CEPIS
Council of European Professional Informatics Societies

CEPIS against total surveillance of digital communications in the EU

Position statement

The European Commission plans to oblige the communication services providers (e-mail, messaging, video conferencing, etc.) to monitor all content, even if it is encrypted; the regulation is pre-announced for December 1, 2021 [1]. CEPIS firmly rejects this plan.

The Commission regards monitoring (for detecting and reporting) as an important tool in the fight against child sexual abuse and child pornography. While the fight against child pornography may ask for new methods, the Commission seems to accept the undermining of the principle of digital communication confidentiality. CEPIS urges the European Commission, the European Parliament and the governments of the EU member states to prevent this serious and far-reaching violation of fundamental rights. The European Parliament, in particular, is called upon to take immediate and decisive action against the Commission's plans that are damaging to our community.

Background

The Directive on privacy and electronic communications (2002/58/EC) for the processing of personal data and the protection of privacy on the Internet has existed since July 1, 2002. On July 6, 2021, the EU Parliament approved a 3-year relaxation of this Directive in order to combat child abuse on the Internet and legalized the scanning of unencrypted content - previously illegally carried out by a number of providers. In the opinion of CEPIS, even this relaxation of the Directive violates the Charter of Fundamental Rights of the European Union, in particular Article 7 (Respect for private and family life), Article 8 (Protection of personal data) and Article 11 (Freedom of expression and information): these basically guarantee confidential communication. This is in line with the assessment by the former ECJ judge Ninon Colneric [2].

Nevertheless, the Commission would like to transform the temporary regulation into permanent and extend it to encrypted content. The Commission launched an open public consultation in this regard [3], and a clear majority of the respondents spoke out against this scanning, especially against breaking the encryption [4]. Breaking the encryption would result in confidential communication no longer being guaranteed, and moreover, far-reaching attacks on IT systems become possible. CEPIS had already earlier pointed out the essential importance of cryptography to protect the confidentiality of communication [5].
Recently the term "Client-Side Scanning" (CSS) was introduced that may give the impression that scanning on users' devices would be less risky for the privacy of communication than earlier proposals. However, an extensive analysis by leading experts in the field [6] clearly shows the opposite: "The introduction of CSS would be much more privacy invasive than previous proposals to weaken encryption. Rather than reading the content of encrypted communications, CSS gives law enforcement the ability to remotely search not just communications, but information stored on user devices."

There is no question that child abuse needs to be combated. However, this fight must be waged in the real world, above all, by taking children seriously, investigating suspected cases more quickly and strengthening the responsible authorities. It cannot be that automated procedures are used to combat crime, which has the consequence that IT systems' security is impaired and fundamental principles of our democracy are abandoned.

References

[1] OJ 2387 - Liste des points prévus à l'ordre du jour des prochaines réunions de la Commission, https://ec.europa.eu/transparency/documents-register/detail?ref=SEC(2021)2387&lang=en.

[2] Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament, Prof. Dr. Ninon Colneric, March 2021, https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf.
[3] EU Open Public Consultation on "Fighting child sexual abuse: detection, removal and reporting of illegal content online", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Child-sexual-abuse-online-detection-removal-and-reporting-/public-consultation_en.
[4] Contribution file of the Survey related to the EU Open Public Consultation on "Fighting child sexual abuse: detection, removal and reporting of illegal content online", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online/public-consultation_en
[5] CEPIS statement "Right to Encryption Instead of a Master Key for Encrypted Communication", https://cepis.org/app/uploads/2020/11/Right-to-encryption-instead-of-a-master-key-for-chat-communication-CEPIS-LSI-SIN.pdf.
[6] Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso: "Bugs in our Pockets: The Risks of Client-Side Scanning", http://arxiv-export-lb.library.cornell.edu/abs/2110.07450