CEPIS
Council of European Professional
Informatics Societies

Brussels, March 2022

Open letter

Concerning: A right to secure communication and effective encryption for Europe

The confidentiality and security of digital communication are essential for our society. Not only does democratic discourse thrive on a free exchange of opinions, but our economy also needs secure communication. Finally, the digitization of our state administration also requires a high level of trust in IT infrastructures. Freedom of information is a valuable asset and is enshrined in Article 11 of the EU Charter of Fundamental Rights.

The European Commission has been considering plans to monitor all communications content, which would contravene these important democratic and economic goals. The Commission has not formally committed itself yet. However, the planned monitoring of all communication content (e.g., chats and e-mails) without a specified reason in order to facilitate the investigation of crime means either the decryption of all encrypted messages by the service providers or the circumvention of end-to-end encryption through automated and mass "client side scanning" (CSS) on the end devices of the users, e.g., on all smartphones. Such CSS is a risky add-on to any communication system [1]. It endangers the human right to liberty and security and thus the acceptance of digitization and, by extension, the trust in the future viability of the European Union. At the same time CSS is a risk for any confidential business communication and endangers the integrity of the device it is put on.

As experts, scientists and professionals in the field of information and communication technologies, we foresee highly problematic side effects of such interventions in our communication systems, especially the introduction of CSS. They lower the IT security level of millions of Internet users and create gateways for cyber criminals. Cybercrime causes over $1 trillion euros in damage to the world economy per year [2]. By deliberately weakening Internet communications, Europe's reputation as a leading location for a secure and data-protection-oriented digital economy is being massively damaged.

Effective encryption of communications and stored data must also become a mandatory standard for public authorities, professional secrecy holders and all communications companies in order to reduce the attack surface of central infrastructures. Current communications systems prove that efficient and user-friendly end-to-end encryption is possible and can be easily integrated. For example, the EU Commission also recommends the use of end-to-end encrypted communication to its own employees [3].

The fight against serious crime is an important task for the state, which in individual cases also legitimizes interventions in the freedom of communication. However, it does not justify undermining the entire digitization of Europe's state, economy and civil society through unprovoked and mass surveillance of chat content, for example. Interventions that are necessary in individual cases may only be carried out in a targeted manner and on an ad hoc basis.

Therefore, as we strongly believe in the right to strong and effective encryption for all EU citizens, companies and institutions, we call on the European legislative bodies

not to undermine it. In addition, providers of communications services must be obliged to provide EU citizens with a secure ICT infrastructure. We also call for an end to all activities that weaken and circumvent encryption, as they expose the security of all EU citizens and our economy to enormous risk.

Yours sincerely,

Byron Nicolaides
President

[1] 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 (2021) "Bugs in our Pockets: The Risks of Client-Side Scanning" *https://arxiv.org/pdf/2110.07450.pdf*
[2] Zhanna Malekos Smith, Eugenia Lostri, James A. Lewis (2020) "The Hidden Costs of Cybercrime" *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf*
[3] *https://joinup.ec.europa.eu/node/702550*

The Council of European Professional Informatics Societies (CEPIS) is the representative body of national informatics associations throughout greater Europe. Established in 1989 by 9 European informatics societies, CEPIS has since grown to represent IT professionals in 28 countries. CEPIS aspires to promote best practice for IT professionals and users throughout Europe by promoting high standards to further mature and promote IT professionalism, building gender balance in IT industry and inspire more young people to pursue IT-related education and careers, advocating for a digitally competent and skilled general workforce in support of employability and higher productivity and for the socially responsible adoption, secure, ethical, inclusive and environmentally friendly application of IT in Europe.