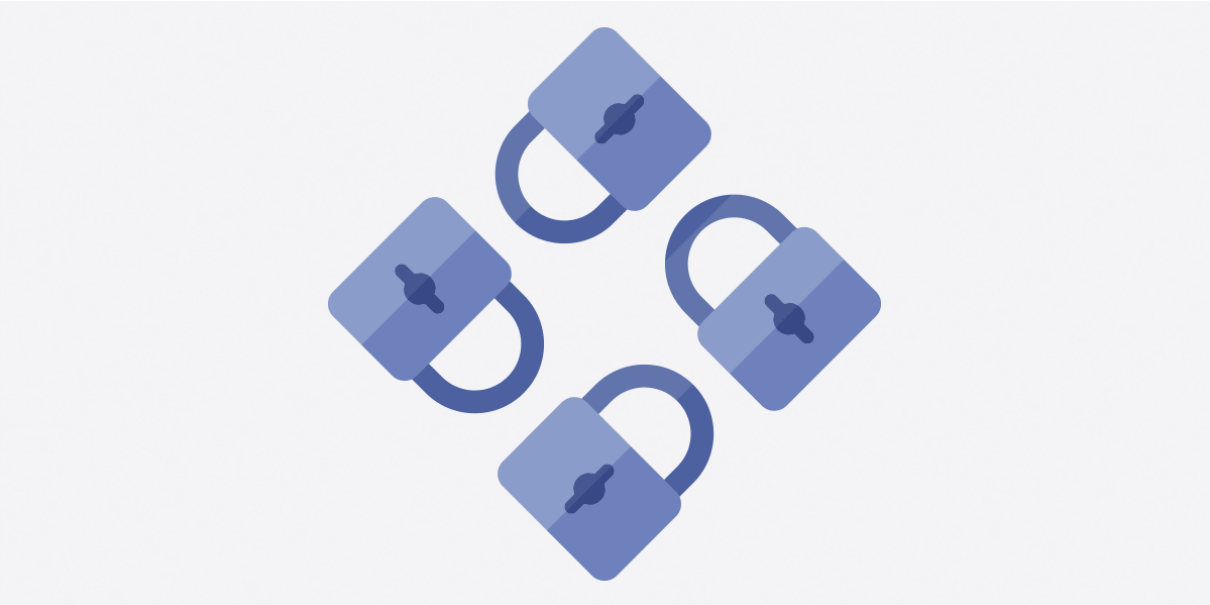
EU citizens' rights are under threat from anti-encryption proposals

Posted on January 28, 2021 by Proton Team



In December 2020, The Council of the European Union released a five-page resolution that called for the EU to pass new rules to govern the use of end-to-end encryption in Europe. We strongly oppose this resolution because it foreshadows an attack on encryption.

We were not the only European-based end-to-end encrypted service that was alarmed by the EU's sudden shift against privacy. Along with Threema, Tresorit, and Tutanota, we are sharing the following joint statement:

ProtonMail, Threema, Tresorit, Tutanota, January 28, 2021 — On Privacy Day, European end-to-end encrypted services ProtonMail, Threema, Tresorit, and Tutanota are calling on EU policymakers to rethink proposals made in December's Council Resolution on Encryption.

The Council's stated aim of "security through encryption and security despite encryption" — and the backdoors to encryption that this would require — will threaten the basic rights of millions of Europeans and undermine a global shift towards adopting end-to-end encryption. In response, these four leading European technology companies reject any attempts to use legal instruments to violate citizens' privacy and stand up to protect the rights of people and businesses choosing end-to-end encryption.

While it's not explicitly stated in the resolution, it's widely understood that the proposal seeks to allow law enforcement access to encrypted platforms via backdoors. However, the resolution

makes a fundamental misunderstanding: encryption is an absolute. Data is either encrypted or it isn't; users have privacy, or they don't. The desire to give law enforcement more tools to fight crime is obviously understandable. But the proposals are the digital equivalent of giving law enforcement a key to every citizen's home and might begin a slippery slope towards greater violations of personal privacy.

Last year's unprecedented shift to remote work saw tens of millions of individuals and businesses turning to technologies like end-to-end encryption to ensure their digital security and privacy. More recently, after more people became aware of WhatsApp sharing data with Facebook, users are switching to privacy-first, end-to-end encrypted services in record numbers. People around the world are taking back control of their privacy, and often it's European companies helping them do it. It seems illogical that policymakers in the EU would now push for laws that fly in the face of public opinion and undermine a growing European technology sector.

The Resolution has effectively given the European Commission the go ahead to start preparing concrete proposals over the coming months. But, as ProtonMail, Threema, Tresorit, and Tutanota point out, the Commission should remember that, from a technological point of view, it is impossible to provide any kind of access to end-to-end encrypted content, even targeted access in a lawful process, without critically weakening the whole system.

"This is not the first time we've seen anti-encryption rhetoric emanating from some parts of Europe, and I doubt it will be the last. But that does not mean we should be complacent," said Andy Yen, CEO and Founder of ProtonMail, the Swiss end-to-end encrypted email service. "Put simply, the resolution is no different from the previous proposals which generated a wide backlash from privacy-conscious companies, civil society members, experts, and MEPs. The difference this time is that the Council has taken a more subtle approach and avoided explicitly using words like 'ban' or 'backdoor.' But make no mistake, this is the intention. It's important that steps are taken now to prevent these proposals going too far and keep European's rights to privacy intact."

"Companies rely on end-to-end encryption for protecting their trade secrets and confidential information. Citizens use apps that follow the zero-knowledge design goal to communicate freely without being tracked and monetized and to exercise their statutory right to privacy. Young European companies are now at the forefront of this revolution in technology and data protection. Experience shows that anything that weakens these achievements can and will be abused by third parties and criminals alike, thus endangering the security of all of us. With the abundance of open-source alternatives, users would simply switch to those applications if they knew a service was compromised," Martin Blatter, CEO of Threema, the end-to-end encrypted instant messaging application, said. "Forcing European vendors to bypass or deliberately weaken end-to-end encryption would not only destroy the European IT startup economy, it would also fail to provide even one bit of additional security. Joining the ranks of the most notorious surveillance states in this world, Europe would recklessly abandon its unique competitive advantage and become a privacy wasteland," he added.

"This resolution would seriously undermine the increasing trust individuals and businesses place in end-to-end encrypted services and threaten the security of users who simply wish to share information securely or leverage end-to-end encryption as part of data protection compliance.

We find this resolution especially alarming given the EU's previously progressive views on data protection. The General Data Protection Regulation (GDPR), the EU's globally recognized model for data protection legislation, explicitly advocates for strong encryption as a fundamental technology to ensure citizens' privacy. These new proposals are irreconcilable with the EU's current stance on data privacy: the current and proposed approaches are at complete odds with each other, as it is impossible to guarantee the integrity of encryption while providing any kind of targeted access to the encrypted data," Istvan Lam, Co-founder and CEO at Tresorit, the end-to-end encrypted file sync & sharing service, said.

"Encryption is the backbone of the internet. Every EU citizen needs encryption to keep their data safe on the web and to protect themselves from malicious attackers. With the latest attempt to backdoor encryption, politicians want an easier way to prevent crimes such as terrorist attacks while disregarding an entire range of other crimes that encryption protects us from. End-to-end encryption protects our data and communication against eavesdroppers such as hackers, (foreign) governments, and terrorists. By demanding encryption backdoors, politicians are not asking us to choose between security and privacy. They are asking us to choose no security," said Arne Möhle, Co-Founder at Tutanota, the German end-to-end encrypted email provider.

As the recent scandal of WhatsApp's privacy policy changes demonstrates, even if a service uses end-to-end encryption, user data can still be misused. European service providers ProtonMail, Threema, Tresorit, and Tutanota are committed to protecting their users' data with transparent privacy policies beyond securing communications with end-to-end encryption.