DMA and interoperability of encrypted messaging

March 11th, 2022

Abstract and recommendations

Current trilogue proposals relating to the Digital Markets Act include one that would require service providers to interoperate their messenger services or online social networks with similar services by other providers upon request. Interoperability between services is a laudable aim. The Internet Society wants to contribute to the discussions, because the proposed obligations could have the dangerous unintended consequence of putting user security and privacy at risk, by undermining end-to-end encrypted services.

In the document, *"Draft Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (digital markets act) - Commission non-papers,"* the European Commission outlines three proposed policy options in pursuit of the goal of interoperability:

> OPTION 1: The European Commission carries out an impact assessment whose results are used as the basis for a delegated act under Article 10 of the DMA or a proposal for a legislative change.
>
> OPTION 2: Strengthen user switching by introducing an obligation for service providers to provide information about contacts using alternative messenger services.
>
> OPTION 3: Oblige service providers to provide interoperability on messenger services.
>
> A. Oblige the use of open access to stable application-programming interfaces ("APIs") of the gatekeepers for basic features of messenger services upon request
> B. Full interoperability based on open interoperability standards.

Recommendations

The Internet Society makes the following recommendations based on the European Commission's proposed policy options:

1. That an **impact assessment** on the risks to end-to-end encryption resulting from mandated interoperability for the providers of messaging services as described in Policy Option 1 **is conducted BEFORE any introduction of these obligations**. The Internet Society's Internet Impact Assessment Toolkit[1] is a relevant resource to assess the implications of policy options on the open, globally connected, secure and trustworthy Internet.

2. That Policy Option 2 be subjected to a privacy impact assessment, recognizing the risks to user security and privacy, and **any resulting implementation be strictly on an "opted-out by default" basis,** with requirements that users are **given appropriate information about the associated risks before opting in.**

3. That Policy Option 3(A) and (B) be assessed in terms of their impact on end-to-end confidential communication and rejected if found to undermine end-to-end encryption through mandated interoperability. Encryption and especially end-to-end encryption are fundamental the security and well-being of European individuals, businesses, communities, and institutions.

About the Internet Society

The Internet Society is a global non-profit organization founded in 1992 by some of the Internet's early pioneers. We believe the Internet is a force for good and we are working towards an open, globally connected, secure and trustworthy Internet that benefits everyone. With 110 active chapters across six continents, of which 28 are in Europe, and more than 80.000 individual users supporting our activities, the Internet Society is a significant stakeholder, and a reliable, technically informed civil society interlocutor for Internet governance issues.

[1] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

European Citizens Rely on End-to-End Encryption

Encryption is an essential tool for securing the personal safety of European Internet users and businesses as well as the security of its member states and institutions. End-to-end encryption (E2EE), in particular, safeguards information even when we have to entrust it to third parties for communication. E2EE is particularly vital for the personal security of members of at-risk groups, including refugees escaping conflict zones[2] journalists,[3] the LGBTQ+ community,[4] and victims of domestic abuse.[5]

European businesses depend on strong encryption to conduct business and manage the data of EU citizens in a compliant and safe manner. European companies use encryption in their products, fueling innovation and growth for the European technology sector.[6] European institutions use encryption, especially during moments of heightened hostilities, for protection against the actions of hostile governments that would seek to cause wide-scale, systemic disruptions to economies, infrastructure, and security.

Contact Sharing Obligations and User Privacy

Option 2: The proposed obligation for service providers to provide information about contacts using alternative messenger services seeks to nudge users to explore the wide array of alternative messaging services on offer. This is a commendable effort to support consumer choice but could put users at risk through privacy violations, and the proposal should be subjected to a thorough privacy impact assessment.

For some users of end-to-end encrypted messaging services, maintaining a clear and robust separation between their communications in different contexts is vital. Under Option 2, if a sender's phone number is given to someone for use on a popular service, the recipient would then be able to see every other messaging app that the sender has registered with the same number.

The use of apps is potentially sensitive information and shouldn't be disclosed automatically. Particularly for members of vulnerable communities, like LGBTQ+ individuals[7] or survivors of domestic violence[8], knowledge that the person is on an end-to-end encrypted service could put them in danger. A popular service having access to this data could also give it an anti-competitive advantage.

---

[2] https://www.nytimes.com/2021/08/28/us/help-afghanistan.html

[3] https://cpj.org/2020/03/cpj-internet-society-journalist-encryption-fact/

[4] https://www.lgbttech.org/post/2019/11/22/lgbt-tech-release-encryption-one-sheet

[5] https://www.internetsociety.org/wp-content/uploads/2020/12/NNEDV_Survivor_FactSheet-EN.pdf

[6] https://techcrunch.com/2021/01/27/protonmail-threema-tresorit-and-tutanota-warn-eu-lawmakers-against-anti-encryption-push/

[7] https://www.internetsociety.org/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community/

[8] https://www.internetsociety.org/wp-content/uploads/2021/05/NNEDV_Survivor_FactSheet-EN.pdf

Further, there are potential usability and user transparency risks with the "contact information" approach under Option 2. Many apps do not maintain their own lists of contact information, but instead rely on a platform or device's native contact book (e.g. on iPhones, laptops, etc.). The contact book is not designed to allow a user to specify which app can have access to which record, raising the risk of inappropriate disclosure.

If contact sharing obligations are implemented by the DMA, they would need to be implemented with opt-in only (off by default) settings for users, with requirements that users are given appropriate information about security and privacy risks before opting in. Further, Policy Option 2 must be subjected to a privacy impact assessment, recognizing the risks to user security and privacy, before any implementation.

Interoperability Obligations and End-to-End Encryption

Option 3(a): Obligations for messenger service providers to provide open access to the stable application-programming interfaces ("APIs") of gatekeepers under Option 3(a) raise security, privacy, and feasibility concerns. The Commission's non-paper notes that under this option "interoperability could be prescribed but only limited to basic features of messenger services such as basic text messages without additional enriched content."

In our view, Option 3(a) starts from an incorrect assumption, namely, that there is consensus about what constitutes an appropriate set of "basic features" for a messenger application and service. For instance, even though the two most similar E2EE apps on the market (Signal and WhatsApp) are based on the same end-to-end protocol[9], there remains a "basic feature" which they implement differently, and which would rule out interoperability.

This "basic feature" is the policy of sending messages when a recipient's device key changes part-way through a conversation. Signal's approach is that it will discard "pending" messages under these circumstances on the basis that they cannot be delivered with an acceptable level of assured security, given the expiry (for whatever reason) of the recipient's device keys. WhatsApp, conversely, will allow pending messages to be delivered and read despite the change of device keys. WhatsApp will then update the recipient's keys to restore synchronization with the sender.

This is a "basic feature", yet the two apps reflect different decisions about the security and usability design, and both development teams think their own solution is the correct one. The two cannot interoperate and still both deliver the security and usability their users expect: in the eyes of the developers, one of the apps would have to function incorrectly to achieve interoperability.

[9] https://en.wikipedia.org/wiki/Signal_Protocol

The Commission's non-paper attempts to offer a solution to this situation: "one could envisage a solution where interoperability would still be served by an API provided by the gatekeeper, but that would also allow for keeping the initial encryption solutions at both sides of the service." This solution is flawed in practice, however, as doing so would undermine end-to-end encryption: the intermediary would have to compromise on the security design of either one encryption service or the other. The service provider or some other third party might even require the ability to decrypt user messages for them to be transferred and re-encrypted by the other messenger service. Introducing this ability would create a dangerous vulnerability that could be exploited by criminals or hostile state actors to access encrypted messages, leaving Europeans at greater risk.

Option 3(B): Under the Policy Option 3b, messenger providers would have to adjust but based on a new, open standard imposed by the Commission. For end-to-end encrypted communications services, this faces the challenge that many such services already exist, and at considerable scale. Motivating the market leaders to converge on a new standard would be a significant challenge. In addition, mandating a common and probably prescriptive standard would give end-to-end encrypted messengers less latitude to address known vulnerabilities, if patching a vulnerability would harm the service's certification of conformance to the standard. This approach may also reduce flexibility, limiting the ability of messaging services to innovate in response to the changing cybersecurity landscape as well as user expectations.

Conclusion

Improving interoperability is an important goal. However, this document has identified several dangers presented by Policy Options 2, 3(a), and 3(b). We recommend that the European Commission conduct a thorough impact assessment as described in Policy Option 1 before implementing any of the discussed measures, and supplement it with specific privacy impact assessments for any remaining candidate Options. The **Internet Society's Internet Impact Assessment Toolkit**[10] can serve as a resource in assessing policy implications to the open, globally connected, secure and trustworthy Internet.

[10] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/