OpenForum
Academy

PRIVATE MESSAGING INTEROPERABILITY IN THE EU DIGITAL MARKETS ACT

IAN BROWN

Ian Brown

Ian Brown is a consultant on Internet regulation, particularly relating to information security and privacy, digital elements of the election cycle, and pro-competition mechanisms such as interoperability. He is a visiting professor at the Centre for Technology and Society at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro, and an ACM Distinguished Scientist. His clients since 1999 include the Open Society Foundations, Global Network Initiative, Vodafone, UK and US governments, German Bundestag, European Commission and Parliament, Council of Europe, OECD, Commonwealth, and the United Nations. He has acted as an expert witness in UK and European criminal, intellectual property and surveillance/human rights cases, including *Cartier v BSkyB* (EWHC), *Privacy International v GCHQ* (IPT) and *Big Brother Watch v UK* (ECtHR).

Dr Brown was previously Principal Scientific Officer at the UK government's Department for Digital, Culture, Media and Sport; Professor of Information Security and Privacy at the University of Oxford's Internet Institute; and a Knowledge Exchange Fellow with the Commonwealth Secretariat and UK National Crime Agency. His books include Cybersecurity for Elections (2020, Commonwealth Secretariat, with Marsden/Lee/Veale), Regulating Code (2013, MIT Press, with Marsden), and Research Handbook on Governance of the Internet (ed., 2013, Edward Elgar).

A civil society enthusiast, Brown co-founded and served on the boards of European Digital Rights, Open Rights Group, the Foundation for Information Policy Research and Privacy International; and has written for The Financial Times and The Guardian. He is a fellow of OpenForum Europe and the International University of Japan, and a member of the *Technology and Regulation* editorial board.

OpenForum Academy

OpenForum Academy is an independent programme established by OpenForum Europe. It has created a link with academia in order to provide new input and insight into the key issues which impact the openness of the IT market.

Central to the operation of OpenForum Academy are the Fellows, each selected as individual contributors to the work of OFA. A number of academic organisations have agreed to work with OFA, working both with the Fellows and within a network of contributors in support of developing research initiatives.

Contents

Figures

Acronyms

API	Application Programming Interface
BKartA	Bundeskartellamt, Germany's Federal Cartel Office
CPS	Core Platform Service
DMA	Digital Markets Act
DSA	Digital Services Act
EC	European Commission
E2EE	End-to-End Encryption
EECC	European Electronic Communications Code
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
IMCO	Internal Market Committee of the European Parliament
NIICS	Number-Independent Interpersonal Communications Service
OSF	Open Society Foundations
RCS	Rich Communication Services
SME	Small/Medium-Sized Enterprise

1   Introduction

Digital markets (such as private messaging) are often "winner takes all", with one firm over time taking a very large market share, and competitors then finding it very difficult to enter or expand into the market. The resulting lack of competition means users are likely to face higher prices or lower innovation, choice and quality, such as greater intrusion to enable targeted advertising.[1]

One of the mechanisms proposed by a number of competition economists and regulators to increase competition in digital markets (discussed further in Section 3.1) is to require the largest firms to make their services *interoperable* with competitors'. This would make it easier for new services to become mainstream by overcoming the incumbency advantage a very large user base gives today's market leaders.

A 2021 German consumer organisation survey found the two most important reasons respondents chose a messenger service were that a service can reach the most contacts (78%) and that it can reach specific people/groups (41%). This is a high hurdle for new messenger services to overcome without an interoperability requirement for the very largest platforms such as WhatsApp (which, according to the same survey, was primarily used by 84% of respondents, well ahead of Facebook Messenger at 5%).[2] And an academic study found that following WhatsApp's privacy policy change in January 2021, "about 26% of participants wanted to switch (at least partially) to other apps, but only a quarter of them felt that they managed to do so. Only 8 participants out of the 1525 reported uninstalling WhatsApp… participants used a median of 5 messaging apps in total, and still couldn't leave WhatsApp."[3]

---

[1] See e.g., UK Competition & Markets Authority, *Online platforms and digital advertising*, Market study final report, 1 July 2020, section 2; and Ian Brown, *Interoperability as a tool for competition regulation*, OpenForum Academy, November 2020, pp.14—15.

[2] Verbraucherzentrale, *interoperabilität Bei Messengerdiensten*, 17 May 2021.

[3] Carla Griggio, *The Great Messaging-App Migration (That Didn't Really Happen)*, 14 March 2021.

1.1 The Digital Markets Act

The European Union's Digital Markets Act (DMA), applying from 2 May 2023, places a range of competition-related obligations on the largest global technology companies offering a "core platform service"[4] (CPS) in at least three EU member states (with a market capitalization over €75bn or EU annual revenues above €7.5bn for the last three years, and a CPS with at least 45m end-users and 10,000 business users in the EU).[5] Figure 1 shows the European Commission's timeline for the DMA's agreement and application.[6]

Timeline for Digital Markets Act

Commission proposal	Political agreement on the DMA	DMA rules enter into force	DMA rules start to apply	Data notification for thresholds check	Designation of gatekeepers	Application of the obligations
15/12/2020	25/03/2022	01/11/2022	02/05/2023	03/07/2023 (at the latest)	06/09/2023 (at the latest)	March 2024

······▶ +6 months ··········▶ +2 months ·····▶ +45 working days ·····▶ +6 months
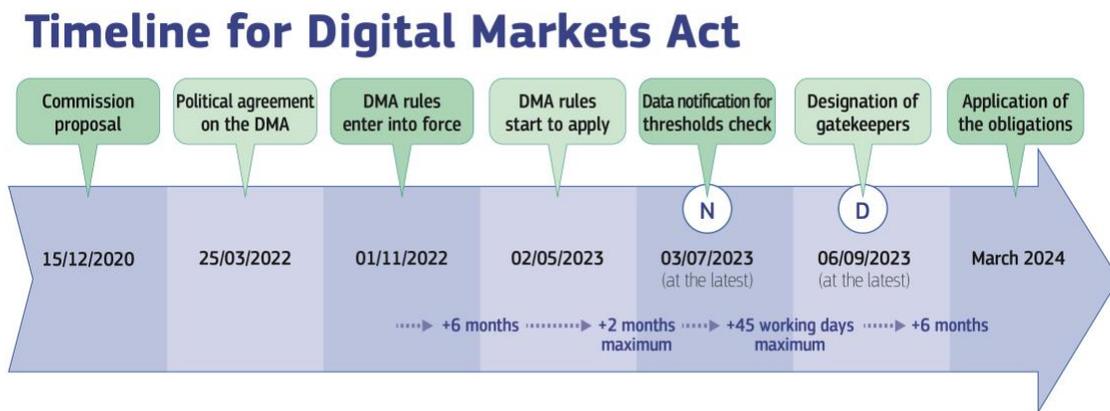   maximum   maximum

Figure 1 Timeline for the Digital Markets Act. Source: European Commission (2022)

One of the DMA's obligations (set out in Article 7) applies to providers of messaging and real-time communication services (in EU legal jargon, *Number-Independent Interpersonal Communications Services* or *NIICS* – defined in the European Electronic Communications Code[7]). These firms will be required to make specific functionality of their services interoperable with other services at the latter's request, free of charge, "where the gatekeeper itself provides those

---

[4] Defined in Article 2(2).

[5] These tests are presumptions set out in Article 3 of the DMA, and the commencement date in Article 54. There is also a more complex test which can be applied to smaller companies in Article 3(8). The *Official Journal of the EU* contains the final text: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *OJ L 265*, 12.10.2022, pp. 1–66.

[6] European Commission, *Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force*, IP/22/6423, 31 October 2022.

[7] Article 2(7) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), *OJ L 321*, 17.12.2018, pp. 36—189.

functionalities to its own end users"[8] – so, for example, a Telegram user could potentially exchange encrypted messages directly with a WhatsApp user, if Telegram decided to request that functionality from Meta.

Once the DMA applies, the European Commission will ("without undue delay"[9]) designate "gatekeeper" firms, and core platform services which "individually are an important gateway for business users to reach end users"[10] subject to this obligation. Services affected are likely to include Meta's WhatsApp/Facebook Messenger and Instagram Direct Messages, Apple's iMessage, and potentially Microsoft's Skype and Teams, and Google's Meet and Chat.[11] Telegram Inc. was reportedly valued at US$30-$40bn in 2021, but anyway already implements interoperability.[12]

The DMA will not impose obligations on smaller services. It seems extremely unlikely the Signal Foundation will ever meet the DMA's size tests (which would need at least 125m EU users donating its lowest suggested amount of 5€/month for three years). It will be entirely up to smaller providers whether they wish to interconnect their services to those of the gatekeepers; and where they do, to their users as to whether they make use of them.[13]

This report describes the implications of this obligation for private messaging services using end-to-end encryption, which is specifically addressed by the DMA. It also covers the provision's legislative history; the response of large and small messaging providers; infrastructural developments which could make the provision more effective; and remaining challenges, and civil society's potential role in addressing them. It includes key points from twelve interviews

---

[8] Article 7(2).

[9] Article 3(4).

[10] Article 3(9), defined in Recital 20 and other recitals.

[11] SnapChat might qualify as a NIICS but following the tech stock crash of 2022, Snap has only around 1/5th of the market capitalisation to be presumed large enough to be a gatekeeper. Twitter DMs are arguably excluded as "a minor ancillary feature that is intrinsically linked to another service" (Art. 2(5) EECC).

[12] A German Federal Network Agency survey found "WhatsApp (93%), Facebook Messenger (39%) and Instagram Direct Messages (25%) are the most widespread among German users. All three services are affiliated with the Meta Group (formerly Facebook). Competing services such as Skype (20%), Zoom (18%), Telegram (16%), Microsoft Teams (14%), Snapchat (14%) or Signal (13%) are significantly less common." Bundesnetzagentur (2021) *Interoperability between messenger services: Overview of potentials and challenges*, p.4.

[13] Article 7(7).

undertaken with stakeholders including small and large technology firms, civil society groups, regulators, and experts on technology, standards and competition policy.

2   What exactly does the DMA specify for end-to-end encryption, and what technical solutions are there today for interoperable encryption?

A comparison of the technical options for regulated E2EE providers to meet the DMA messaging interoperability requirement while preserving security protections, including encryption and spam protection

2.1   The DMA messaging interoperability article (7)

Once the DMA applies from 2 May 2023,[14] firms meeting the quantitative thresholds specified in Article 3 must provide the Commission with information on their turnover/capitalization and user numbers within two months.[15] The Commission must then within 45 working days make the designation of covered firms and core platform services.[16] Designated gatekeepers have six months to comply with the DMA obligations[17] (so at the latest, March 2024).

A firm may notify the Commission if it believes one of its services which meet these tests "exceptionally" should not be designated. Article 3(5) sets out this process, and the potential responses of the Commission.

Within six months of designation, a gatekeeper NIICS must publish "a reference offer laying down the technical details and general terms and conditions" enabling competitors to interoperate with its communications services.[18] It must then comply within three months with "any reasonable request" to interoperate from "any provider… offering or intending to offer such services in the Union".[19] The Commission may "consult the Body of European Regulators for Electronic Communications [BEREC], in order to determine whether the technical details and

---

[14] Article 54.
[15] Article 3(3) and Annex.
[16] Article 3(4).
[17] Article 3(10).
[18] Article 7(4).The effective time limit for publication will be March 2024.
[19] Article 7(5).

the general terms and conditions published in the reference offer that the gatekeeper intends to implement or has implemented ensures compliance with this obligation."[20] BEREC intends to publish its own guidance on compliance.

The NIICS interoperability obligation applies only to specific "basic functionalities" of designated gatekeeper services, initially only one-to-one text messaging, including images/voice messages/video/other types of files. Within two years of designation, support for text messaging (with attachments) within a group is required, as well as sharing images/voice messages/ video/other types of files between a group and an individual. Four years after designation, this will extend to voice/video calls between two individuals, and a group and an individual.[21] This process is summarised in Figure 2 below.

These deadlines may "exceptionally" be further extended by the European Commission if "the gatekeeper demonstrates that this is necessary to ensure effective interoperability and to maintain the necessary level of security, including end-to-end encryption, where applicable."[22] The Commission may also suspend obligations which "would endanger, due to exceptional circumstances beyond the gatekeeper's control, the economic viability of its operation in the Union",[23] or exempt a gatekeeper "on grounds of public health or public security."[24]

The interoperability obligation requires that "The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services."[25] A service such as WhatsApp which only provides end-to-end encryption (E2EE) to its own users will not be required to introduce any features which are *not* end-to-end encrypted.

E2EE means messages and audiovisual communications are encrypted on the sending/"calling" user's own device, and decrypted on the recipient's device(s).

---

[20] Recital 64 and Article 48.
[21] Article 7(1) and 7(2).
[22] Article 7(6).
[23] Article 9.
[24] Article 10.
[25] Article 7(3).

Designation
- EC already "engaging proactively with industry stakeholders to ensure effective compliance"
- Gatekeeper must notify EC if it meets quantitative tests (EU turnover > €7.5bn/market cap > €75bn, CPS in 3+ member states with EU end-users > 45m and biz-users > 10k) by 3 July 2023
- EC designates gatekeepers and core platform services by 6 Sept 2023. GKs must report on compliance within 6 months, and annually

Reference offer
- Gatekeeper must publish tech details and T+Cs by 6 Mar 24
- EC holding workshops with stakeholders from Dec 2022 "to gauge third party views on compliance"
- EC may consult national regulators (BEREC) on offer compliance
- When taken up, gatekeeper must enable within 3 months

Required functionalities
- Initially: 1-1 messaging
- 2 years: group messaging support
- 4 years: voice/video calls between individuals, and group-individual

Enforcement
- Periodic penalty payments, and fines up to 10% of global turnover
- Fines up to 20% and behavioural/structural remedies for systematic non-compliance
- EC consulting on procedural issues in an implementing act in Nov/Dec 2022
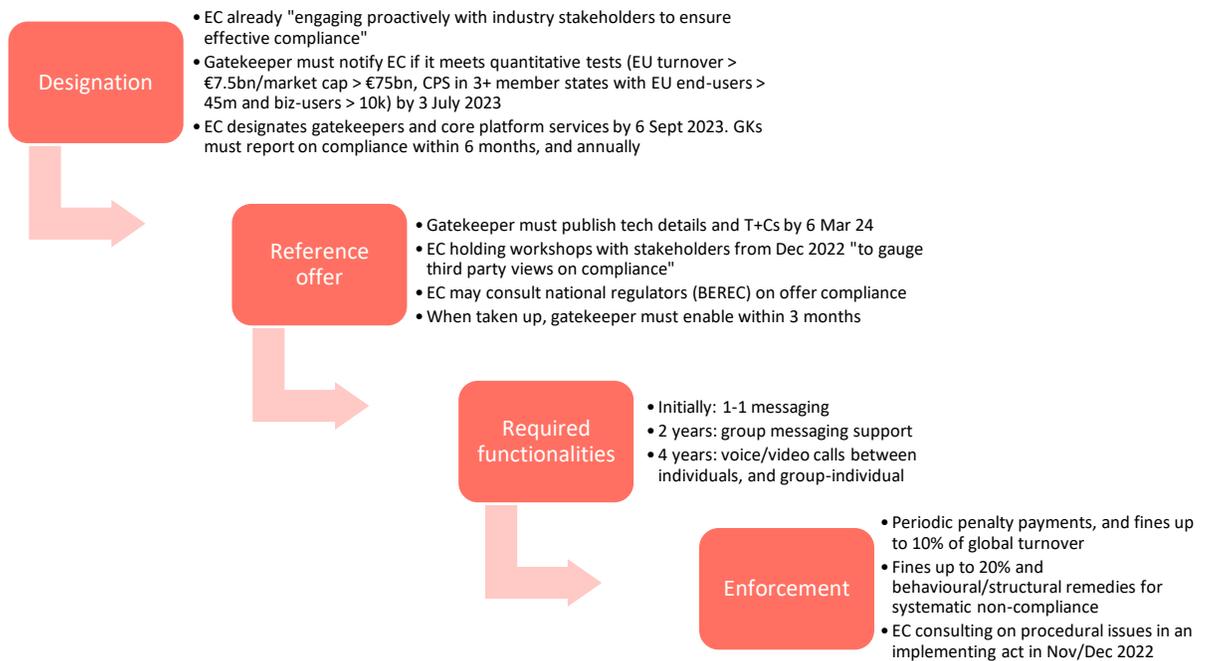
Figure 2 Application of the DMA NIICS interoperability obligation

Even the service provider, for example WhatsApp, cannot read the message contents. The service provider *will* see some unencrypted metadata associated with encrypted messages, such as the IP address of the sender, the time/date it is sent, and other user activity with the service — which are all useful in fighting spam, phishing, and other types of service abuse. (Signal and other privacy-focused messaging services limit their collection of this data.[26])

This type of metadata may be required by gatekeepers from interoperating services to continue operating these critical security features. This of course raises privacy issues: Article 7(8) of the DMA also specifies "The gatekeeper shall collect and exchange with the provider of number-independent interpersonal communications services that makes a request for interoperability only the personal data of end users that is strictly necessary to provide effective interoperability. Any such collection and exchange of the personal data of end users shall fully comply with

---

[26] Nilay Patel, Why Signal won't compromise on encryption, with president Meredith Whittaker, *The Verge*, 18 October 2022.

Regulation (EU) 2016/679 [GDPR] and Directive 2002/58/EC [ePrivacy Directive]." But paragraph 9 of the article further specifies:

> *The gatekeeper shall not be prevented from taking measures to ensure that third-party providers of number-independent interpersonal communications services requesting interoperability do not endanger the integrity, security and privacy of its services, provided that such measures are strictly necessary and proportionate and are duly justified by the gatekeeper.*

The GDPR and e-Privacy Directive (ePD) would strictly limit the use of metadata by services processing messages to or from users of interoperable third-party systems. The ePD has been in the process of being updated for several years, and potentially could be extended to further cover interoperable messaging if required.

The DMA does not explicitly refer to disappearing messages, and gatekeeper services with this feature would most likely be free to refuse to allow a disappearing message to be sent to a user on an interoperating service (or, if they wished, only to other services which also support the feature, and demonstrate some assurance it will be enforced.) As Cory Doctorow has noted, disappearing messages can only ever be effective as an agreement between sender and recipient to automate deletion.

Finally, designated gatekeeper services must meet the interoperability obligation "by providing the necessary technical interfaces or similar solutions that facilitate interoperability, upon request, and free of charge".[27] The most straightforward option will likely be public, limited versions of Application Programming Interfaces (APIs) and related functionality gatekeepers already use within their own systems.

The gatekeeper must not "engage in any behaviour that undermines effective compliance with the obligations… regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design."[28] Nor may it "degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices

---

[27] Article 7(1).
[28] Article 13(4).

laid down … or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof."[29]

A designated firm may challenge the decision before the General Court and ask for specific obligations to be suspended until the appeal is concluded. This process would be likely to take up to two years (one in the case of an accelerated procedure.)

2.1.1   Enforcement

If the European Commission is not satisfied a gatekeeper is complying with a DMA obligation, it may open an investigation, then within six months adopt an implementing act "specifying the measures that the gatekeeper concerned is to implement in order to effectively comply".[30] For non-compliance, it may impose fines of up to 10% of an undertaking's worldwide annual revenue, and in the case of repeated infringements up to 20%,[31] as well as periodic penalty payments.[32] Any of these may be reviewed by the EU Court of Justice.[33]

In the case of systematic non-compliance, the Commission may "adopt an implementing act imposing on such gatekeeper any behavioural or structural remedies which are proportionate and necessary to ensure effective compliance with this Regulation."[34] While politically unlikely, this could go as far as breaking up a gatekeeper firm.

2.2   Applicable technical standards

Alongside making public APIs available, another option for designated gatekeepers would be to support open technical standards for messaging, which would save competitors from having to support a set of APIs and related messaging protocols per gatekeeper they wish to interoperate

---

[29] Article 13(6).
[30] Article 8(3).
[31] Article 30.
[32] Article 31.
[33] Article 45.
[34] Article 18(1).

with. Options include Matrix, the Extensible Messaging and Presence Protocol (XMPP), or the IETF's Messaging Layer Security (MLS) once completed.[35]

However, it is unlikely to be in the commercial interests of gatekeepers to reduce costs or friction for competitors to enable connections to their users. Civil society and open-source groups, and the Greens/Pirate group of MEPs, pushed for the final DMA to require the use of such technical standards, without success.

The DMA specifies this could be changed in future by an implementing act on "operational and technical arrangements".[36] This process requires the Commission to consult the EU member states before adopting an act, as well as seeking feedback from the public on a draft text four weeks before this.

Another provision allows the "basic functionalities" list to be changed in future by a delegated act following a market investigation.[37] Such acts require the Commission to consult experts (often academics) from each member state before adopting an act, as well as seeking feedback from the public on a draft text four weeks before this. The most relevant expert group for this purpose is the Commission's Group of Experts for the Observatory on the Online Platform Economy. It has also created a High-Level Forum on European Standardisation.

The Commission may request the European standards bodies to develop technical standards:

> Recital (96) *The implementation of some of the gatekeepers' obligations, such as those related to data access, data portability or interoperability could be facilitated by the use of technical standards. In this respect, it should be possible for the Commission, where appropriate and necessary, to request European standardisation bodies to develop them.*

> Article 48. *Standardisation. Where appropriate and necessary, the Commission may mandate European standardisation bodies to facilitate the implementation of the obligations set out in this Regulation by developing appropriate standards.*

---

[35] Ian Brown, *The technical components of interoperability as a tool for competition regulation*, OpenForum Academy, November 2020, pp.5—10.
[36] Article 46(1)(c).
[37] Article 12(3).

Such decisions are unlikely to be early priorities of the Commission, which was at times sceptical of a NIICS interoperability obligation in the DMA.

Further discussion of technical standards development is in Section 5.1 below.

3   What is the legislative history behind the inclusion of this mandate in the DMA?

Key elements in the two-year advocacy campaign by European civil society groups for an interoperability mandate in the DMA, and the evolving positions of the EU's co-legislators (Commission, Council and Parliament).

3.1   Background

An interoperability obligation for the largest technology firms has in various forms been supported by a number of major reviews of digital competition, including for the UK Treasury (Unlocking digital competition) and the European Commission's competition commissioner (Competition policy for the digital era). It has also been advocated by a major report by the US House of Representatives antitrust subcommittee, and articles by noted competition economists such as Prof. Fiona Scott Morton, as well as digital rights groups such as EDRi, EFF and the Open Rights Group.

Prof. Scott Morton and colleagues called interoperability the "super tool" for digital platform governance. It has also long been included in the European telecommunications regulatory framework,[38] and is also beginning to have a significant impact in financial regulation (through the second EU Payment Services Directive and especially the UK's Open Banking.[39])

These reviews, alongside concerns on digital competition from the European Parliament and major EU member states such as Germany and France, were the main drivers for the European Commission to initially propose the Digital Markets Act in 2020. This proposal included a direct interoperability requirement for "ancillary" services (such as smartphone payments), but not the "core services" identified by the DMA, including messaging.

---

[38] Most recently updated in the European Electronic Communications Code.
[39] Ian Brown, The UK's Midata and Open Banking programmes: a case study of data portability and interoperability requirements, *Technology and Regulation* (2022).

A draft US law with similar interoperability requirements to the DMA (the ACCESS Act) is under debate in the US Congress, while another bill with greater political support (the American Innovation and Choice Online Act) contains broader provisions against platform self-preferencing which could have similar effects. The Chinese government has taken significant action on platform interoperability, while the UK government has committed to introducing legislation enabling its Competition & Markets Authority to impose it on firms with "systemic market status".

3.2   Civil society advocacy

Following academic research into the potential impact of platform interoperability on competition and user control since the 2000s,[40] civil society groups in Brussels such as EDRi and EFF have campaigned for interoperability mandates since early 2020. EDRi's position paper on platform regulation[41] for the European Commission's planned Digital Services Act (later split into a separate DSA and Digital Markets Act) stated:

> *Interoperability would drastically reduce the imbalance of power between platforms on the one side and individuals on the other. It would (re)em-power Internet users to interact across digital silos and allow them to choose their own online community and appropriate guidelines. An interoperability requirement would ensure that citizens do not sign up to dominant platforms just because there is no other way to communicate with their friends and participate in the social life of their local community, e.g. students at a university. It would also directly strengthen healthy competition among platforms and could even create whole new markets of online services built on top of existing platforms, such as third-party client apps or content moderation plug-ins.*

From 1 April 2020, there was a weekly conference call between civil society groups (including EDRi, BEUC, EFF and later ARTICLE 19), academics, and open-source projects and small European technology firms (such as Proton and Open-Xchange) interested in this topic. EDRi hosted a mailing list and document store. Open Society Foundations (OSF) supported research into the

---

[40] See for example the author's work with Prof. Chris Marsden, including Social Utilities, Dominance and Interoperability: A Modest Proposal (2008) and *Regulating Code* (2013), and *Interoperability: The Promise and Perils of Highly Interconnected Systems* by Urs Gasser and John Palfrey (2012).
[41] EDRi, Platform Regulation Done Right, 9 April 2020, p.22.

policy and technical details of an interoperability mandate, published in November 2020,[42] and coordinated a "Friends of the DMA" civil society group which also included groups such as Amnesty International, LobbyControl, Corporate Observatory Europe and the Centre for Research on Multinational Corporations.

This sustained civil society/academic/tech coalition, complemented later by a SME-focused Coalition for Competitive Digital Markets, worked intensively throughout the development of the DMA. It first lobbied the European Commission as the DMA was drafted, with calls and consultation responses. The Commission's public DMA proposal in December 2020 included an interoperability requirements provision for "ancillary" services (such as Apple and Google Pay), and provisions on app stores and search engines as well as "data interoperability". However, it did not include interoperability requirements for "core platform services" such as messaging and social networks.

The coalition in 2021 lobbied the Council of Ministers (the 27 national governments of the EU) and especially the different political groups in the European Parliament as they amended the proposal. The centre-left and Green/Pirate groups were particularly interested in talking to civil society groups about adding an "end-user" focus to the business-focused Commission proposal, while elements of the liberal and centre-right groups were interested in hearing from business about competitive platform markets more open to European firms.

Members of the coalition took part in stakeholder meetings organised by MEPs and particularly rapporteurs and shadow rapporteurs for the various parliamentary committees with oversight of the proposal, principally the Internal Market committee IMCO, and the economics and legal affairs committees. IMCO and then the full Parliament included NIICS and social networking services interoperability requirements in its final version of the DMA (in its annual review for 2021, campaign group LobbyControl commented: "Digital Markets Act: Facebook & Co did not expect that"). However, the Council version contained few significant amendments to the Commission proposal.[43]

---

[42] See *Interoperability as a tool for competition regulation* and *The technical details of interoperability as a tool for competition regulation* (2020) OpenForum Academy.

[43] A comparison of the two versions can be read at https://www.ianbrown.tech/2021/12/20/digital-markets-act-latest-imco-vs-council/

In the final phase (the "trilogues"), the Council, Parliament, and Commission negotiated an agreed version of the DMA. The coalition worked closely with some of the Parliament's shadow rapporteurs and their staff on both the political and "technical" trilogue meetings. OSF facilitated a civil society meeting with the responsible French minister for the Council (since France then held the rotating presidency).

Throughout this process, members of the coalition briefed journalists, sent open letters to the EU institutions, and maintained public information resources such as Interoperability News.

The final DMA retained specific NIICS interoperability obligations, which can be updated by the Commission following a market investigation. But the Council would not accept social media interoperability obligations, except potentially via a review process in the DMA and a broader requirement for "fair, reasonable, and non-discriminatory" business access to designated "software application stores, online search engines and online social networking services".[44]

Some Council members had difficulty imagining what interoperable social networking services look like (which is strange, given the existence of just such a service, Mastodon, which has added millions of users following Elon Musk's takeover of Twitter.) Others apparently preferred a regulated monopoly to deal with safety issues (discussed further in Section 6.2).

A policy expert inside the legislative process told us the most important contributions of civil society were as follows:

> *1. Solid evidence base for drafting amendments and that we could use during the negotiations (website, studies, expert reports from France, UK). Position papers are great, but fundamentally new proposals are often dismissed if their impact hasn't been tested by the Commission, e.g. in the Impact Assessment.*
> *2. Pool of experts we could consult, and refer to the Commission, and to the German government (at some point we`ve created that contact list).*
> *3. Public awareness raising event very early in the process, that helped to make interoperability a topic for public/political discussion, in the EP but also outside.*
> *4. Transparency, and keeping up the press attention was equally useful. Otherwise, the Rapporteur would have 'forgotten' about the promises he had made.*

---

[44] Article 6(12).

5. Internal group discussions, and an official position on this, which made its way to the German coalition agreement. We were very lucky that the German elections and the DMA process happened at the same time.

An SME executive told us civil society had been crucial in achieving the messaging interoperability mandate in the DMA, and could play a similar role in other jurisdictions: "Activism was critical. Civil society should continue being very active and vocal, explaining why these issues are so important for business, innovation, users, and how hacking dominance is important for data protection and security." S/he suggested: "These kinds of activities are very helpful and can be very powerful. Especially in jurisdictions where the mindset/regulatory approach will change. Civil society can help with continued pressure, reaching out to politicians, explaining even the basics, translating these concepts into real life."

3.2.1   Digital Services Act

Free-speech group ARTICLE 19 also lobbied the Parliament and Commission to include a specific interoperability requirement for social media recommendation and newsfeed algorithms in the Digital Services Act. This would have allowed users to choose recommendation engines from third parties, thereby reducing the incentives of current platforms to focus so relentlessly on user engagement to the exclusion of quality. However, while some MEPs were enthusiastic, this requirement was not included in the final DSA.

One civil society expert told us:

ARTICLE 19's main challenge was to make a powerful case that both consumers and businesses were interested in this idea. I think many legislators saw it as a potentially interesting idea but one that wasn't fully developed, nor very convincing as they insufficiently demonstrated interests from a wider group of stakeholders (such as businesses) in their proposal. I think that's one of the key reasons why they weren't successful and the DMA coalition was.

A second civil society expert noted a chicken-and-egg problem in finding business support: "there are not many SMEs working on recommender systems out there because there's no real market for them currently on social media." Ironically, court filings have since showed this policy is also broadly supported by one of Europe's most influential businessmen, Mathias Döpfner (chief executive of German publisher Axel Springer).

3.3   Scepticism from some competition economists

Not all competition economists and authorities have been as enthusiastic about a platform interoperability obligation as the reviews cited in Section 3.1. Least approving was the Bundeskartellamt's (BKartA) interim sector inquiry report into messaging and video communications services, which found many companies surveyed were against an interoperability requirement, and questioned "to what extent [an] impact on innovation incentives and the intensity of competition in the industry can be expected."[45] Relatedly, a report for think-tank CERRE concluded:

> *In practice, horizontal interoperability will never be perfect and can only achieve limited interoperability between a set of common features. Thus, network effects for the dominant platform remain, while at the same time interoperability reduces the incentives of consumers to multi-home. This means that horizontal interoperability can be anti-competitive in digital markets and has the potential to enshrine the dominance of digital incumbents.*

In plain English, "horizontal interoperability" refers to interoperability between two directly competing products, such as WhatsApp and Telegram. "Network effects" are the benefits a new user provides to all existing members of a network, since they all now have an additional person they can communicate with.[46] And "multi-homing" is people making use of competing services simultaneously, which is easier – but not cost-free – with "free" messaging apps.[47]

The CERRE report is more positive about "vertical interoperability" (between complementary services) mandates for vertically integrated companies such as Meta. This type of requirement was also the initial recommendation of the UK Competition & Markets Authority market study on online platforms (while suggesting an interoperability requirement might need to go further).

---

[45] *Zwischenbericht zur Sektoruntersuchung Messenger- und Video-Dienste*, 4 November 2021. The quotes in this report are taken from an auto-translation by Microsoft Word.

[46] As Germany's Federal Network Agency explained, "Network effects have a self-reinforcing effect and grant a competitive advantage to the service that is the first to have a critical mass of users. If a user wants to switch to another provider, he must also encourage his communication partners or entire groups of communication partners to switch." *Interoperability between messenger services*, p.6, note 12.

[47] Ian Brown, *Interoperability as a tool for competition regulation*, OpenForum Academy, November 2020, pp.16—26.

It is included in the final DMA for designated search engines, social networking services, operating systems and app stores. However, as Ariel Ezrachi and Maurice Stucke have described, "gatekeeper" firms can shape the innovations supplied within their platforms by third parties to support their own value chains, while complementary services can also further entrench the platform.[48]

A competition law expert told us "vertical interoperability might be useful for intra-platform competition but cannot deliver inter-platform competition, therefore it's not enough for the ambitious contestability the DMA is supposed to achieve." The EU national telecoms regulators similarly concluded: "without the inclusion of such [horizontal interoperability] measures in the regulatory toolbox for relevant [Core Platform Services], the DMA would be unlikely to create effective conditions for competitors to arise (inter-platform competition)."[49]

A French Conseil national du numerique (CNNum) study on interoperability suggested "a gradual approach should be favoured, starting with the introduction of a light option (option 2: possibility to send and receive instant messages or option 3.1 possibility to consult content)." This is close to the approach adopted by the DMA for messaging.

Similarly, Germany's Monopolkomission concluded in a nuanced report that "An asymmetric interoperability obligation for number-independent interpersonal communication services, if necessary, should be limited to basic functions to be defined so that competition via innovative additional functions remains possible" (§236), while assessing there was not currently a market failure in such services that justified it. Germany's Federal Network Agency took a similar position.[50]

---

[48] Ariel Ezrachi and Maurice E. Stucke, *How Big-Tech Barons Smash Innovation*, HarperCollins, ch. 3 (2022).
[49] Body of European Regulators for Electronic Communications, *BEREC Report on the ex ante regulation of digital gatekeepers*, BoR (21) 131, 30 September 2021, p.26.
[50] *Interoperability between messenger services*, pp.18—19, note 12.

4   How are companies likely to respond, and what are the opportunities for smaller/open-source groups to benefit from this provision?

What has been the position of large "gatekeeper" messaging platforms likely to be designated under the DMA, and smaller/open-source messaging providers? How are these positions likely to evolve?

4.1   Large corporate positions

From an economic perspective, the strong incentives for DMA gatekeepers whose messaging services are designated will be to do the minimum technical work to comply with the interoperability obligation (probably by opening up public APIs based closely on their existing internal technical standards), while having little incentive to reduce costs for competitors that take advantage of their interoperability obligation (e.g., by adopting or developing open technical standards).

One competition policy expert we talked to asked: "Asset owners will say what do I get for this? This is my intellectual property. This is my property. So I have to do the work to open it up and at low cost for competitors? Never going to happen. Which is why in telecoms things have been mandated in detail and access prices calculated for them. This is a HUGE issue. The underlying problem is fundamental. Companies will absolutely drag their feet. And why shouldn't they?"[51] A second competition policy expert was (slightly) more optimistic, asking:

> *Incumbents want to keep network externalities for themselves, they are not interested whatsoever in creating their own competitors. If they were, for whatever reason, they would have done it without regulators telling them, right?*

---

[51] Cory Doctorow wrote: '"*IP is any law that I can invoke that allows me to control the conduct of my competitors, critics, and customers.*" That is, in a world of uncertainty, where other people's unpredictability can erode your profits, mire you in scandal, or even tank your business, "IP" is a means of forcing other people to arrange their affairs to suit your needs, even if that undermines their own needs.' *Locus*, 7 September 2020.

Will they do the minimum thing? Following the above, yes, they'll do the absolute
minimum. The counterargument to this is that they may now "fear" the regulators and
their penalties. This of course assumes that regulators know what they are doing, and
are on top of it – something I have doubts about. I do not know how they are preparing
themselves, let's be hopeful.

A final perspective is that Meta's three messaging platforms are so dominant in the EU that even
the other gatekeeper firms offering or considering messaging tools might have an incentive to
support and even go beyond the DMA's interoperability obligation. This would enable them to
benefit from Meta's much larger user base. It is also possible a greater focus by WhatsApp on its
paid-for business services would give the company more incentive to let other platforms
interoperate.

Google has run a campaign in 2022 to push Apple to also support the Rich Communication
Services (RCS) standard for messaging built to replace mobile telephony's Short Messaging
Service (although the end-to-end encryption used is Google's own extension to the standard.)
Microsoft has a much more diverse range of products than Meta, so is less dependent on
defending its market power in any one service. Both companies have their own ecosystem of
related products, which would be strengthened by a widely used interoperable messaging
service. Similarly, Amazon might find it useful to add interoperable messaging to its hardware
products and cloud services, based on the Wickr service it acquired in 2021.

However, these large companies are yet to make public statements on their interoperability
plans. A technical expert told us: "Apple is always super tight-lipped until they aren't." S/he
added: "Meta may actually like the DMA requirement, to get their promised internal
interoperability (between WhatsApp, Facebook Messenger and Instagram Direct Messages)
working."

The BKartA interim sector report discussed in Section 3.3 found some individual video services
already provide public APIs, so "Microsoft Teams users could, for example, start a video call to
Zoom from their user interface." The report also discusses "middleware" companies such as
m.io which "connect to leading video services such as Microsoft Teams, WebEx, Zoom or even
Slack".

Cisco integrates with m.io and recently announced a partnership with Microsoft that allows for
greater interoperability between Microsoft Teams and Cisco Webex. One technical expert we

consulted about enterprise messaging noted that "given Wickr/Wire/Slack/Salesforce, there's a lot to be gained. Users are unhappy about the extensive multihoming currently needed."

The BKartA found mixed views among messenger and video services surveyed on interoperability. Only a fifth of respondents were in favour of a legal obligation for the largest providers. Those unwilling to participate voluntarily in interoperability efforts cited development costs, and "concerns about the enormous 'bureaucracy' and technical effort that any interoperability project will trigger, without really explaining it in more detail."

The BKartA inquiry covers a very broad range of consumer and business-facing services (messaging but also videoconferencing, online meetings, webinars, etc.), with associated revenues ranging from free/open source to tens of millions of euros, and user bases from 50,000-25m+. Unsurprisingly, it has found a wide range of business models and opinions. This reduces the value of some of the report's economic analysis regarding innovation, since messaging is much more homogeneous and well-developed than videoconferencing (that said, the latter is 35+ years old, while the former is as old as the Internet). A more differentiated approach might have been more productive.

Many of the negative comments from individual providers quoted in the interim report stem from ideas that are not serious policy proposals, such as an interoperability requirement covering all providers (rather than just the largest "gatekeepers" in EU terms), and mandates for complete functional standardisation rather than a requirement covering only core industry-standard functionality, as suggested by the UK's Competition and Markets Authority and adopted in the European Parliament's version of the Digital Markets Act, using extensible protocols to enable innovation. The final DMA obligation is even more limited.

4.2   SME/open-source positions

A number of European SMEs (such as Open-Xchange and Element) are enthusiastic supporters, setting up a Coalition for Competitive Digital Markets to support a broad DMA interoperability obligation. Europe's Digital SME Alliance trade group has been strongly in favour. However, the BKartA found some German "[s]maller providers focus on niche offerings, such as e-learning, or business customer groups that do not want interoperability and attach great importance to confidentiality and the highest security of their data" (the latter is discussed further in Section 6.1).

The BKartA also found: "Many vendors with an open-source philosophy pursue interoperability as a business strategy or mission statement. For example, providers such as BigBlueButton or Jitsi Meet, which call themselves open source, use open standards (e.g. WebRTC) that create interoperability and are basically intended to enable it vis-à-vis all messenger and video services." German open-source firm Wire has been another proponent. The BKartA also noted: "The open-source project Matterbridge also offers bridges between a number of chat protocols. Protocols are e.g., XMPP, Slack, Discord, Telegram, Rocket.Chat or Matrix."

However, the Swiss open-source firm Threema has been a notable opponent of an interoperability obligation, particularly given the company's focus on randomly-assigned user-IDs which avoids the need for users to share phone numbers as with many other messengers (discussed further in Section 5.2).

The founder of Signal, Moxie Marlinspike, has also been a vocal opponent due to fears of "ossification" of messenger features and protocols once they are standardised (since adding new features to technical standards inevitably takes significantly longer than implementation by a single firm). The developer of the decentralised Snikket messaging app has written a thoughtful response to Marlinspike's concerns.

New Signal President Meredith Whittaker has also stated (in relation to interoperability with the RCS messaging standard) she doesn't yet "have a clear answer. I think that the answer is [To Be Determined]. Our goal is for Signal to offer unequivocal, casual, just completely reliable security and privacy. So we would want to make sure RCS wasn't an issue." She acknowledged some Signal users want a single messaging interface, rather than to multi-home using multiple apps.[52]

One SME executive we interviewed was not yet clear how many users will want to take advantage of interoperability, or how the obligation will develop, so has not made support their "highest implementation priority." S/he felt the "big thing missing" from the DMA is a requirement for gatekeeper firms to support open standards, and was a "bit concerned about putting all these detailed features in the regulation" – as well as the possibility "gatekeepers publish APIs that really cannot be used." S/he plans to encourage the European Commission to

---

[52] *Why Signal won't compromise on encryption, with president Meredith Whittaker*, note 26.

push gatekeeper firms to provide such support. But a second SME manager was enthusiastic, and is planning to make an implementation request to Meta as soon as possible once the firm has published its reference offer.

Our first SME interviewee also suggested open-source developers could create "middleware" software to bridge between different messaging systems (running on users' own smartphones and PCs to preserve end-to-end encryption), as Matrix and Matterbridge are doing. It would also be possible for the European Commission to financially support the production and maintenance of free/open-source libraries which enable software to easily make use of the gatekeeper APIs.

5   What needs to happen at the infrastructural level of private messaging for interoperable encryption to become a reality?

Beyond messaging companies' own systems, are there infrastructural technologies which would make interoperability easier/cheaper/more secure for private messaging services? If so, what incentives are needed to produce them?

5.1   Developing technical standards

One standards expert told us the gatekeepers each exposing their own API for the purposes of interoperable messaging (the minimum required by the DMA) is "completely suboptimal, so beyond the non-gatekeepers there's a lot of motivation to make a standard. There was a side-meeting at the last Internet Engineering Task Force (IETF), everyone has tried this before. The difference now is the DMA."

There is broad consensus that interoperability requirements should only apply to the core functions of the largest digital platforms, leaving room for innovation and product differentiation. And some communication protocols such as Extensible Messaging and Presence Protocol (XMPP) are designed to be easily extended over time as new features are added.

Gatekeeper implementation of a common standard would significantly reduce the resources needed for competitors to implement interoperability, which would thereby only have to implement a single interface, rather than one per gatekeeper. SME messaging firm Element's Amandine Le Pape noted that otherwise, gatekeepers can "drag their feet on opening an API. Release it without fanfare or enthusiasm, and make sure it's not particularly good; a bit of a pig. Clunky. Unreliable. 'This stuff is tricky, you know?' And just when people are finally getting to grips with it… they can update it! To make it worse. Or just different. Different enough to put a bunch of smaller companies through a whole lot more development cost."

While there is no initial DMA mechanism enabling regulators to compel gatekeeper firms to adopt a specific technical standard, it would be possible for the European Commission to encourage them to do so, and in the longer term to adopt an implementing act giving the EC this

power (discussed in Section 2.2). Germany's Monopolkomission suggested an interoperability obligation should contain "comprehensive non-discrimination conditions" and not "certain (proprietary) standards or interfaces" (§236).

Google has been campaigning for Apple to adopt the Rich Communication Services (RCS) standard for iMessage. However, two technical experts we consulted were sceptical. One noted "RCS is a bloated set of bullshit designed by old people who have tons of money and political weight but do not understand the Internet, and I suspect that pushing it is a good way to make interop fail at a technical level… I'm not saying that it will necessarily fail – everything can be made work with adequate effort and money – but it definitely is not the simplest or best possible standard." A second warned:

> *In practice it's a nightmare to implement, and what you would expect from people building on 150 year-old technology that the phone network is, completely ignoring the fact the web is a thing and they would be better off learning from it… having tried to use it, it's the best way to get app developers to go do their own simple HTTP based silo because it is so inefficient and complicated.*

The EU already has a standards regulation to ensure that standards development is open, transparent and consensus based. The three EU legislative institutions reached political agreement on 13 October 2022 to update the regulation to give more power to national standards authorities.

The Bundeskartellamt interim report discussed in Section 4.1 recommended that if interoperability is to be mandated, global technical standards should be used: "Otherwise, it would be very difficult for the industry to have to meet different requirements worldwide and offer different sets of interoperable functions. For such a global standardization process, a good 60% of respondents describe the IETF as the most suitable."[53] The German Federal Network Agency similarly suggested "messenger services as Internet- based services are in principle offered worldwide. Therefore, possible measures to create interoperability must ideally also be coordinated internationally."[54]

---

[53] It is worth noting the IETF is the only standards body mentioned in the BKartA's two most relevant survey questions (qq. 45 and 47).

[54] *Interoperability between messenger services*, p.26, note 12.

The most relevant standards work underway at the IETF is on the Messaging Layer Security protocol for "efficient, secure group messaging." The organisation is also considering a new working group on More Instant Messaging Interoperability (MIMI) which would address the DMA requirement. This has already had support from organisations such as Wire, Cisco, Mozilla and 5Nine, but the gatekeepers have "so far been silent" according to one participant.

The DMA's Article 48 allows the commission to request standards be draw up by the "European standardization organisations". These are defined in the European Electronic Communications Code Art.39(1) as the "European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardisation (Cenelec), and European Telecommunications Standards Institute (ETSI))." ETSI is the most relevant in this context, although has recently been excluded from standard-setting under the EU's draft Artificial Intelligence Act as too private-sector driven.[55]

It would be possible the Commission to ask ETSI to choose one a pre-existing standard (such as from the IETF) and adopt that. According to one standards expert, "the 3rd Generation Partnership project (3GPP) on mobile telecoms references IETF standards all over the place, and ETSI adopts what 3GPP specifies, so this already happens."

A standards expert also told us there are good existing examples of public authorities working with the IETF, noting:

> *Look at STIR and SHAKEN (anti-robo-calling stuff, basically signed SIP messages). This was done entirely in parallel and driven by activity at the US Federal Communications Commission (FCC), now taken up by UK and Canadian regulators Ofcom and CRTC, which needed the standards (particularly in the incubation phase). It needed the regulators to be there at the start to cajole people into this. This was also the case for large-scale broadband measurement and emergency services. European Commission people could become part of the fabric in the same way chief technologist Henning Schulzrinne was while at the FCC.*

---

[55] Luza Bertuzzi, Commission leaves European standardisation body out of AI standard-setting, *EurActiv*, 7 December 2022.

If the Commission made a standardisation request in the medium term, it would be important civil society is able to contribute to the development of such standards. This would require the sustained ability to participate in highly technical discussions online and in person. ARTICLE 19, the ACLU and the Center for Democracy and Technology have extensive experience with participating in the work of international standards bodies such as the IETF and World-Wide Web Consortium (W3C).

5.2   Identity/discovery protocols

Messaging interoperability does not require a single identity system, but simply a service-specific format by which users of interoperable systems can refer to each other, probably based on the same domain name system which e-mail addressing is based on today. The main gatekeeper services all use mobile phone numbers and e-mail addresses to identify users, but other identifiers could be developed, such as Threema's randomly generated 8-digit identifier. Users could share identifiers using existing communication channels such as e-mail or in-person.

It *could* be argued by the European Commission that a user-friendly mechanism for a user of a competitor messaging service to connect with a specific gatekeeper service user is within the scope of the DMA. However, there are good privacy arguments against the user of a competitor service being able to upload their address book to a gatekeeper service to identify contacts (as indeed there are against this common mechanism being used within an individual service.)

The development of more privacy-friendly contact discovery mechanisms is something the Commission could support financially through its research and development programmes. Firefox Chief Technology Officer Eric Rescorla has outlined some of the various technical options and their costs/benefits.

One SME executive told us: "To be a seamless experience we need this, otherwise it's just extra hooks. If you don't know someone's e-mail address, you can't get in touch with them. But what if they have multiple addresses?" A technical expert added that in the long run "I think we need a community public key infrastructure – Keybase is an interesting go at it, but we need something that (like Matrix does for messaging) talks to all public-key infrastructure systems that are used for identity." S/he also suggested: "Who will take care of that? There are many groups, not moving very fast. Maybe the answer is people doing the messaging take some of these groups and have a more organised approach."

6   What challenges are there in the implementation of this mandate? How should civil society be involved in ensuring its successful implementation?

Which DMA implementation details remain to be fleshed out in European Commission guidance and case law, and how can civil society advocate for successful outcomes?

6.1   Privacy and security

When the EU institutions announced political agreement on the DMA, the lack of detail in the announcement on what messaging interoperability specifically meant led to criticism from some US and UK-based security experts, who noted different cryptographic protocols cannot simply be bridged while maintaining end-to-end security, as well as the difficulties of maintaining a coherent "namespace" of user identities between interoperable systems (discussed further in Section 5.2).

The EU has addressed the former criticism by allowing gatekeeper firms to meet the interoperability obligation using their own APIs, at the cost of requiring competitors to potentially implement cryptographic frameworks and protocols separately for each gatekeeper (or alternately some firms agreeing technical standards for these elements, discussed further in Section 5.1). This means, for example, that an interoperable client sending a message to a WhatsApp user must first encrypt it using WhatsApp's cryptographic framework and create a WhatsApp-compatible "envelope" for the message before delivering it to a WhatsApp server using an API or similar provided by Meta.

More broadly, the German Bundeskartellamt interim sector report discussed in Section 3.3 cites a number of concerns about the impact of interoperability on data security and privacy: "Some voices in the industry argue that the difficulties with data security and data protection could be raised on a technical level, ultimately everything is a question of willingness to invest." The report found "Respondents are relatively unanimous that interoperability, which is mandatory

by law, would make it more complicated to ensure the security of the data and thus also to comply with data protection laws."

However, the report contains some questionable statements, for example: "Since end-to-end encryption does not work under interoperability, according to [a respondent]" or "The more different providers are involved in the communication, the more points of attack there are for spying on this [meta]data. Centralization is a dangerous dynamic for this, since suddenly all this data is at a single point". One of the benefits of interoperability is a larger number of providers, and their infrastructure, make up the overall market, *reducing* centralisation (particularly from a jurisdictional perspective) and hence the ease of large-scale surveillance.

Germany's Federal Office for Information Security (BSI) published a parallel report Modern messengers – encrypted today, interoperable tomorrow? One of its conclusions was "a future, standardized communication protocol [such as the IETF's Messaging Layer Security]…would enable interoperability of different messengers with simultaneous end-to-end encryption according to the state of the art – an important step that shows that greater user-friendliness with a high level of security is not mutually exclusive." A standards expert similarly told us "users are unhappy with the disparity in the end-to-end encryption and other security properties of the proliferation of current messaging clients. There is another opportunity here — to take the best E2EE design and proliferate it via technical standards".

Eric Rescorla has published a careful analysis of the impact of the DMA on security. He concludes: "I'm more positive on the idea of interoperability for messaging systems than some others are, but it's certainly not a trivial problem and at least some of the EU timelines seem pretty unreasonable… I don't think [criticisms] are entirely without merit, but I also believe that interoperability would have real benefits that need to be weighed against these concerns." His analysis was written before the final version of the DMA was published, which includes provisions for interoperability deadlines to be relaxed if necessary, for security purposes (discussed further in Section 2.1, along with provisions for dealing with spam and other types of abuse).

Writing for the Center for Democracy & Technology, researchers Sukhi Gulati-Gilbert and Michal Luria have described how interoperable systems can remain "intuitive and easy to use", by considering privacy by design and user experience design to create "more human-centered, transparent and easy to use encrypted messaging, optimizing privacy and security." Figure 3

shows one of the user journeys they designed to illustrate issues raised by two users of a hypothetical interoperable WhatsApp and Signal communicating after meeting at a conference:
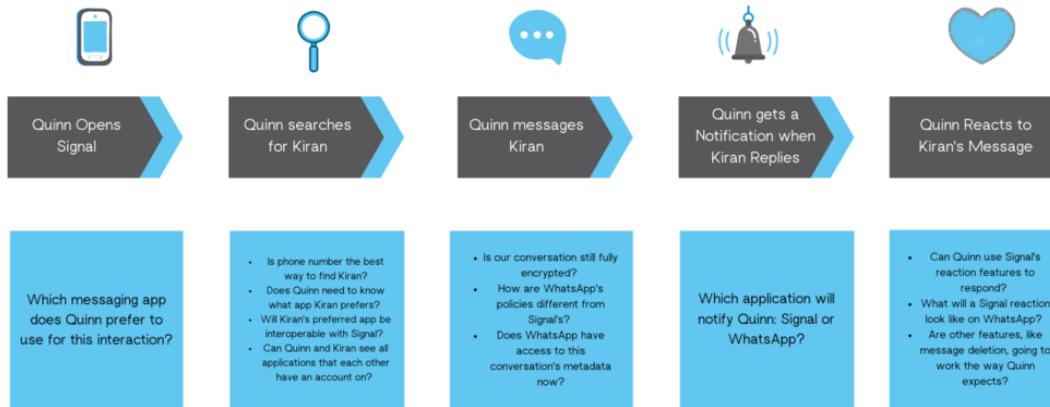

Figure 3 An interoperable messaging user journey. Source: Gulati-Gilbert & Luria (2022)

The European Data Protection Supervisor (EDPS), responsible for advising and overseeing compliance of EU institutions with data protection law, published an Opinion (2/2001) on the European Commission's original DMA proposal. It noted interoperability "has the potential to facilitate the development of a more open, pluralistic digital environment, as well as to create new opportunities for the development of innovative digital services." The EDPS recommended an explicit interoperability obligation, and the development of technical standards, which "should be in compliance with European data protection law, not lower the level of security provided by platforms and not hinder innovation via too detailed interoperability standards."

The EDPS and the European Data Protection Board (the national EU data protection authorities) are also part of a DMA "high-level group" which the European Commission must meet at least annually to receive "advice and expertise in the areas falling within the competences of its members".[56]

6.2   Safety

There has also been some criticism of interoperability provisions for their potential effect on service safety, for example from Meta whistleblower Frances Haugen, although mainly in

---

[56] Article 40.

relation to the European Parliament's discussion whether to apply them to social networking in the Digital Services Act (which was blocked from the final DMA by the EU member states).

Interoperability does not change the safety obligations of services under laws such as the DSA, whether content originates from their own service or an affiliated interoperable service. And technical measures can reduce the proliferation of content taken down from the originating service on interoperable services (for example, by sharing links to the original rather than the content itself, or takedown notifications, as is analogously required by Article 17(2) of the EU's General Data Protection Regulation).[57]

For more sophisticated moderation mechanisms, which are common in social networking services (for example down-ranking in recommendations), gatekeepers may wish to include mechanisms in their technical interfaces to notify interoperating services when such measures have been applied.

Haugen argued for "human scale content moderation". A plurality of connected, human scale platforms would be much more likely to allow this to happen than content moderation by one giant platform, giving users the option to choose to avoid the "harassment, hate-speech, conspiratorialism, disinformation and trolling that Facebook, Twitter and Reddit *won't* block".[58]

In a piece of speculative design, Cory Doctorow has mocked-up user interface elements of an interoperable social media service, showing for example how an interoperable "User Republic" service could block specific content for its users which the originating service still makes available:[59]

---

[57] The circumstances under which other services are free to ignore such notifications is an important but separate policy debate.

[58] Cory Doctorow, Unspeakable, *Medium*, 16 October 2022.

[59] Cory Doctorow, *Interoperable Facebook: How to ditch Facebook without losing friends*, Electronic Frontier Foundation, 12 September 2022.
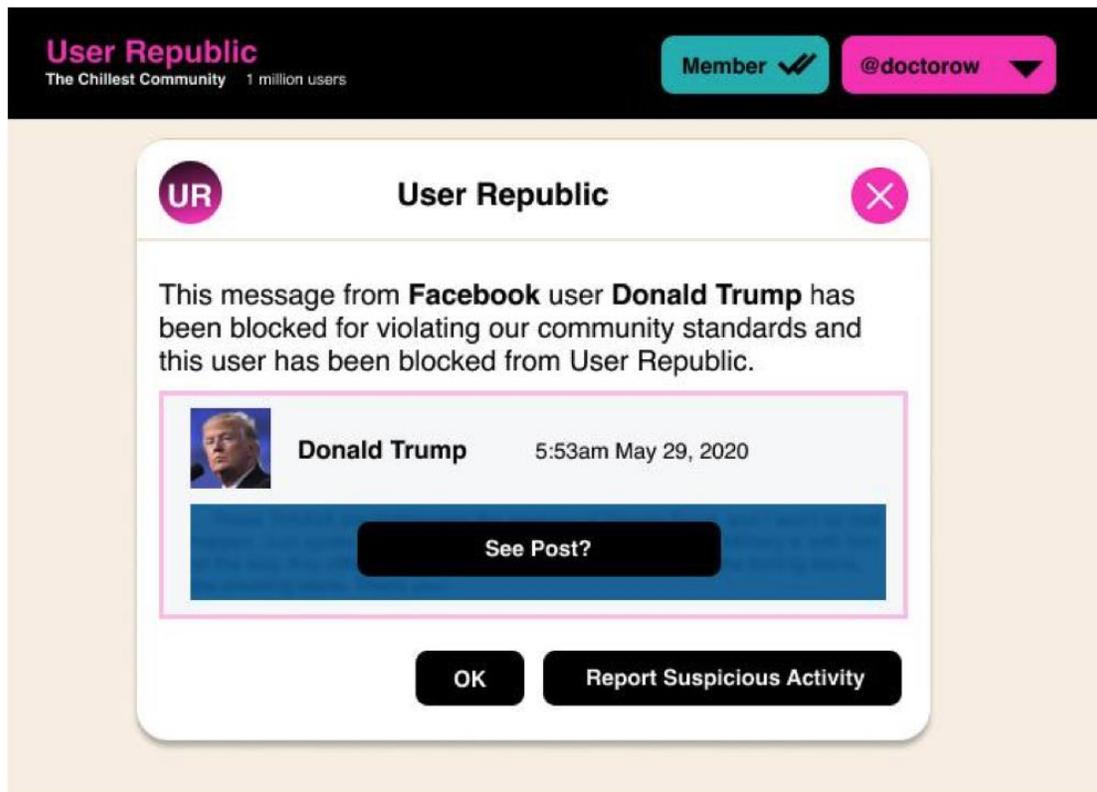
Figure 4 Mock-up dialogue showing content blocking by an interoperating service. Source: Doctorow (2022)

A real-world example is the decentralised and interoperable social networking service Mastodon, with over 4 million users. An early journalist user reported she found "the predominant culture of mastodon.social [one of many servers users can choose from] isn't San Francisco techies, it's really more of an LGBTQ-oriented space, one with a lot of anime avatars and a lot of furries. A veritable multitude of anime avatars, but sans Nazis".[60] An academic review found "the decentralized structure of Mastodon enables community autonomy", with the federation becoming "a social enterprise in and of itself" due to its open protocol, and that its "horizontal structure shifts the site's scaling focus from sheer number of users to quality engagement and niche communities."[61]

Element Chief Executive Officer Matthew Hodgson has concluded:

---

[60] S Jeong, Mastodon Is Like Twitter Without Nazis, So Why Are We Not Using It? *Motherboard*, 4 April 2017.
[61] M Liu, RW Gehl and D Zulli (2020) Rethinking the 'Social' in 'Social Media': Insights into Topology, Abstraction, and Scale on the Mastodon Social Network, *New Media and Society* 22(7), 1188–1205.

> [M]oderation and anti-abuse approaches on the Internet today are infamously broken,
> with centralised moderation by gatekeepers producing increasingly erratic results. By
> opening the walled gardens, we are forcing a much-needed opportunity to review how
> to empower users and admins to filter unwanted content on their own terms. There's a
> recent write-up of the proposed approach for Matrix which outlines one strategy – but
> there are many others. Honestly, having to improve moderation tooling is a worthwhile
> price to pay for the benefits of open APIs.

While noting interoperable E2EE messaging is more difficult to implement successfully than other services such as interoperable social media and app stores, Cory Doctorow suggests it can also strengthen user safety by providing "better, more accountable processes for disconnection and reconnection" and "using different mechanisms for deciding who is accused of spamming or harassment."[62]

6.3   Venues for enforcement and civil society advocacy

6.3.1   European Commission

The Commission may adopt guidelines on the DMA "to facilitate its effective implementation and enforcement"[63] but this is likely to happen after first experiences of gatekeeper compliance. There is a Commission consultation on an implementing regulation for the Act in December 2022,[64] but mainly on procedural (the exercise of investigatory and enforcement powers) rather than substantive issues.

This implementing regulation may also be used by the Commission to set rules on "operational and technical arrangements" for NIICS interoperability. A committee of the EU member states (with a non-voting Commission chair) gives its opinion, which the Commission must take the "utmost account of", which provides a base level of transparency which would not necessarily apply to the creation of guidelines.[65] No delegated acts are currently planned.

---

[62] Cory Doctorow, End-To-End Encryption is Too Important to Be Proprietary, *Medium*, 1 May 2022.

[63] Article 47.

[64] Article 46.

[65] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, *OJ L 55*, 28.2.2011, p. 13–18.

Competition Commissioner Margrethe Vestager has announced technical workshops on implementation, and SME Open eXchange has suggested there should be stakeholder meetings. A civil society expert told us: "these MUST include civil society organisations – the DMA should consider/help business and end-users alike." The EU's national telecoms regulators also recommended "constant regulatory dialogue is needed to develop hands-on experience and knowledge. This can only be done in a framework fostering structured and regular interactions with all relevant types of stakeholders."[66] The first, open workshop was held on 5 December 2022.

One competition policy expert was pessimistic about the progress of DMA enforcement, telling us:

> The European Commission are now saying they will 'market test' designations. Guess what? Market test will say nooooo. Then companies will sit it out a bit longer and sue. Meantime we are not even getting to obligations. Parliament are asking what is going on – but who cares? Commissioner Vestager announced workshops no one even internally knows anything about. And so on, and so forth.

A second competition policy expert was slightly less pessimistic, noting: "Interoperability is quite visible and a concept that can be explained and understood. If they immediately screw up on that it'll be a disaster also for the Commission. That's why I keep being worried about staffing with the right expertise."

A regulator told us a regulatory dialogue is needed, where the Commission will "have to engage with stakeholders in the large sense," and will "probably be more collaborative now the DMA is finalised." S/he expects the High-Level Group of regulators created by Article 40 will also be part of this dialogue, and "for instance can say some of the obligations aren't well specified, or need to be updated, amended and so on." S/he also noted:

> It's always the gatekeepers and competitors talking about the needs of the users, but it should be the users – represented by civil society – saying what they need. So civil

---

[66] BEREC, note 49, p.34.

society should sell themselves as representing the user. Basic functionality for interoperability would be a good point to share what users want.

There is also an important role for independent experts. This is something I hope will also be kept in the future in the implementation [as it was in the negotiation of the DMA].

The technical people are often working for companies, so it's very hard to find independent experts to give their opinion.

A civil society expert added that competition policy expertise is also in short supply in that sector, and further capacity-building exercises could be helpful.

6.3.2   European Parliament working group

The European Parliament rapporteur for the DMA, Andreas Schwab, is chairing an informal intergroup of MEPs to scrutinise the Commission's work on the Act, based on the Economics committee's competition working group. It held a first meeting on 7 November 2022 to "collect information on the preparatory work of the Commission and discuss future follow-ups." Legislators "are well aware that the Commission would have little to share before the implementing and delegated acts are published."[67]

The main other mechanism available to the Parliament is to ensure the Commission has sufficient resources in its budget to adequately enforce the DMA. While the Parliament failed to amend the 2023 budget to do so, the Commission is reallocating resources internally to this end. The Coalition for App Fairness, a lobby group with over 70 members such as Epic Games and the European Publishers Council, has continued to push for enforcement budget increases.

One competition policy expert told us they were pessimistic about the ability of the Parliament to influence enforcement: "I don't know [it] can do anything either. While the asymmetry of information remains so complete, this will all fail." A civil society expert added: "Everyone who thinks the EP will have anything to say about the content of DMA-enforcement/investigations lives in a fantasy world."

---

[67] Luca Bertuzzi and Molly Killeen, Tech Brief, *EURACTIV*, 7 October 2022.

6.3.3   Enforcement actions

Representative legal actions can be brought for breaches of the DMA which "may harm the collective interests of consumers."[68]

Digital rights groups in Europe are pessimistic about the prospects of directly taking private enforcement actions, due to the statutory hurdles and the high costs. Large consumer protection groups might find it slightly easier to do so under the representative action regime.[69] But both think that persuading government authorities to take enforcement action is likely to be a more effective option, not least due to the investigatory powers they have.

While national competition authorities may undertake investigations into gatekeeper non-compliance with DMA obligations (Articles 5—7) on their territories, they have limited incentive to do so, since any enforcement action must subsequently be taken by the European Commission. NCAs may also play other, limited roles in DMA enforcement.[70] The head of the Netherlands authority has suggested seconding NCA staff to the European Commission, and setting up "joint enforcement" teams.[71]

---

[68] Article 42.

[69] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, *OJ L 409,* 4.12.2020, p. 1–27.

[70] Marco Hartmann-Rüpell and Stefan Horn, The Digital Markets Act – how will it impact national competition authorities? TaylorWessing *Interface*, 28 July 2022.

[71] Natalie McNelis and Nicholas Hirst, Tech giant 'gatekeepers' should face enforcers drawn from EU and national authorities, Snoep says, *MLex Market Insight*, 9 September 2022.

7   Conclusions

The DMA's NIICS interoperability obligation will require the largest communications services to publish a reference offer for one-to-one interoperable messaging by March 2024, and to implement that offer for competitors which request it within three months, via "technical interfaces [such as APIs] or similar solutions".[72] Group chat support is required two years after services are designated by the European Commission, and video call support four years later. These deadlines may be extended if needed to "maintain the necessary level of security, including end-to-end encryption",[73] which must be "preserved across the interoperable services."[74]

A designated service which only provides E2EE to its own users (such as WhatsApp) will not be required to introduce any features which are *not* end-to-end encrypted. Designated services will also be able to require data from competitors necessary for fighting spam, phishing, and other types of service abuse – but must comply with European data protection law in using it. They may take further steps to ensure interoperable services "do not endanger the integrity, security and privacy of its services, provided that such measures are strictly necessary and proportionate and are duly justified by the gatekeeper."[75]

The largest, "gatekeeper" firms targeted by the DMA will have strong economic incentives to resist this regulation and are already reportedly preparing legal challenges.[76] Several smaller European firms and free/open-source software projects are enthusiastic about the opportunity to give their users the option to connect to the much larger numbers of users of the gatekeepers.

---

[72] Article 7(1).

[73] Article 7(6).

[74] Article 7(3).

[75] Article 7(9).

[76] Emily Birnbaum, EU's Digital Diplomat to Silicon Valley Braces for Tech Lawsuits, Bloomberg, 17 October 2022. Gatekeepers may attack the legal basis of the entire statute (as an internal market rather than competition measure); the proportionality of designations; whether specific obligations will meet the statute's aims of contestability and fairness (see recitals 32—34)…

One regulator we talked to felt the DMA obligation could have been improved with a more precise specification of the services it applied to, as well as greater consideration of the extent to which it benefits both business and end-users. S/he recognised Article 7 as a compromise but wondered if the basic functionalities specified go far enough to appeal to users, and questioned how attractive the option will be to competitor firms.

The other main potential improvement identified by our interviewees (and several regulators) would be a mechanism to require gatekeepers to implement a specific technical standard for E2EE private messaging, as the IETF is developing in its MLS working group. This would reduce costs for competitors in connecting to multiple services.

Such measures could be included in similar legislation under consideration in other jurisdictions, and added to the DMA through implementing and delegated acts. Civil society groups played a key role in the inclusion of the obligation in the DMA, and can continue to influence guidance and enforcement by the European Commission, and shape similar provisions in other jurisdictions.

8   Acknowledgments