Interoperability for messenger services and online social networks in the DMA

Fundamental concerns regarding mandated interoperability requirements remain

Given its narrow scope, the DMA is not well placed to mandate meaningful, holistic and comprehensive interoperability obligations for social network platforms and messaging services. As it only applies to a limited number of gatekeepers, what is proposed would be more akin to an access obligation.

Legislators should ensure that any final provisions included in the DMA are well-evidenced, proportionate and do not produce side effects that cause significant detriment to users (i.e, consumers) and/or the wider EU economy.

Against this background, any final proposals to mandate interoperability of social network platforms and/or between 3rd party messaging services risks stifling innovation, compromising privacy and security, and creating more homogenous services. To the extent that the DMA's provisions are focused on fostering market contestability, it is already the case that digital services operate in a largely open environment which has served to enrich users' online experiences significantly. That is particularly the case at the app layer of the internet technology stack which is evidenced by the wide variety of existing messages services and widespread multi-homing by users.

Notwithstanding the above fundamental concerns regarding any proposed interoperability requirements in the DMA, in the interests of enabling a meaningful compromise position to be reached, we set out below:

- Key concerns regarding Option 3A, which is set out in the EU Commission's Non-Paper and which limits itself to messaging services, need to be addressed should this option be pursued.
- A mark-up of the draft text provided by the European Parliament, which as a minimum is necessary in order to reflect a more appropriate, proportionate and workable version of Option 3A.

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 order to make this option appropriate, proportionate and workable, it is critical that this option:

(i) Is limited to basic features only and protect innovation, which should be strictly limited to basic text, and possibly video, audio and image attachments (as suggested in recital 52a EP text)).
(ii) Protects the ability to offer E2EE services.
(iii) Ensures user & recipient choice and consent.
(iv) Does not require gatekeepers subject to this option to open-up their proprietary APIs.

(v) Is afforded additional time for compliance that reflects the complexity of this option, and incorporates appropriate processes to ensure meaningful stakeholder engagement and for complex technical matters to be settled.

Key additional items that must be reflected in Option 3A	**Rationale**
Option 3A should be limited to basic features ● The features should be limited to basic text and possibly video, audio and image attachments; and in any event, not go beyond those indicated in recital 52a.	These are the core features that users value. It would be incredibly challenging to implement and maintain anything beyond these basic features. Attempting to do so would significantly delay the process, and risk a sub-par experience for users if features don't work correctly. Extending beyond basic features also risks dampening broader innovation, as the market would have to move at the pace of the slowest, least feature rich experience.
Option 3A should not compromise data security and privacy of communication. ● *End-to-end encryption:* A provider should be allowed to set the privacy and security standard of its API and not be obliged to degrade this standard or offer API-enabled interoperability to entities which have less secure data use and data management capabilities or policies. ● *Rejection:* there should be a possibility for a messaging service to reject 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. ● Profile search: Gatekeepers should not be obliged to offer identity/profile search capabilities to third parties, which would conflict with their users' privacy wishes. Interoperability can be facilitated via specific identifiers that can be shared by users.	It is imperative that interoperability does not weaken EU users' privacy, security and safety when using messaging services. Without these guardrails, users would be at greater risk of data hacks, surveillance, fraudulent or scam messages, unwanted contact, spam, and illegal and harmful content such as CSAM and misinformation. The circumstances of the recent conflict in Ukraine demonstrate the importance of people's ability to communicate securely and free from government / foreign government surveillance.

Option 3A should be based on users' and recipients' choice. ● *Opt-in*: Gatekeepers should be allowed to provide end users of their qualifying messaging CPS the choice to initiate or receive communication using the API in order to communicate with users who are not on their own networks/services - instead of imposing it. ● *Recipient's consent*: messaging services should provide end users with the ability to accept any or all incoming communications transmitted through the API-enabled interoperability.	As above, to protect privacy and safety, it is essential that EU users have control over their messaging experience and are given the choice to opt in to receiving communication via the API and can reject any or all incoming communications should they wish to do so.
Option 3A should not compromise proprietary messaging protocols. ● Gatekeepers should be allowed to retain their own proprietary messaging protocols whereupon they are free to innovate and improve privacy and security.	In order to protect innovation and privacy and security improvements for users, gatekeepers should be allowed to retain their own proprietary protocols. Without this, there is a risk of homogenisation of messaging services in the EU and a risk that EU citizens would not have access to new features and enhanced privacy, security and safety measures that are available to others around the world.
Option 3A should acknowledge that interoperability is very complex and difficult to implement and the timeline should reflect this. ● *Appropriate timeline:* the timeline for compliance with the requirements (e.g., drafting of Reference Offer in this option, publication of the Offer, development of the relevant messaging protocols) should duly reflect the complexity here and allow for a thoughtful approach. ● *Appropriate processes:* there needs to be proper consideration and consultation, that takes into account the many difficulties here of ensuring appropriate implementation, as well as technical and practical issues that will arise. These should be solved in a thoughtful manner, which takes time.	Interoperability is complex and very hard to implement. A lot of work will be required to ensure adequate privacy, safety and security protections for EU users and there is a lot to design. It is critical that the right stakeholders are involved (e.g., European Commission, BEREC and others, as well as the industry) and that the right processes are followed. It is key that this is not rushed if the legislature is truly interested in turning this into reality.

REQUESTED MARK-UP OF RECITAL 52a), AND ARTICLE 6(fa)

Additions requested are identified in blue, and deletions in ~~strikethrough~~.

R52a. The lack of interconnection ~~features~~ among the gatekeepers' number independent interpersonal communication services may substantially affect users' choice and ability to switch due to the incapacity for end users to reconstruct social connections and networks provided by the gatekeeper even if multi-homing is possible. Therefore, it should be allowed for any providers of equivalent ~~core platform~~ services active in the Union to interconnect with the gatekeeper's number independent interpersonal communication services ~~or social network services~~ upon their request and free of charge, subject to the consent of relevant end users of each service. Interconnection should be provided through open application programming interfaces under the conditions and quality that are available or used by the gatekeeper, while ensuring a high level of security and personal data protection. In particular, a gatekeeper using end-to-end encryption to safeguard the security of its services shall not be required to interconnect with providers using a less secure standard and any exchange of personal data shall be kept to the minimum required to ensure interconnection. ~~In the particular case of number-dependent intercommunication services,~~ iInterconnection requirements should mean giving the possibility for third-party providers to request access and interconnection for basic features ~~[such as text, video, voice and picture]~~ but should not prevent the gatekeeper from innovating and introducing new features in relation to its service. ~~, while it should provide access and interconnection on basic features such as posts, likes and comments for social networking services. Interconnection measures of number independent interpersonal communication services should be imposed in accordance with the provisions of the Electronic Communications Code and particularly the conditions and procedures laid down in Article 61 thereof. It should nevertheless presume that the providers of number independent interpersonal communications services that has been designated as a gatekeeper, reaches the conditions required to trigger the procedures, namely they reach a significant level of coverage and user uptake, and should therefore provide for minimum applicable interoperability requirements.~~

A3(8a) The gatekeeper shall comply with the obligation laid down in Articles 6(1)(fa) within six months after the Commission has adopted implementing acts pursuant to Article 36(1)(ba).

A6(1)(fa). Allow any providers of number independent interpersonal communication services active in the Union upon their request and free of charge to interconnect with the gatekeepers' number independent interpersonal communication services identified pursuant to Article 3(7) subject to the consent of relevant end users of each service. 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 basic features of these services, while guaranteeing a high level of innovation, security and personal data protection.

A24(1) The Commission may take the necessary actions to monitor the effective implementation and compliance with the obligations laid down in Articles 5 and 6 and the decisions taken pursuant to Articles 7, 16, 22 and 23.
(2) The actions pursuant to paragraph 1 may include the appointment of BEREC, independent external experts and auditors to assist the Commission to monitor the obligations and measures and to provide specific expertise or knowledge to the Commission.

A36(1) The Commission may, and in respect of Article 6(1)(fa) shall, adopt implementing acts concerning:
(ba) the nature and scope of the obligations referred to in Article 6(1)(fa), which shall be imposed only to the extent necessary to ensure interconnection of number independent interpersonal communications services for basic features and may include, after consulting BEREC and taking utmost account of its opinion, proportionate obligations on providers of those services to publish open application programming interfaces, including relevant technical and commercial information.

****