Mailfence Nextcloud ProtonMail

Tutanota
mail. done. right. matomo

26 November 2019

Dear Members of the LIBE Committee,

This week, you will examine Rapporteur Birgit Sippel's draft report on cross-border access to data for law enforcement ("e-evidence"). The undersigned European companies and start-ups urge you to support the many good proposals made by Rapporteur Sippel and to consider some key improvements to the file.

WHO WE ARE

As part of the flourishing European privacy tech industry, we provide highly secure data hosting, email, messaging and collaboration platforms built in Europe and for Europe. The privacy tech industry helps the EU, its businesses and citizens to strengthen their digital sovereignty and become more independent from the Big Data behemoths of Silicon Valley. We build software and online services with the needs of real businesses and people in mind, rather than for creepy advertisement and data collection.

THE PROBLEM

The Commission's e-evidence proposal threatens the competitive advantage European tech businesses have over their American counterparts by undermining the protections we can provide to our customers. It breaks with the long-standing rule that only trusted national judicial authorities can order companies to hand over customer data for criminal investigations. Instead, the Commission's e-evidence proposal would allow any foreign law enforcement agency from across the EU to force us to hand out customer data without our own authorities double-checking the foreign order.

Different from American Big Tech firms, European privacy tech companies lack the resources to verify the legality of each foreign order. Because of the way the e-evidence proposal is phrased, we would not even be able to properly authenticate foreign authorities to ensure that we are not replying to a malicious actor – let alone object to an order if we found it to be unwarranted.

HOW TO FIX IT

The Rapporteur's draft report contains a number of crucial improvements that deserve support:

- 👍 It suggests to involve national judicial authorities whenever foreign data requests come in (amendments 127, 141, 142, 161);
- 👍 It fixes the Commission's failed attempt to define workable data categories (amendments 90-97); and
- 👍 It enables online service providers such as ourselves to inform our customers about foreign data requests having taken place as long as that does not obstruct an ongoing investigation (amendments 163 and 164).

We strongly encourage you to support the above-mentioned amendments. In addition, the following provisions should be improved:

👎 The reimbursement of costs incurred from data access requests by the issuing authority should be mandatory (as proposed by MEP Sippel's amendment 168) but the reimbursed amount should also be proportionate to the amount of data requested. This would help preventing fishing campaigns without suspicion where a law enforcement agency demands large amounts of data in the hope of finding unrelated evidence.

👎 The draft report should mandate a secure way of authentication and of exchanging information between companies and law enforcement agencies. Currently, too often tech companies receive requests for data via fax machine or unsecured emails, putting the data that is transmitted in both directions at risk. It is particularly crucial for companies to be able to authenticate with absolute certainty the foreign authority they are communicating with in order to avoid the leakage of customer data to malicious actors.

We stand ready to support your work in improving the e-evidence proposal and provide clear safeguards for European privacy tech companies and our users. We thank you for your consideration and remain at your full disposal to respond to any question you may have.

With kind regards,

Mailfence is one of the world's leading secure email services operated by ContactOffice Group sa in Belgium. Its end-to-end encrypted email solution is integrated into a suite with numerous features; Mailfence Contacts, Mailfence Docs, Mailfence Calendar, and Mailfence Groups. Mailfence is considered as an ideal solutions for anybody wanting to de-Google.

Matomo is an all-in-one premium web analytics platform designed by InnoCraft Ltd. to give you the most conclusive insights with our complete range of features. With Matomo, the philosophy around data ownership is simple: You own your data, no one else. Today Matomo is one of the most trusted names in analytics, one of the market leaders on the EU market and currently used on over 1.4 million websites in over 190 countries.

Nextcloud GmbH in Germany offers the industry-leading, on-premises content collaboration platform Nextcloud. Our technology combines the convenience and ease of use of consumer-grade solutions like Dropbox and Google Drive with the security, privacy and control business needs.

ProtonMail is the world's largest provider of secure email. The company offers users end-to-end encrypted email as well as VPN services and has received EU funding via the Horizon 2020 programme. ProtonMail is used by journalists, activists, doctors, lawyers, businesses, and ordinary citizens who want email that is both safer and more private. ProtonMail is email as it should be — private and secure.

Tutanota is an end-to-end encrypted mail service provided by Tutao GmbH in Germany. Tutanota started before the Snowden leaks in 2011 and has now millions of users. With its unique open source technology, Tutanota's affordable business version enables companies and organisations of all sizes to easily secure their email communication.