SQUIRE PATTON BOGGS

Are We Heading Towards EU Legislation Banning End-to-End Encryption?

December 2020

Introduction

The possibility to impose EU obligations to messaging services using end-to-end encryption to cooperate with law enforcement agencies has been dominating justice and home affairs discussions for some time now, as a way to better prepare for planned terrorist attacks throughout Europe. A Council of Home Affairs Ministers endorsed on 14 December 2020 a Council Resolution on Encryption, paving the way to create a regulatory framework to that effect.

Since 2015, a series of campaigns run alternately by Europol and the Federal Bureau of Investigation, or the services of the "Five Eyes"[1] alliance, were building towards the development of this Council Resolution. In October, Interior Ministers of the alliance called on the internet companies once again to equip their IT networks with backdoors so that law enforcement agencies and competent authorities could access end-to-end encrypted apps to police online criminality.

Overview

The Council Resolution (Resolution) on Encryption has been in the works for some months now. The German Presidency has concluded the work on the Resolution that could lead in the long term to a ban of end-to-end encryption for messenger services, to allow investigating authorities to have direct access to end-to-end encrypted communications from such providers.

Even though this proposal was originally initiated by the UK, it was picked up by Germany in 2019, and France has been pushing this proposal throughout the year – with renewed impetus following the terrorist attacks in France and Austria.

What Is at Stake?

However, necessary safeguards need to be established to ensure EU citizens' privacy is respected and cybersecurity systems are not compromised. The Resolution underlines that "Protecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world, and upholding the rule of law, are extremely important."

Most importantly, it is noted that "Any actions taken have to balance these interests carefully against the principles of necessity, proportionality and subsidiarity." With the adoption of the Resolution, there is a clear message on the need to develop an EU regulatory framework and to further assess how such a framework would be established.

Importantly, the regulatory framework should encompass technical and operational solutions to be developed with service providers and relevant stakeholders to enable access to authorities to encrypted data.

At this point, the legislative route by which they would be given effect is uncertain. However, considering the Council has not directly asked the European Commission to prepare a legislative proposal, it is most likely that a future legislative measure would be introduced within the national security remit, in a form of a Council Decision, which would require unanimity voting to be adopted. France, Germany and Austria appear to be the countries to lead the efforts to create such a regulatory framework, following the adoption of the Resolution.

Similarly, the adoption of the Resolution could also have an impact *vis-à-vis* the implementation of the European Electronic Communications Code (EECC, Directive EU/2018/1972), due by 21 December 2020. Member states could leverage the adoption of the Resolution to adopt their own measures at national level using the provisions of EECC Article 3(c) that the "Directive is without prejudice to ... actions taken by member states for public order and public security purposes and for defence."

Conclusions

Whereas the adoption of the Resolution aims to put a framework in place that would strengthen investigative powers against terrorism, services using end-to-end encryption could face a significant risk. The Resolution calls on the tech industry to devise mechanisms under which encrypted data can be accessed by competent authorities, while complying with "the principles of legality, necessity, proportionality and subsidiarity". Notwithstanding the principle of the Resolution, creating backdoors to communication services – analogous to the lawful intercept capability required of telecommunications operators – could weaken IT security and could incite action by cyber criminals and foreign intelligence services.

The broad range of consequences to the tech sector stemming from the Resolution should be closely monitored and assessed. We stand ready to provide assistance in advising clients on the most effective strategic business decisions and legal considerations in this context.

1 The Alliance includes the UK, the US, Australia, New Zealand and Canada.

Contacts

Matthew Kirk
International Affairs Advisor, London
T +44 20 7655 1389
E matthew.kirk@squirepb.com

Francesco Liberatore
Partner, London
T +44 20 7655 1505
E francesco.liberatore@squirepb.com

Georg Serentschy
Senior Advisor, Brussels
T +322 627 1111
E georg.serentschy@squirepb.com

Wolfgang Maschek
Partner, Chair of European Public Policy Practice, Brussels
T +32 2 627 1104
E wolfgang.maschek@squirepb.com

Christina Economides
Public Policy Advisor, Brussels
T +32 2 627 1105
E christina.economides@squirepb.com