

RE: Secure services express their support for the ePrivacy Regulation

Brussels, 06 June 2018

Dear Ministers,

As companies that built our services around protecting users' data, we very much welcomed the entry into force of the General Data Protection Regulation on 25 May. It is a much-needed legislation that helps to strengthen individuals' privacy and control over their data.

Another timely legislation is the ePrivacy Regulation which aims to provide a high-level privacy protection for users of electronic communications services and to level the playing field for all market players. The proliferation of data breaches and misuses, such as the recent Cambridge Analytica scandal, has made it difficult for anyone to trust online companies with their data. It is therefore of utmost importance that we continue to set high standards for all players in the digital economy.

There has been a lot of fear-mongering about the potential devastating impact the rules could have on the digital economy. Contrary to these voices, we believe the Regulation will create an opportunity for EU businesses and spark innovation. It will force data-driven companies to rethink their business model and bring the emergence of a service-led economy in which users increasingly share their data with companies who respect their rights and handle their data with care.

We, therefore, firmly support the draft proposal. However, we also believe it is incomplete without provisions requiring a privacy by design and by default approach to software development. In this regard, we would like to bring one particular element to the Ministers' attention: the indispensable role end-to-end encryption plays in protecting individuals' data online and in increasing their trust in the security of digital services. That is why we welcome the European Parliament's amendment on end-to-end encryption and urge the Ministers, ahead of the 8 June Telecommunications Council, to consider its addition to the proposal:

"Providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the **confidentiality and integrity** of the communication in transmission or stored are also **guaranteed by technical measures** according to the state of the art, **such as cryptographic methods including end-to-end encryption of the electronic communications data**. When encryption of electronic communications data is used, **decryption by anybody else other than the user shall be prohibited**. [...] Member States shall not impose any obligations on electronic communications service providers or software manufacturers that would result in the weakening of the confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used."¹

We look forward to the outcome of the 8 June Council meeting and remain at the Council's disposal to discuss the best way forward to restore trust in the digital economy and to encourage privacy-focused entrepreneurship.

Navroop Mitter, CEO, [ArmorText](#) (Gryphn Corporation)
Szabolcs Kun, Co-Founder & CEO, [CryptTalk](#)
Ladar Levison, Founder, [Lavabit](#)
Dr. Andy Yen, Founder & CEO, [ProtonMail](#)
Detlef Schmuck, CEO, [TeamDrive](#)
István Lám, CEO, [Tresorit](#)
Arne Moehle, CEO, [Tutanota](#)
Morten Brøgger, CEO, [Wire](#)

¹ Amendment 140 in the European Parliament's report on the ePrivacy Regulation, available here:
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0324+0+DOC+PDF+V0//EN>