October 2021

DOT Europe paper

End-to-end encryption
Between privacy enhancement and law enforcement

Encryption and particularly end-to-end encryption (E2EE) are more and more often discussed in relation to debates on digital issues at European and national level. DOT Europe, the leading voice of digital companies in Europe, has already published a one-pager explaining how encryption, and more precisely end-to-end encryption, work. In this new paper, we outline the state of the debate on this kind of encryption and offer our position on the issue.

As E2EE enables only the parties on the sending and receiving ends of encrypted content to access it, it is **considered one of the best methods of ensuring privacy, security and confidentiality of communications**. It is encouraged in numerous pieces of current and upcoming EU legislation (GDPR, EECC, Cyber Security ACT; NIS II) and regulators (DPAs, security agencies) and courts (Case C-311/18 "Schrems II") have recommended it for compliance with many legal requirements. Inasmuch as it protects privacy of communications, it provides a **safeguard against human rights abuses and illegitimate surveillance by outside parties** and by the platform used to communicate itself.

However, E2EE is also described as a hindrance for law enforcement authorities, which sometimes require access to illegal content to complete their investigations. Indeed, current initiatives in the Council and the European Commission on the role of encryption in criminal investigations to detect and report CSAM represent a move towards providing "lawful access" to end-to-end encrypted content. Similarly, the expanded scope of the recently adopted EU Telecoms code (EECC) has exposed over the top communication services, many of which are E2E encrypted, to national interception laws that were designed for the analogue wiretapping world where intercepting one communication did not create a security vulnerability for them all.

With this in mind, DOT Europe would like to emphasise the following considerations:

- We fully support the need to cooperate with law enforcement and authorities in the context of a criminal investigations or other matters of public interest. When presented with a valid legal request, the companies operating communication systems should cooperate and provide data when and where available in compliance with applicable laws, international legal norms.
- Whilst we acknowledge that the lack of ability for provider facilitated real – time intercept of E2EE can in certain situations be presented as a challenge for law enforcement, technology, new processing capabilities etc. have given authorities access to an unprecedented amount of data and opened up many new channels to monitor and investigate criminal activities without the need to expose all users to security and privacy risks.
- As the entire economy, commerce, infrastructure and services move online, strong encryption has become fundamental in securing this eco-system. It not only protects users and systems from increasingly sophisticated cyber-attacks, but also from basic errors that might result in data being compromised.
- Due to the nature of E2EE services, **any requirement to engineer an intercept capability, in whatever form, is akin to asking for a backdoor that would impact the entire service and constitute a significant security and privacy risk for all its users**.

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 2 626 1990

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA