To:
Henna Virkkunen
Executive Vice President for Tech Sovereignty, Security and Democracy
European Commission

Magnus Brunner
Commission for Internal Affairs and Migration
European Commission

The undersigned civil society organizations, companies, and cybersecurity experts, including members of the Global Encryption Coalition,[1] urgently share their concerns regarding aspects of the recently announced European Internal Security Strategy (Protect EU)[2] due to its potential impact on end-to-end encryption.

On April 1st the European Commission shared its new five-year strategy, ProtectEU, to address elevated security concerns for the European Union in the midst of a rapidly evolving geopolitical landscape. Included in the strategy is the European Commission's intent to develop a "*Technology Roadmap on encryption, to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner*."

While we recognise the importance of elevating security efforts during moments of increased geopolitical instability, we are concerned by the framing of the technology roadmap. Government agencies elsewhere in the world[3] actively encourage more usage of end-to-end encryption, not less, to protect the integrity of cyberspace against increased security threats. Strong encryption, including end-to-end encryption, is a key cybersecurity tool that protects the European Union against cyberattacks, hybrid threats, espionage, and attacks on critical infrastructure.

The European Commission itself has acknowledged the need to step up efforts and investment to protect the integrity of cyberspace as reflected in the Revised Directive on Security of Network and Information (NIS2).[4] The Revised Directive introduces obligations for platforms and service providers to implement appropriate and proportionate cybersecurity risk-management measures, including encryption, to protect the confidentiality, integrity, and availability of their systems and services. The European Data Protection Supervisor echoes this message, stating that "restrictions on encryption pose significant risks to the economy and society in general."[5]

Yet, against this backdrop, we are deeply concerned by the Commission's continued focus on identifying ways to weaken or circumvent encryption. This undermines its own security objectives under the ProtectEU strategy, which emphasises the importance of resilience and

[1] https://www.globalencryption.org/
[2] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920
[3] https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf
[4] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[5] https://www.edps.europa.eu/data-protection/our-work/subjects/encryption_en

preparedness in the face of more sophisticated cyber threats. Undermining encryption weakens the very foundation of secure communications and systems, leaving individuals, businesses, and public institutions more vulnerable to attacks.

Past[6] and ongoing[7] efforts in the European Union to grant law enforcement access to encrypted data have primarily focused on client-side scanning, a technology that circumvents encryption by scanning user devices before the encryption mechanism starts. Scanning not only violates the promises of end-to-end encryption but also creates vulnerabilities that could be exploited by criminals and hostile state actors.[8] There is widespread consensus among technical experts that encryption circumvention tools create new risks that threaten national security, concerns recently echoed by member state authorities in Sweden[9] and the Netherlands[10]. The European Court of Human Rights and European Union Agency for Fundamental Rights have emphasized that statutory requirements that “weaken the encryption mechanism for all users” would be disproportionate under the Charter of the Fundamental Rights of the EU.[11]

The technology roadmap announced by the European Commission mirrors efforts taken by other governments to identify encryption circumvention tools, such as the UK’s “Safety Tech Challenge,”[12] which pledged funding for proof-of-concept tools for preventing and detecting child sexual abuse material in end-to-end encrypted environments. In the case of UK efforts, the selected independent third party reviewer, REPHRAIN, found that none of the resulting proofs of concept fulfilled their evaluation framework for human rights, security, accountability, and other criteria.[13] We believe that any similar EU approach would produce the same results, wasting valuable resources.

We call on the European Commission to:

- Acknowledge that strong encryption is not an obstacle to EU security but a prerequisite for it, positioning the widespread use of end-to-end encryption as a tool for advancing cybersecurity and EU’s resilience in the current geopolitical context.

[6] https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/

[7] https://www.globalencryption.org/2024/09/gec-steering-committee-statement-on-9-september-text-of-the-european-csa-regulation/

[8] https://datatracker.ietf.org/doc/statement-iab-statement-on-encryption-and-mandatory-client-side-scanning-of-content/

[9] https://regeringen.se/contentassets/e22f777eb1964c258c5d9a21adb6a355/forsvarsmakten.pdf

[10] https://gegevensmagazijn.tweedekamer.nl/SyncFeed/2.0/Resources/6b0e965e-76c0-489a-a253-1cb81d1bace8

[11] https://fra.europa.eu/sites/default/files/fra_uploads/ecthr-fra-2025-mass-surveillance_en.pdf

[12] https://apply-for-innovation-funding.service.gov.uk/competition/1457/overview/68f93702-cc80-469d-9056-b0f4fdc0d394

[13] https://www.rephrain.ac.uk/wp-content/uploads/Safety-Tech-Challenge-Fund-evaluation-framework-report-1.pdf

- Reframe the Technology Roadmap on Encryption, highlighting the benefits of encryption and identifying areas for increased usage to strengthen cyber defense in alignment with the European Union's existing security strategies.
- Develop the Technology Roadmap by drawing on a wide range of perspectives, not only those of law enforcement, but also cybersecurity experts, civil society, digital rights advocates and private companies. Any future roadmap that aspires to be credible and balanced must consider the feasibility of any potential technological capabilities and their societal, technical, and legal impact.

Please direct your response to Callum Voge, Director of Governmental Affairs and Advocacy at the Internet Society (voge@isoc.org), and to Silvia Lorenzo Perez, Programme Director of the Security, Surveillance and Human Rights Programme at the Centre for Democracy & Technology — Europe (sperez@cdt.org).

Sincerely,

Organizational Signatories

3 Steps Data
ACT | The App Association
Africa Media and Information Technology Initiative (AfriMITI)
Africa Rural Internet and STEM Initiative (AFRISTEMI)
Alternatif Bilisim
AMS-IX
Big Brother Watch
Bits of Freedom
Blacknight
Blockchain Association
Center for the Study of Organized Hate (CSOH)
Centre for Democracy and Technology Europe
Centro Latinoamericano de Investigaciones Sobre Internet
Chaos Computer Club
Comunitatea Internet Association
Cybersecurity Advisors Network (CyAN)
Danes je nov dan, Inštitut za druga vprašanja
Datenpunks
Digitale Gesellschaft
Digital Rights Ireland
Digital Society
Državljan D / Citizen D
eco - Association of the Internet Industry
Electronic Frontier Finland - Effi ry
Electronic Frontier Foundation

Electronic Frontier Norway
Element
Emerald Onion
Epicenter.works
EuroISPA - The European Association of Internet Services Providers
European Digital Rights (EDRi)
FiCom ry
Freedom of the Press Foundation
Global Partners Digital
Hermes Center
Internet Architecture Board
Internet Australia
Internet Society
Internet Society Brazil Chapter
Internet Society Catalan Chapter (ISOC-CAT)
Internet Society Mali Chapter
Internet Society Nepal Chapter
Internet Society Portugal Chapter
IT-Pol Denmark
Japan Network Information Center
JCA-NET
Kleindatenverein
LGBT Tech
Matrix.org Foundation
Mozilla
OpenMedia
Phoenix R&D GmbH
Politiscope
Privacy & Access Council of Canada
PrivID, Inc
Proton
SABOA foundation
SecureCrypt
SkypLabs
Statewatch
SUPERRR Lab
Surfshark
Tech for Good Asia
Tuta Mail
Vircos Tecnologia
Vrijschrift.org
Wikimedia Europe
Xnet. Institute for Democratic Digitalisation
X-Lab

Individual Cybersecurity Experts*

Jon Callas, Indiana University
Sofia Celi, Brave
Claudia Diaz, KU Leuven
Donald E. Eastlake 3rd, Independent
Nicola Fabiano, Fabiano Law Firm
Stephen Farrell, Trinity College Dublin
Masayuki Hatta, Surugadai University
Mallory Knodel, New York University
Sascha Meinrath, X-Lab
Peter Neumann, Moderator, ACM Risks Forum
Riana Pfefferkorn, Stanford University
Jonathan Rudenberg, Grace
Bruce Schneier,
Adam Shostack, Author of Threat Modeling: Designing for Security
Eugene H. Spafford, Purdue University
Asli Telli, University of Cologne
Peter Thomassen, deSEC
Kenn White
Matthew Wright, Rochester Institute of Technology
Philip Zimmermann, Associate Professor Emeritus in Cybersecurity, Delft University of Technology

*Affiliations are indicated for purposes of identification only