The myth of data security, data protection & privacy

Description

Wer einmal lügt, dem glaubt man nicht, und wenn er auch die Wahrheit spricht.
Whoever lies once is not believed, even if he speaks the truth.

In order to identify a teenager who is a climate-activist, Proton handed over data to the government (under “terrorist law”).

https://cognitive-liberty.online/wp-content/uploads/The-Myth-of-Data-Internet-Privacy-.mp4

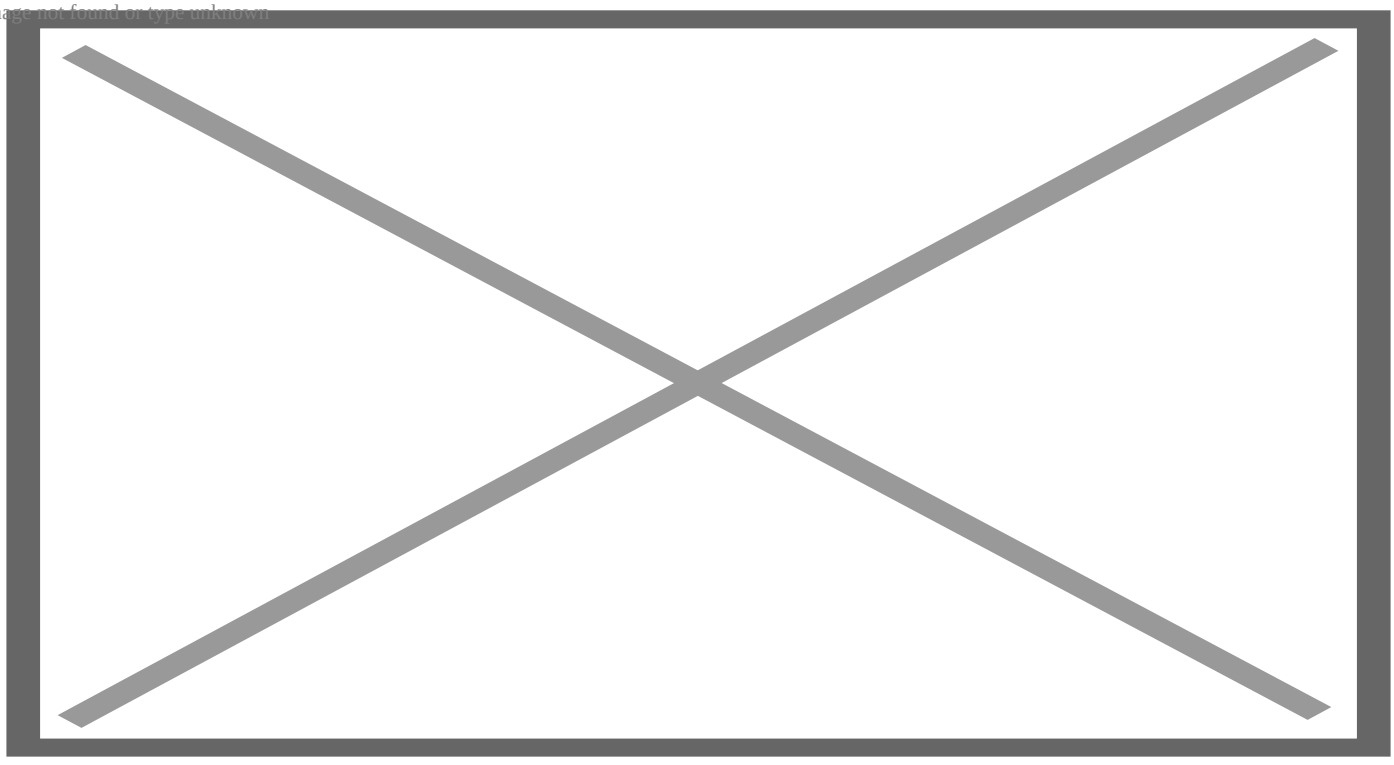
[icon name=”file” style=”regular” class=”” unprefixed_class=””]

- paris-luttes.info/recit-policier-de-sainte-marthe-15258?lang=fr

The article above, which claims that Proton passed on the IP address of the “activist”, was posted on Twitter by someone. (ProtonMail has explicitly stated in its privacy policy that it does not log IP addresses.)

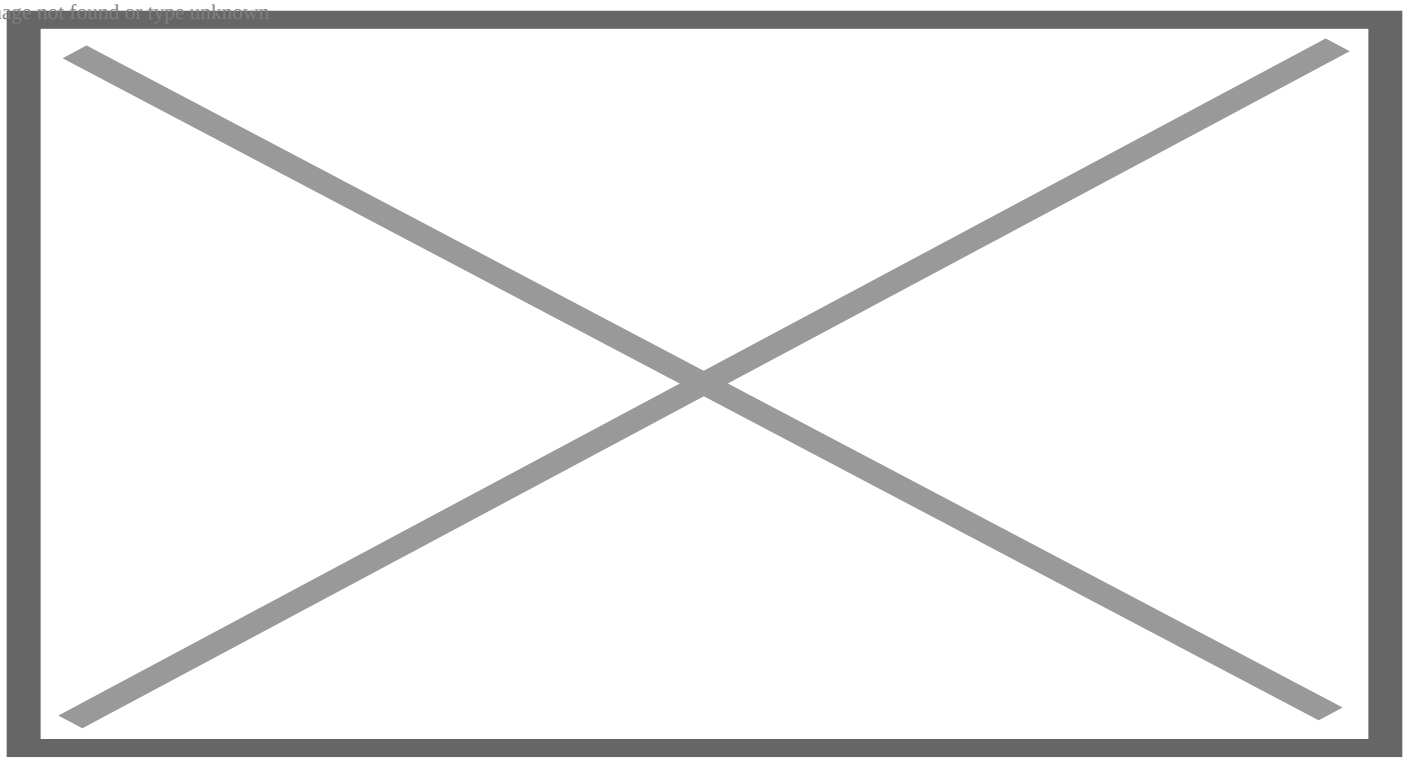
Proton’s CEO responded to the tweet:

Image not found or type unknown



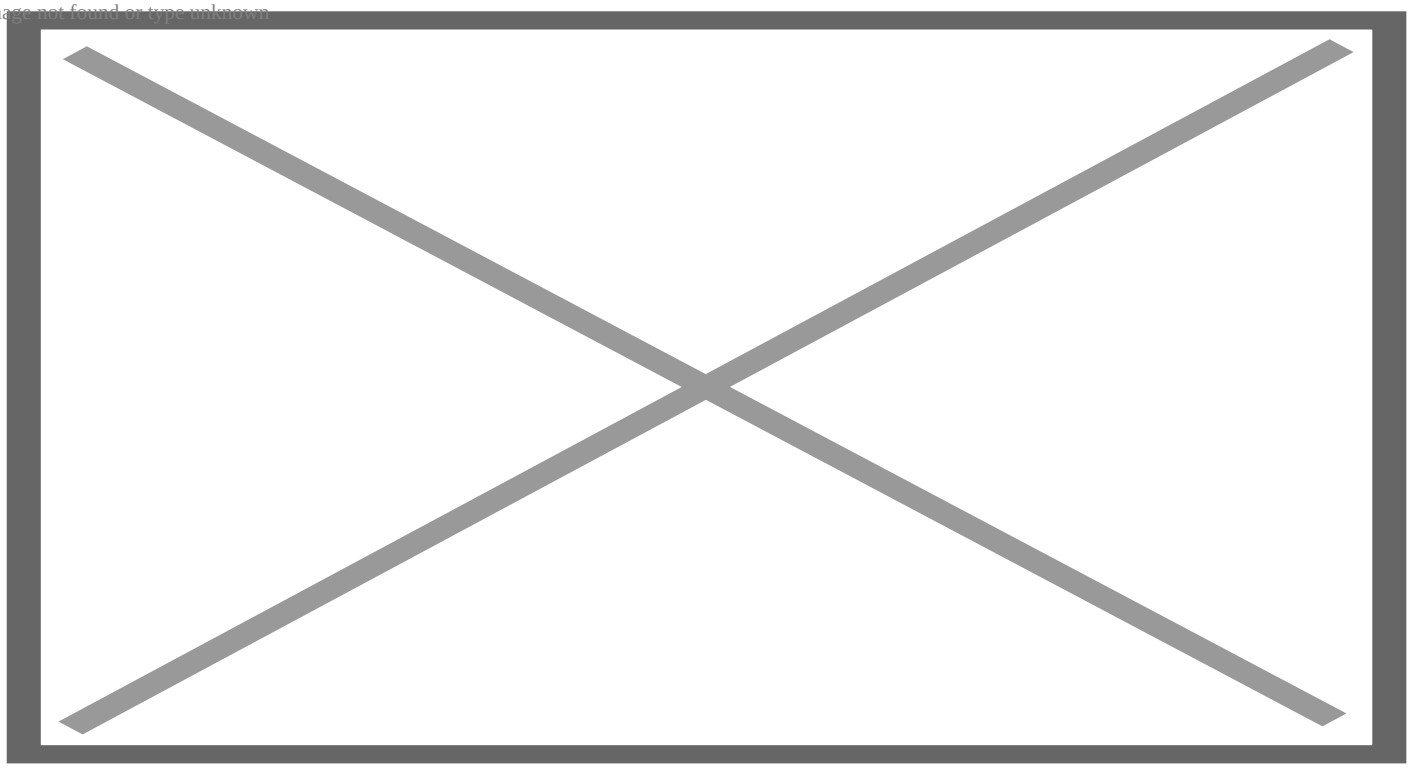
After the case was denied by Protons CEO someone posted the actual police report which clearly shows what was going on:

Image not found or type unknown



Then the CEO admitted:

Image not found or type unknown



Proton now changed its IP-log statement: arstechnica.com/information-technology/2021/09/privacy-focused-protonmail-provided-a-users-ip-address-to-authorities/

Wikipeadia states:
en.wikipedia.org/wiki/Proton_Mail (accessed 24.11.2023)

Due to the encryption utilized, Proton Mail is unable to hand over the contents of encrypted emails under any circumstances, but according to Proton's privacy policy, Proton Mail can be legally compelled to log IP addresses as part of a Swiss criminal investigation.[64] For this reason, the company strongly suggests that users who need to hide their identity from the Swiss government use their Tor hidden service/onion site. I

Kobeissi, N.. (2018). An Analysis of the ProtonMail Cryptographic Architecture. Cryptology EPrint Archive

Show/hide publication abstract

"ProtonMail is an online email service that claims to oer end-to-end encryption such that even [protonmail] cannot read and decrypt [user] emails. the service, based in switzerland, oers email access via webmail and smartphone applications to over ve million users as of november 2018. in this work, we provide the rst independent analysis of pro-tonmail's cryptographic architecture. we nd that for the majority of protonmail users, no end-to-end encryption guarantees have ever been provided by the protonmail service and that the zero-knowledge password proofs are negated by the service itself. we also nd and document weaknesses in protonmail's encrypt-to-outside feature. we justify our ndings against well-dened security goals and conclude with recommendations ."
Saxena, K., Rajdev, D., Bhatia, D., & Bahl, M.. (2021). ProtonMail: Advance Encryption and Security. In Proceedings – International Conference on Communication, Information and Computing Technology, ICCICT 2021

Plain numerical DOI: 10.1109/ICCICT50803.2021.9510041
DOI URL
directSciHub download

Show/hide publication abstract

"The objective of the paper was to reinforce security and to make privacy a priority in mailing services. there has been an excellent effort over a few decades to enhance the security of emails. protonmail has made an enormous breakthrough in the security field by using encryption as a base to reinforce the user's data privacy and digital wellbeing. the security constraints prevent protonmail itself from deciphering the messages. protonmail has implemented various algorithms like ssl, tls, tor, and open pgp to upgrade privacy. protonmail helps the field of information technology as it provides a secure e-mail experience with zero data sharing, which other mailing platforms cannot ensure. an analytical comparison was conducted to demonstrate how protonmail eradicates the vulnerabilities that other mailing services allow. the results demonstrated that the algorithms effectively prevent data breaches and are protected with the keys provided. the scope for threat significantly decreases and reflects on how it is an ideal platform to adopt in the coming future to seize possibilities of misconduct."

Hur, U., Park, M., & Kim, J.. (2022). A reused key attack on an encrypted mobile app database: Case study on KakaoTalk and ProtonMail. Journal of Information Security and Applications

Plain numerical DOI: 10.1016/j.jisa.2022.103181
DOI URL
directSciHub download

Show/hide publication abstract

“Many mobile apps use encryption to protect user data. therefore, research on the use of encrypted data in forensic investigations is warranted. when encrypting data, developers can incorporate data such as user information and passwords during the encryption key generation process. currently, encryption keys can be protected by hardware security modules such as keystore and keychain using an os-provided api. hardware security modules use a built-in random number generator to create random keys and securely store them. as a result, it is practically impossible to decrypt data that have been encrypted using a hardware security module. however, cryptographic algorithm misuse, regardless of whether encryption keys are acquired, present an opportunity for data acquisition. in this paper, we show that a reused key attack that exploits a vulnerability caused by encryption scheme misuse can be used against a secure email service, protonmail, and korea’s representative instant messenger kakaotalk.”
See also:
Silva, Gioia da (August 4, 2021). “”If you say the word compulsory vaccination again, I’ll knock your and your wife’s teeth out”: The Swiss service Proton Mail is repeatedly misused for threats”. Neue Zürcher Zeitung. Retrieved September 10, 2021.

“Important clarifications regarding arrest of climate activist”. proton.me. September 6, 2021. Retrieved September 10, 2021.

Category

1. General

Date Created
23. November 2023
Author
web45