, S. 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, S. 20-32

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

Amazon (2022). Amazon - Selling Partner API. Abgerufen von: https://developer-docs.amazon.com/. Abgerufen am: 2022/03/31

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

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

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

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

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

Armstrong, Mark (2006). Competition in Two-Sided Markets. In: *The RAND Journal of Economics* 37, 3, S. 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). Abgerufen von: 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: S.

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, S. 116-131

Autorité de la Concurrence & CMA (2014). The Economics of open and closed systems. Abgerufen von: 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, S. 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. Abgerufen von: https://www.skadden.com/insights/publications/2020/12/cma-proposes-new-uk-competition-regime. Abgerufen am: 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, S. 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* S. 119-143

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

Belleflamme, Paul & Peitz, Martin (2019). Platform competition: Who benefits from multihoming? In: *International Journal of Industrial Organization* 64, S. 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, S. 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: S. 17-33

BEREC (2016). Report on OTT services. Abgerufen von: 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. Abgerufen von: https://hal.inria.fr/hal-02425247.

Bishop, DT & Cannings, Chris (1978). A generalized war of attrition. In: *Journal of theoretical biology* 70, 1, S. 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*. S. 506-507

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

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

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

Boudreau, Kevin (2010). Open platform strategies and innovation: Granting access vs. devolving control. In: *Management science* 56, 10, S. 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, S. 1409-1427

Bourreau, Marc; Krämer, Jan & Buiten, Miriam (2022). Interoperability in Digital Markets. Abgerufen von: 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,. Abgerufen von: https://ec.europa.eu/commission/commissioners/sites/commcwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf. Abgerufen am: 2022/07/06

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

Brown, Ian (2020). Interoperability as a tool for competition regulation. In: *OFA Research Paper* S. 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, S. 1580-1596

BSI (2021). Moderne Messenger – heute verschlüsselt , morgen interoperabel ? Abgerufen von: 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“. Abgerufen von: 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. Abgerufen von: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile.

Bundesnetzagentur (2021). Interoperabilität zwischen Messengerdiensten Überblick der Potenziale und Herausforderungen. Abgerufen von: 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. Abgerufen von: 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. Abgerufen von: https://www.wired.co.uk/article/dma-interoperability-messaging-imessage-whatsapp. Abgerufen am: 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, S. 15

BusinessWire (2021). The Connectivity Standards Alliance Unveils Matter, Formerly Known as Project CHIP. Abgerufen von: https://www.businesswire.com/news/home/20210511005928/en/The-Connectivity-Standards-Alliance-Unveils-Matter-Formerly-Known-as-Project-CHIP. Abgerufen am: 2022/05/31

Cadwalladr, Carole & Graham-Harrison, Emma (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Abgerufen von: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Abgerufen am: 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, S. 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, S. 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, S. 987-1022

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

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

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

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

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

Cocorada, Sorin (2018). Signal Messanger Architecture – IT Security Operations. Abgerufen von: https://sorincocorada.ro/signal-messanger-architecture/. Abgerufen am: 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, S. 224-239

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

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

CSA (2022). CSA Mitglieder. Abgerufen von: https://csa-iot.org/members/. Abgerufen am: 2022/07/06

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

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

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

David, Paul A. (1985). Clio and the Economics of QWERTY. In: *The American Economic Review* 75, 2, S. 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, S. 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, S. 209-227

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

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

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

Doganoglu, Toker & Wright, Julian (2006). Multihoming and compatibility. In: *International Journal of Industrial Organization* 24, 1, S. 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, S. 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". Abgerufen von: https://edri.org/EDRiDSAAnsweringGuide.html. Abgerufen am: 2022/07/06

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

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

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

Element (2022b). Hosted Matrix bridges | Element Matrix Services. Abgerufen von: https://element.io/matrix-services/hosted-bridges. Abgerufen am: 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, S. 343-363

ETSI (2022). ETSI ICT Standards. Abgerufen von: https://www.etsi.org/standards. Abgerufen am: 2022/04/01

Europäische Kommission (2022a). Non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA. Abgerufen von: https://www.lobbycontrol.de/wp-content/uploads/non_paper_interoperability_dma.pdf. Abgerufen am: 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. Abgerufen von: https://ec.europa.eu/commission/presscorner/home/en. Abgerufen am: 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. Abgerufen von: https://developers.facebook.com/docs/whatsapp/on-premises/reference/messages/. Abgerufen am: 2022/05/28

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

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

Farrell, Joseph & Klemperer, Paul (2007). Coordination and lock-in: Competition with switching costs and network effects. In: *Handbook of industrial organization* 3, S. 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* S. 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* S. 940-955

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

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

Farrell, Joseph & Simcoe, Timothy (2012a). Choosing the rules for consensus standardization. In: *The RAND Journal of Economics* 43, 2, S. 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, S. 131-154

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

Gekeler, Martin (2022). Schnellübersicht Messengersysteme. Abgerufen von: https://www.freie-messenger.de/systemvergleich/. Abgerufen am: 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, S. 101-161

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

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

Google (2022b). Overview | Geocoding API. Abgerufen von: https://developers.google.com/maps/documentation/geocoding/overview. Abgerufen am: 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, S. Article 104

Grüner, Sebastian (2019). Chat over IMAP - Gut gemeint ist leider nicht gut gemacht. Abgerufen von: https://www.golem.de/news/chat-over-imap-gut-gemeint-ist-leider-nicht-gut-gemacht-1905-141009.html. Abgerufen am: 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, S. 94-101

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

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

HM Government (2022). Government response to the consultation on a new pro-competition regime for digital markets. Abgerufen von: 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: S.

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

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

Internet Society (2022). DMA and interoperability of encrypted messaging. Abgerufen von: https://www.internetsociety.org/wp-content/uploads/2022/03/ISOC-EU-DMA-interoperability-encrypted-messaging-20220311.pdf. Abgerufen am: 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, S. 1199-1229

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

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

Johannsen, Jan (2015). WhatsApp Plus: Immer noch Finger weg vom Messenger-Klon - CURVED.de. Abgerufen von: https://curved.de/news/whatsapp-plus-faq-21036. Abgerufen am: 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, S. 100880

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

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

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

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

Kokolakis, Spyros (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In: *Computers & security* 64, S. 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, S. 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. Abgerufen von: https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/.

Kröner, Peter & Divya, Manian (2013). SpecGraph. Abgerufen von: https://github.com/SirPepe/SpecGraph. Abgerufen am: 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). Abgerufen von: 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. Abgerufen von: https://www.wik.org/en/veroeffentlichungen/studien/weitere-seiten/digital-sovereignty?msclkid=a0794a20b3ea11ec910c887fdf5c32cc.

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

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

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

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

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

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

Lerner, Josh & Tirole, Jean (2006). A model of forum shopping. In: *American economic review* 96, 4, S. 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. Abgerufen von: https://techcrunch.com/2022/03/24/dma-political-agreement/?guccounter=1. Abgerufen am: 2022/07/06

Lyles, Taylor (2020). A year later, Amazon's voice assistant alliance still hasn't attracted any of its rivals. Abgerufen von: https://www.theverge.com/2020/9/9/21429893/amazon-voice-interoperability-initiative-alexa-apple-google-samsung. Abgerufen am: 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, S. 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, S. 327-341

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

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

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

Marlinspike, Moxie & Perrin, Trevor (2016). The X3DH Key Agreement Protocol. Signal. Abgerufen von: 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, S. 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, S. 516-527

Matrix (2022). Bridges. Abgerufen von: https://matrix.org. Abgerufen am: 2022/05/24/

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

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

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

Monopolkommission (2021). Telekommunikation 2021: Wettbewerb im Umbruch, 12. Sektorgutachten. Abgerufen von: 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. Abgerufen von: https://alecmuffett.com/alecm/e2e-primer/e2e-primer-web.html. Abgerufen am: 2022/07/27

Nominet (2019). Cyber security and the cloud - Enterprise security leaders have their say. Abgerufen von: 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, S. 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, S. 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, S. 727-735

OECD (2018). Rethinking Antitrust Tools for Multi-Sided Platforms. OECD. Abgerufen von: 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. Abgerufen von: https://www.iphone-ticker.de/weitgehend-unbemerkt-vodafone-und-o2-stellen-ihre-messenger-ein-125269/. Abgerufen am: 2022/06/13
Open Banking (2022a). About the Open Banking Implementation Entitiy. Abgerufen von: https://www.openbanking.org.uk/about-us/. Abgerufen am: 2022/07/06
Open Banking (2022b). Fintechs. Abgerufen von: https://www.openbanking.org.uk/fintechs/. Abgerufen am: 2022/07/06
Oracle (2010). Fusion Middleware Interoperability and Compatibility Guide. Abgerufen von: https://docs.oracle.com/cd/E17904_01/doc.1111/e17836/overview.htm#INTOP109. Abgerufen am: 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. Abgerufen von: https://social.techcrunch.com/2020/04/10/apple-and-google-are-launching-a-joint-covid-19-tracing-tool/. Abgerufen am: 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* S. 21-42
Porell, Jim (2020). Rocket and Open Source: A Brief History on the Open Mainframe Movement. Abgerufen von: https://blog.rocketsoftware.com/2020/09/rocket-and-open-source-a-brief-history-on-the-open-mainframe-movement/#.YN9p9RNue3. Abgerufen am: 2022/07/06
Prüfer, Jens & Schottmüller, Christoph (2021). Competing with big data. In: *The Journal of Industrial Economics* 69, 4, S. 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), S. 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, S. 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. Abgerufen von: https://netzpolitik.org/2022/digital-markets-act-sichere-messenger-threema-und-signal-sind-gegen-interoperabilitaet/. Abgerufen am: 2022/07/08/
Riley, Chris (2020). Unpacking interoperability in competition. In: *Journal of Cyber Policy* 5, 1, S. 94-106
Rochet, Jean-Charles & Tirole, Jean (2003). Platform competition in two-sided markets. In: *Journal of the european economic association* 1, 4, S. 990-1029
Roettgers, Janko (2021). OK Google, meet Alexa: Interoperability emerges as key antitrust issue. Abgerufen von: https://www.protocol.com/google-alexa-sonos-antitrust. Abgerufen am: 2022/05/03/
Rohlfs, Jeffrey (1974). A theory of interdependent demand for a communications service. In: *The Bell journal of economics and management science* S. 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)*. S. 415-429

RTR (2020). Monitoring von digitalen Kommunikations Plattformen und Gatekeepern des offenen Internetzugangs. Abgerufen von: 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, S. 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, S. 01-17

Samuelson, William & Zeckhauser, Richard (1988). Status quo bias in decision making. In: *Journal of risk and uncertainty* 1, 1, S. 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, S. 452-487

Sanders, James (2019). Multicloud deployments are twice as likely to fall victim to security breaches. Abgerufen von: https://www.techrepublic.com/article/multicloud-deployments-are-twice-as-likely-to-fall-victim-to-security-breaches/. Abgerufen am: 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* S. 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, S. 742-757

Shapiro, Carl (2001). Setting compatibility standards: cooperation or collusion. In: *Expanding the Boundaries of Intellectual Property* 81, S. 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, S. 107

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

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

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

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

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)* S. 357-363

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

Statista (2022). Public Cloud - Europe | Statista Market Forecast. Abgerufen von: https://www.statista.com/outlook/tmo/public-cloud/europe. Abgerufen am: 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. Abgerufen von: https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises. Abgerufen am: 2022/07/06

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

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, S. 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, S. 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, S. 21-35

Taş, Serpil & Arnold, René (2019). Auswirkungen von OTT-1-Diensten auf das Kommunikationsverhalten – Eine nachfrageseitige Betrachtung. WIK. Abgerufen von: 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. Abgerufen von: https://www.wik.org/fileadmin/Studien/2021/Kommunikationsverhalten.pdf.

Telegram (2022). Telegram Ad Platform Explained. Abgerufen von: https://promote.telegram.org/getting-started. Abgerufen am: 2022/07/06

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

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

Tiwana, Amrit & Konsynski, Benn (2010). Complementarities between organizational IT architecture and governance structure. In: *Information Systems Research* 21, 2, S. 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, S. 675-687

Twitter (2022). Twitter API Documentation. Abgerufen von: https://developer.twitter.com/en/docs/twitter-api. Abgerufen am: 2022/07/06

Tyntec (2022). tyntec | APIs for Messaging, Chat Apps, Number Data, and Authentication | tyntec. Abgerufen von: https://www.tyntec.com/. Abgerufen am: 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*. S. 232-249

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

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. S. 973-990

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

VZBV (2021). INTEROPERABILITÄT BEI MESSENGERDIENSTEN. Abgerufen von.

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

WhatsApp (2021). WhatsApp Security Whitepaper. Abgerufen von: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf. Abgerufen am: 2022/05/18

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

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

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

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

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

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

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