# DMA INTEROPERABILITY AMBITIONS NEED TO BE TEMPERED BY REALITY

As the European Union and member states move forward with implementing the ambitious Digital Markets Act (DMA), they face some big challenges in terms of how they will harmonize potentially conflicting goals and statutes. These challenges are especially acute around the big questions related to how they can protect user privacy, security and elevate trusted technologies.

These questions will be on full display, and will be especially difficult to grapple with as the European Commission hosts its next workshop on February 27th on the DMA's requirement for interoperability between popular encrypted messaging apps. This meeting comes after a growing number of experts have warned that end-to-end encryption interoperability, as proposed by the DMA, is nearly impossible without sacrificing and undermining the basic user privacy and security that users have come to rely upon.

With respect to interoperability for encrypted messaging apps, the European Commission's ambitions may need to be tempered by technical realities. One thing that is likely to become apparent in the workshop, messaging is simply a tough place to begin to try and achieve interoperability. Steve Bellovin, one of the world's leading cryptographers and a former chief technologist at the U.S. Federal Trade Commission, warns that end-to-end encryption interoperability as proposed in the DMA is "somewhere between extraordinarily difficult and impossible." Others are even less sanguine, predicting that the policy is doomed to fail. But the risk is not just that competing goals are fundamentally at odds with each other, cryptography experts have argued that moving forward without considering the technical complications is "mind numbingly foolish, privacy-destroying, encryption-busting, [and] innovating-killing."

Why are these experts so concerned? One specific challenge involves identification and authentication of users and the way that mandated interoperability could undermine existing security mechanisms and ultimately enable new forms of spoofing and phishing. At present, each messaging platform is built around a different ID verification mechanism: an e-mail address, telephone number, AppleID, Facebook name, Twitter handle, and so on to authenticate users. Thus, one of the extremely hard questions European regulators will face involves how to facilitate the identification and authentication of users across messaging systems without undermining encryption for millions of users in Europe.

A few outliers have suggested it is technically possible to create interoperability without sacrificing privacy by using a "Bridge," which would involve decrypting messages, potentially on someone's device, before re-encrypting the message for the second half of the message's journey. This solution raises its own set of complications. A bridge would, quite simply, create new vulnerability vectors for invading privacy and enabling access to protected communications. Achieving interoperability by multiplying the threats to user security and privacy is, needless to say, very problematic.

Given the technical complications, the Commission's accelerated timeline has raised further alarms. Many question whether the DMA's three-month compliance timeframe is even achievable across companies. Meta Platforms (Facebook), for instance, announced plans to interconnect and encrypt three of its own messaging products in March 2019. This project is still not completed.

We hope that the February 27th workshop and subsequent DMA workshops will lead European regulators to focus first on achieving interoperability between its policy goals. That may require it to make some course corrections to ensure that its DMA policy goals are fully interoperable with critical security and privacy goals.

In a global communication ecosystem, mandates that could weaken private and secure encrypted communications in Europe, could have big impacts on the privacy and security of communication for American users too. In the U.S., in the wake of the Supreme Court's decision repealing **Roe v. Wade**, companies are being urged to take steps to better protect private communications by adopting strong encryption, privacy and security measures. Access to private communications is not a hypothetical concern. After the **Dobbs** decision, we saw how unencrypted direct messages between a mother and her teenage daughter about seeking an abortion were handed over to local police for prosecution.

Our own Trusted Future research has shown that American consumers want their private messages kept private and protected with strong encryption that ensures that no one but the sender and the intended recipients are able to read their messages, and they want policymakers to reject efforts that have the effect of weakening strong encryption.