Non-paper from the Commission services on interoperability for messenger services
and online social networks in the DMA

The purpose of this non-paper from the Commission services is to provide technical assistance to inform and facilitate the exploration of a possible compromise between the European Parliament and the Council on the interoperability obligations for gatekeepers that provide number-independent interpersonal communication services (NI-ICS or messenger services) or online social network services.[1]

1. Background

In the Commission proposal, Article 6(1)(f) of the Digital Markets Act (DMA) allows business users and providers of ancillary services to access and interoperate with the same operating system, hardware or software features that are available for gatekeepers' ancillary services. The main goal of this "vertical" interoperability is to give such providers the opportunity to interoperate with the gatekeepers' operating system and the features controlled by it, ensuring contestability in such ancillary services.

In its mandate, the European Parliament (EP), in addition to introducing some amendments to Article 6(1)(f),[2] proposes adding an obligation for gatekeepers to interoperate their messenger services or online social networks listed in the designation decisions with similar services by other providers upon request (Articles 6(1)(fa)[3] and (fb)[4] of EP mandate, respectively). Moreover, for interoperability between social networks, it would be for the Commission to specify the conditions to comply with such obligation via delegated act (Article 10(2a) of EP mandate).

The Commission services understand that the aim of these "horizontal" interoperability obligations for messenger services and social networks is to allow users of other messenger and social network services to communicate with users of the gatekeeper's services; thereby tackling the strong network effects that

[1] This non-paper does not represent nor has any bearing on the official position of the Commission.

[2] The Council mandate also introduces some changes to Article 6(1)(f). However, this paper exclusively focuses on the interoperability obligations for providers of messenger services and of online social networks.

[3] Amendment 127 reads: "(fa) ***allow any providers of number independent interpersonal communication services upon their request and free of charge to interconnect with the gatekeepers number independent interpersonal communication services identified pursuant to Article 3(7). Interconnection shall be provided under objectively the same conditions and quality that are available or used by the gatekeeper, its subsidiaries or its partners, thus allowing for a functional interaction with these services, while guaranteeing a high level of security and personal data protection;"***

[4] Amendment 128 reads: "(fb) ***allow any providers of social network services upon their request and free of charge to interconnect with the gatekeepers social network services identified pursuant to Article 3(7). Interconnection shall be provided under objectively the same conditions and quality that are available or used by the gatekeeper, its subsidiaries or its partners, thus allowing for a functional interaction with these services, while guaranteeing a high level of security and personal data protection. The implementation of this obligation is subjected to the Commission's specification under Article 10(2a);"***

gatekeepers enjoy in the context of these services, allowing newcomers to overcome those, and promoting user switching. It is understood that this is considered by the EP as a necessary means to address a lack of contestability regarding these two services.

It is useful to recall at the outset that the DMA already includes provisions that address contestability and fairness in relation to messenger services and social networks (section 2). Moreover, when considering further-reaching intervention towards interoperability, there are a number of points that require further analysis when it comes to devising an effective and proportionate solution. These can be divided into technical issues (section 3) and impact-related issues (section 4). Lastly, this non-paper closes with a number of policy options for consideration (section 5).

2. Ways in which the DMA proposal already promotes contestability and fairness in messenger services and social network services

Although the Commission's DMA proposal does not contain an interoperability obligation for messenger services and social network services, it tackles the problems that arise in the context of these two services (i.e. high entry barriers, consumer lock-in effects, strong economies of scale, capacity of gatekeepers to accumulate vast amount of data) in several manners:

- **Article 5(a) on ban on personal data combination**. This article covers those situations where gatekeepers are able to create super-profiles of consumers by combining their personal data collected across several services, including from third parties. The aim is to tackle the competitive advantage that gatekeepers have over their competitors from accumulating data and benefiting from associated network effects, as well as unfair behaviour vis-à-vis end users whose personal data is collected and combined excessively and opaquely.
- **Article 5(f) on ban on tying**. This article prohibits the bundling of core platform services identified pursuant to Article 3(7) of the DMA or core platform services that meet threshold laid down in point (b) of Article 3(2); i.e. when gatekeepers require business users or end users to subscribe or use other core platform services to use another core platform service. This is relevant for cases where gatekeepers that bundle their social network services or messenger services with other core platform services; for example, a provider of an online marketplace ties this core platform service with its own messenger service as a condition for business users to be able to sell their products on that online marketplace.
- **Article 6(1)(b) on un-installing pre-installed apps**. This article allows end-users to un-install any pre-installed software application. It promotes user switching and covers cases where an instant messaging app or a social network app is pre-installed in an Operating System.
- **Article 6(1)(d) on self-preferencing**. This article prohibits gatekeepers to engage in any form of self-preferencing to the detriment of competitors in ranking services and products offered by themselves. This includes situations

where, for example, social networks rank their own services in users' timelines more prominently than those offered by third parties.

- **Article 6(1)(h) on data portability together with Article 6(1)(i) on access to data generated by users**. These articles require gatekeepers to provide effective portability of data generated in the context of their own platform and to provide business users with real-time access to data related to the relevant core platform service. Both articles, which are particularly relevant for social networks, facilitate switching and multi-homing, giving competitors and newcomers a chance to capture a new stream of demand.

Furthermore, the EU regulatory framework already contains or foresees interoperability obligations for concrete situations. Examples are the interoperability obligation for NI-ICS or interoperability between set-top TV boxes in the European Electronic Communications Code (EECC).[5] Admittedly, these interoperability cases relate to different contexts and purposes than those pursued by the DMA. For instance, the EECC envisages interoperability between NI-ICS only for cases where end-to-end connectivity between end users is endangered due to the lack of interoperability between interpersonal communication services, which includes both NI-ICS and number-based interpersonal communication services.

3. Technical issues related to interoperability

Interoperability between messenger services and social networks raises several technical questions:

- **Data security and encryption**: Most messenger service providers offer end-to-end encryption systems to ensure that each user has an encrypted session and allow the encryption of message content with a message key that only the receiver can decipher. Current providers use a variety of encryption methods, which rely on the same technological principles but contain significant individual modifications, differing also in the level of security. For encryption to work, both interconnected networks must use the same encryption method. There are initiatives exploring new standardized protocols with a high degree of protection like the "Messaging-Layer-Security" (MLS) Protocol; however, these initiatives are relatively recent and do not seem to be widely adopted yet.
- **Data minimisation:** Limiting data collection and data sharing is one of key features that providers of messenger services have to differentiate themselves from gatekeepers. Interoperability creates new challenges in this respect: some messenger services generate and retain very little metadata whereas interoperability will tend to make use of identifiable data such as phone numbers and generate metadata in multiple contexts. Some messenger service providers do not use phone numbers to identify users but allocate IDs randomly (i.a. to protect user privacy), which is difficult to replicate across different messenger services. Moreover, with interoperability, more data would be shared across services and the gatekeeper could

[5] Article 61(2)(c) of the EECC and Article 113(3) of the EECC, respectively.

potentially have access to the messages/posts sent by users of other services to its own messaging/social network service.

- **Heterogeneity of services**: The services offered by each competitor differ considerably, particularly regarding social networks. However, full interoperability would require aligning or creating interfaces for a multitude of features that may not be exactly equivalent on both sides. In other words, unless the two interconnected services mirror each other's features, interoperability will unlikely encompass all elements of a particular service. It would be necessary to discern beforehand what functions are considered essential to be covered by any interoperability obligation as well as the design of a security-related safeguard, if any.
- **Content moderation and illegal content:** Horizontal interoperability between online platforms could create the conditions to boost the proliferation of illegal and/or harmful content as it can spread more easily and faster across different online platforms. This is relevant not only for interoperability between social networks but also between some instant messaging apps that come very close in their nature and functions to social networks. Although some decentralized networks have developed some tools for content moderation, interoperability will add an extra challenge for online platforms to address effectively the risks of availability and dissemination of illegal or harmful content.

4. Impact-related issues to interoperability

- **Incentives for users to switch and potential inverse effects:** while interoperability could increase the appeal of alternative social networks or messenger services to reach users of gatekeepers' services, this effect can also work the other way: network effects may lead to a de facto discouragement for gatekeepers' users to switch (or multi-home) as they could seamlessly reach users of other social networks or messenger services too. Furthermore, gatekeepers could benefit from the increase of incoming traffic and content that they can monetise.

- **Multi-homing:** some recent reports (e.g. Bundesnetzagentur's 2021 study on interoperability) confirmed that users, particularly of messenger services, actively engage in multi-homing, which is possible without relevant costs as apps are usually free and space on smartphones is not a limiting factor. Partly this might be a "forced" choice to stay in touch with contacts that use different services. However, many users also multi-home to keep their networks separated (e.g. family/friends/work) while benefiting from the differentiated features that each service provider offers. The DMA includes several rules enhancing choice and multi-homing (see above).

- **Impact on innovation and incentives to invest:** Interoperability generally requires mirror services and features on each side as well as common

interfaces and protocols to achieve full inter-connection. This can lead to a degree of product homogenization for every feature where interoperability is prescribed, leaving less room to engage in innovation and product differentiation. In this sense, interoperability can also discourage market players to invest in view to innovate. Alternative providers of messenger services or social network services would have already access to a user base without contributing necessarily to innovation. Thus, it would be necessary to assess carefully the risks and the benefits that an interoperability obligation would bring for users in terms of innovation.

- **Impact on business models:** Some small messenger service providers charge a small fee for the use of their services, which arguably would not work if they interoperated with others that offer their services at a zero rate. Moreover, these messenger service providers could lose their market share and would be compelled to change their business models if other market players start interoperating with gatekeepers.

5. Possible options on introducing new interoperability related obligations

From the above three important key principles emerge which should, in the view of the Commission services, determine the design of policy options on the way forward on the interoperability of messenger services and online social network services:

I. Free choice: the use of any new interoperability rights is upon request by an alternative provider of the respective core platform service to the gatekeeper only. In addition, the individual user of a service provider should be able to opt in to receiving anything from another provider;
II. The solution shall not compromise data security and privacy of communication; and
III. Incentives and room for differentiation and innovation should be preserved.

The Commission services understand that the co-legislators can converge on the principles listed above. If this is confirmed, there are three main policy options to address interoperability in the DMA that would respect these principles.

5.1. Option 1: Obligation on the Commission to further impact assess interoperability obligations

The impact assessment for the DMA proposal did not cover “horizontal” interoperability obligations between core platform services. As said in sections (3) and (4), this is a complex matter with potentially far-reaching and partly contradictory effects. Thus, under option 1, an obligation would be added for the Commission to undertake, shortly after the DMA enters into force, a market investigation pursuant to Article 17 of the DMA into messenger services and/or online social network services. The report deriving from the market investigation

could be the basis for a delegated act under Article 10 of the DMA or a proposal for a legislative change, depending on the final shape of Article 10 agreed by the co-legislators.

Pros:

- Any additional interoperability obligation would be based on a deeper evidence base;
- Allows tailoring of potential new rules to needs and dynamics in the sector; and
- Allows to map demand for interoperability and minimises the risk of unintended effects.

Cons:

- Further procedural steps necessary before effects take place.

5.2. Option 2: Strengthen user switching: obligation to provide information about contacts using alternative messenger services

Option 2 would oblige gatekeepers (upon request) to make their users pro-actively aware that one of their contacts is using a competing messenger service. This would give more visibility to other messenger services and transparency to users concerning the various messenger services that are being used by their contacts, which would promote switching and multi-homing.

This could be implemented in two ways. First, it could take the form of prompts. Currently, a number of messenger service providers already issue very similar messages if a new contact of their existing users has started using their own service.

Second, instead of receiving a message every time a contact signs up in a different messenger service, users would be able to see what messenger services are being used by their contacts directly in the respective entry of their address book. While this possibility exists today for some messenger services that already appear in address books, this option would extend it to any messenger service. Such information may help users to consider what messenger services they can use to reach their contacts while giving more visibility to alternative messenger service providers. It encourages user switching because users can see more clearly that their contacts are using other services as well.

As this obligation would require gatekeepers to be aware of the use of different messenger services by their users, it would require an agreement by the provider of an alternative messenger service (and its respective users) that such information is made available to the gatekeeper. In addition, under this variant, the obligation would not be imposed directly on the gatekeeper providing messenger services but rather on the gatekeeper for operating systems; notably in cases where the address book is an in-built software feature of the OS. In view of the nature of the service at hand, this would seem to be an obligation particularly relevant for gatekeepers of operating systems on mobile devices.

Pros:

- Builds on other DMA rules promoting switching and multi-homing;
- Fully preserves incentives to differentiate and innovate; and
- Limited technical issues around implementation (e.g. mainly the need of a common identification system of users).

Cons:

- The gatekeeper providing the messenger service may get further information about alternative services used by its end users, i.e. additional data accumulation; and
- Users have more visibility about services used by their contacts (subject to the latter's consent). This could facilitate manners of controlling communication channels in the context of an abusive behaviour (e.g. gender-based violence, stalking).

5.3. Option 3: obligation to provide interoperability for messenger services, potentially to be extended to social networks at a later stage

This option focuses on messenger services. The heterogeneity of services and complexity of technical and other issues listed above suggest that further assessment is necessary before addressing social networks. In addition, there seems to be a difference with those services as in contrast to messenger services the user is in control on where to post content. Following further in-depth analysis and experience gathered from interoperability for messenger services, the obligation could be extended later to social networks via Articles 10 and 17 of the DMA. What follows presents two sub-options that can be considered individually or can be combined to devise an intermediate sub-option, which could for example include partial interoperability based on open interoperability standards for basic features.

5.3.a. Sub-option 3a: obligation to open access to stable application-programming interfaces ("APIs") of the gatekeepers for basic features of messenger services upon request

In this sub-option, interoperability could be prescribed but only limited to basic features of messenger services such as basic text messages without additional enriched content.[6] All other features would remain proprietary to the gatekeeper (and the alternative providers). In principle, this option would still leave room for innovation and differentiation on top of the basic features of messenger services on both sides of interoperated services, given that additional features would not be interoperable.

Interoperability would have to be provided based on the existing encryption technologies and other protocols used by the gatekeeper, to which it would have to open stable application-programming interfaces ("APIs"). As a variant, one could envisage a solution where interoperability would still be provided by an API provided

[6] Further reflection may be required on whether other features such as voice and video calls over the messenger services or basic group functionalities fall into the category of basic features as they are available on nearly all messenger services.

by the gatekeeper, but that would also allow for keeping the initial encryption solutions at both sides of the service. However, as this would not be “end-to-end encryption” strictly speaking, this variant would require a sort of a “gateway” or “clearing house” in the middle, which would enable that messages that use different encryption solutions on either side of interoperable services can be read by users. Although this solution allows for keeping different encryption methods as they exist today, it also introduces further complexity, it likely leads to further collection of (meta)data by the gateway, and it opens additional entry points for cyberattacks.

A number of additional requirements on the gatekeeper could accompany the obligation, which would be laid down in the DMA:

- Interoperability to be provided only upon request by a provider currently or intending to be active in the EU;
- Possibility of rejecting requests from “rogue providers” upfront based on public security grounds of Article 9, or to terminate interoperability in case of repeat breaches of security/privacy laws;
- Obligation on the gatekeeper to publish a “reference offer”, which would identify the main commercial and technical characteristics of such an API-enabled interoperability, regardless of any request being submitted;
- Interoperability would have to be provided free of charge; and
- Exchange of (meta)data and access to contact lists should be limited to the extent that is necessary to provide effective interoperability and remain at the choice of the provider requesting interoperability, where possible. It would remain the obligation of the requesting provider to inform its users about any personal and non-personal data that the provider intends to collect and share with the gatekeeper to ensure effective interoperability, and collect the relevant consent in line with applicable EU law (for example GDPR or ePrivacy Directive).

Regarding the adequacy of the reference offer, the Commission could, on its own initiative or upon request of the gatekeeper, apply the regulatory dialogue process to specify measures further. Due to the technicality of the issues at stake, a mechanism would have to be provided for involving experts or regulators such as BEREC or its members in the assessment of the reference offer and potentially also in the settlement of individual disputes. In addition, co-legislators already converge on the possibility for the Commission to develop guidelines under the DMA, which could address operational and technical questions that may arise once more experience of various interoperability aspects has been gained.

Due to the factors above, this solution may require an exception to the implementation timelines of the DMA. It could be foreseen, for example, that the reference offer has to be made available within the standard compliance period under Article 3(8) and actual interoperability has to be provided within an additional timeframe following a request for interoperability from any alternative provider. Those specificities may also suggest that this provision should be developed as a tailored, self-standing obligation outside Articles 5 or 6.

Pros:

- Allows users to communicate across services (assuming that competing providers request interoperability with the gatekeeper services and that users of each service accept);
- Preserves incentives to differentiate and innovate, mainly on features beyond basic functionalities; and
- Can be implemented in a shorter period compared to sub-option 3b below that proposes prior development of a standardized framework, and be enforced by the Commission albeit with assistance from expert bodies.

Cons:

- Risk of certain commoditization of messenger services and slow down of innovation speed; entails some free-riding of providers on the network built by the gatekeeper;
- May limit incentives for multi-homing, leading to a reinforcement of the gatekeeper's position (alternative service providers of messenger services would need to assess this risk before requesting interoperability);
- Uncertainty of demand, as requesting providers have to adapt to API/protocols of the gatekeeper, which inevitably implies an increase of costs for smaller providers;
- need for constant regulatory oversight, which may imply additional resources for regulators
- Exchange of contact and metadata with gatekeeper unavoidable; and
- Need to address risk of proliferation of illegal and/or harmful content.

5.3.b. Sub-option 3b: full interoperability based on open interoperability standards

Under this sub-option, the DMA would prescribe a full interoperability obligation on gatekeepers. However, this would not be based on the existing protocols of the gatekeeper to which the other providers have to adjust but based on a new, open standard imposed by the Commission. This standard would be developed by the industry upon mandate by the Commission to the relevant European standardization bodies. In other words, the obligation would be subject to the development, most likely by the European standardization bodies under the mandate and auspices of the Commission, of an open interoperability protocol that would then become mandatory to comply with the obligation.

Pros:

- Full communication across services (assuming that other messenger service providers request interoperability with the gatekeeper services); and
- Avoids that the gatekeeper designs the APIs in a biased way and that it continues to determine de facto the main industry standard.

Cons:

- Development of a standardized framework will take considerable time, no immediate impact;

- Standardized framework seems more relevant in an scenario where all providers are subject to interoperability obligation;
- Need of a standard to be updated regularly to adapt to technical developments (with the risk of falling behind rapid developments in case of full interoperability) as well as need for constant regulatory oversight, which may imply additional resources for regulators;
- Requires significant adaptations on the side of the gatekeeper without it being clear whether there is significant demand, i.e. when no or very few alternative messenger service providers may show interest and most may prefer to continue with proprietary solutions;
- Requesting providers also have to adapt to new standard, which inevitably implies an increase of costs for smaller providers (similarly to adaptations also required under sub-option 3a);
- No differentiation or innovation on all features covered by the standard, which would apply to a wider scope of features than in sub-option 3a where the features covered would be more limited (i.e. basic features);
- Exchange of contact and metadata with the gatekeeper; and
- Risk of proliferation of illegal and/or harmful content across different services.