

Secure services express their support for the ePrivacy Regulation

6 June 2018 – As discussions are ongoing on the draft ePrivacy Regulation, privacy-focused online services ArmorText, CryptTalk, Lavabit, Protonmail, TeamDrive, Tresorit, Tutanota and Wire highlight the indispensable role end-to-end encryption plays in protecting individuals' data online and in increasing trust in the security of digital services.

The EU is currently working on updating the legal framework that governs the privacy of electronic communications with the aim of reinforcing trust and security in the Digital Single Market. The European Parliament, in its [report](#) adopted in October last year, included much-needed provisions supporting the use of end-to-end encryption and against backdoors. Meanwhile, Member States in the Council have not managed to find a compromise so far. This has significantly slowed down the process and the adoption of the Regulation which was originally foreseen for 25 May together with the GDPR.

In an [open letter to Ministers](#), who will discuss the draft ePrivacy regulation during the Telecommunications Council on Friday 08 June, privacy-focused online services express their support for the draft and urge ministers to add provisions that require a privacy by design and by default approach to software development.

It's time to reinforce trust online

“With the proliferation of data breaches and misuses, such as the recent Cambridge Analytica scandal, the majority of people do not 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” – the letter reads.

The ePrivacy regulation is an opportunity

The letter's signatories also believe that “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.”

Encryption plays an indispensable role in protecting individuals' data online

Finally, the letter also highlights “the indispensable role end-to-end encryption plays in protecting individuals' data online and in increasing their trust in the security of digital services.”

Not all encryption is created equal: encryption keys should be stored separately and data should be encrypted on the client side before being uploaded to the cloud. Unlike in-transit and at-rest encryption, end-to-end encrypted services store encryption keys at the client side. This guarantees that the encrypted data is never readable for the service provider. In this regard, it is also important to stress that no one, not even governments should have access to the encrypted data. Backdoors violate end user privacy and undermine the world's overall cybersecurity.



About CryptTalk and Arenim Technologies AB

[CryptTalk](#) is an enterprise grade, subscription based service that allows its users to make totally secure calls and conference calls on their mobiles, as well as send secure instant messages. CryptTalk operates in the B2B sphere and provides a unique white labelling solution as well, including customization of the client application. CryptTalk uses Best Practice cryptography that has been through several rounds of third-party independent testing and security reviews, including by the NCC Group (www.nccgroup.trust), this past January. Arenim Technologies, CryptTalk's parent, is Swedish based and is subject to that country's strict privacy and data protection laws.

About Lavabit

[Lavabit](#) is a pioneer in email security and founded on the principle that everyone has the innate right to private and secure communication. The company has never wavered from that mission. Lavabit's revolutionary Dark Internet Mail Environment (DIME) and encrypted Magma server technology provides automatic, transparent, and secure end-to-end email by encrypting every facet of the communication: the body, metadata, and the transport layer to offer customers the highest level of security available.

About ProtonMail

[ProtonMail](#) is the world's largest secure email company, providing encrypted email solutions to governments, enterprises, and consumers around the world. ProtonMail is also the preferred method of communication for many journalists and activists throughout the world. The company was founded in 2013 by scientists who met at CERN and MIT and were drawn together by a shared vision of a more secure and private Internet.

About TeamDrive

[TeamDrive](#) is a German software manufacturer that has specialized in creating solutions for secure collaborative work over the Internet or on premise. TeamDrive provides enterprises with a secure, redundant infrastructure for cloud computing business based on a unique zero knowledge architecture. High flexibility and availability increases work efficiency for corporate customers by allowing them to focus on their core business. Consistent end-to-end encryption represents the core of the high TeamDrive security for over 10 Years.

About Tresorit

[Tresorit](#) is the cloud encryption company providing secure yet user-friendly file sync & sharing for businesses. Tresorit's zero knowledge, end-to-end encryption protects user files from data breaches and government surveillance alike, and enables organizations to work and collaborate safely in the cloud.

About Tutanota

[Tutanota](#) is the world's first end-to-end encrypted email service that encrypts the entire mailbox. Started before the Snowden leaks in 2011, Tutanota now has millions of users. With its unique open source technology Tutanota fights for privacy and freedom of speech online, allowing everybody including NGOs, journalists and activists to send encrypted emails on desktop and mobile. In addition, Tutanota's affordable business version enables companies and organisations of all sizes to easily secure their email communication.

About Wire

[Wire](#) is an end-to-end encrypted, open source communications platform. Based in Europe, it helps people and businesses text, voice and video call, share files while protecting their privacy. Wire works on all major platforms.