Encryption in the age of surveillance

Background note

States' attempts to control encryption to preserve their surveillance capabilities are not new[1]. However, since the 1990s, methods to circumvent and weaken encryption have diversified. The stakes are also way higher: encryption is nowadays used by many messaging services, and in every sector of society. Encryption serves the interests of every stakeholder in a democracy: it protects people as a vital human rights tool, supports the economy and secures the government in delivering its missions. All of us need the freedom to conduct personal and private conversations online without interference. For human rights defenders, that freedom can be the difference between life and death.

We see three types of threats endangering encryption in the European Union (EU):

Harmful legislation: While purported to address the dissemination of child sexual abuse material (CSAM) online, the European Commission proposed a draft law in 2022 mandating the monitoring of virtually all public and private digital communications, including encrypted ones. Although it does not require the use of a specific technology, this proposal would force private companies to implement surveillance and censorship mechanisms that fundamentally undermine encryption. On top of this, recent leaks have shown that there is an explicit call to ban end-to-end encryption by a number of EU Member States, and a desire to use the CSA Regulation to set a broader precedent for systematic access to encrypted messages.

Criminalisation: In the criminal justice area, the use of encrypted tools is used as a pretext to justify mass and arbitrary surveillance and repression measures. It also legitimises harsher criminal charges and sanctions. Encryption is framed as concrete evidence of the suspects' intention to "hide something" or remain "clandestine". Whether in France or in Greece, this criminalisation of encryption mainly targets activists and human rights defenders. The recent international police operations against communications networks such as EncroChat and SkyECC also showed how encryption has been used to justify government mass hacking, treating all users as suspects and undermining their presumption of innocence and fair trial rights.

Lack of regulatory action: On the contrary, the EU is failing to take proper regulatory steps to promote encryption and protect everyone's rights and online safety. Beside the European Parliament, European institutions have remained largely helpless following the various spyware scandals like Pegasus. Yet, there is a clear need for common rules on governments' surveillance capacities, control over the unregulated market of surveillance technologies and more substantial public investments in vulnerability research and open and free software development.

For press inquiries, reach out to press@edri.org

For any further question regarding the content, reach out to chloe.berthelemy@edri.org

[1] See key escrow initiatives (such as the U.S. Clipper Chip)

Annex: Resources

EDRi, "State access to encrypted data. A digital rights perspective.", 17 October 2022, https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf

CSA Regulation

EDRi network position paper on the "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse" 2022/0155(COD) (CSA Regulation), "A safe internet for all. Upholding private and secure communications", 19 October 2022, https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

See many other EDRi resouces on our dedicated CSAR document pool: https://edri.org/our-work/csa-regulation-document-pool/

Bulk hacking operations

Fair Trials, "EncroChat hack: Fair Trials denounces lack of transparency and oversight, 18 February 2022", https://www.fairtrials.org/articles/news/encrochat-hack-fair-trials-denounces-lack-of-transparency-and-oversight/

Hendrik Mildebrath, "EncroChat's path to Europe's highest courts", EPRS, December 2022, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739268/EPRS_ATA(2022)739268_EN.pdf

Spyware

EDRi, "Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware Draft Recommendation to the Council and the Commission. EDRi comments and recommendations", 21 February 2023, https://edri.org/wp-content/uploads/2023/02/EDRi-Amendments-PEGA-Draft-Recommendations.pdf

Amnesty International, **"**EU: Final vote on spyware inquiry must lead to stronger regulation", 15 June 2023 https://www.amnesty.org/en/latest/news/2023/06/eu-final-vote-on-spyware-inquiry-must-lead-to-stronger-regulation/

Access Now, "No to spyware: media, civil society demand ban on tech used for human rights abuses", 3 May 2023, https://www.accessnow.org/press-release/world-press-freedom-day-no-to-spyware/

European Media Freedom Act (EMFA)

EDRi, "Proposal for a European Media Freedom Act (EMFA): EDRi amendments and recommendations", 20 April 2023, https://edri.org/wp-content/uploads/2023/04/EDRi-Amendments-EMFA-Surveillance.pdf

EDRi and al., **"**Civil society and journalists associations urge the Council to protect journalists against spyware and surveillance in the European Media Freedom Act (EMFA)", 19 June 2023, https://edri.org/wp-content/uploads/2023/04/Open-Letter-Council-Protection-of-Journalists-Against-Spyware-in-EMFA.pdf

EDRi, "LIBE Committee's opinion fails to include a total ban on the use of spyware in the European Media Freedom Act" 20 July 2023 https://edri.org/our-work/eu-parliament-libe-committee-opinion-spyware-ban-european-media-freedom-act/