Global Encryption Coalition Steering Committee Statement on the Dangers of the French "Narcotrafic" Legislation

The Center for Democracy & Technology, Global Partners Digital, the Internet Freedom Foundation, the Internet Society, and Mozilla, constituting the Steering Committee of the Global Encryption Coalition[1], raise grave concerns with the impact that the Article 8 *ter* of the legislation "Sortir la France du piège du narcotrafic," will have on the security and privacy of French citizens, companies, and institutions. Through this legislative proposal, the government aims to tackle a serious societal problem, drug trafficking. Yet the implication of compromising encryption to do so sets a dangerous precedent for security and privacy, while other more effective approaches can be taken.

By forcing companies to undermine end-to-end encryption with encryption backdoors, the legislation will leave France less safe against criminals and foreign adversaries. As France faces the real threat of cyberwarfare, ensuring that French citizens, companies, and institutions have access to end-to-end encrypted communications is more vital than ever. As noted by the Commission nationale de l'informatique et des libertés (CNIL), no provision should be able to be interpreted as prohibiting or weakening encryption.[2] Article 8 *ter* of the "Sortir la France du piège du narcotrafic, must be removed from the legislation in order to protect end-to-end encryption.

Article 8 *ter* forces certain platforms to build encryption backdoors. It requires that they be able to hand over decrypted chat messages of suspected criminals within 72 hours of the request even if it is technically impossible to do so. Encryption backdoors are intentional security flaws and forcing their introduction would put every users' security and privacy at risk, not just in France but also globally. An additional concern is the security of the endpoints, which the bill undermines by enabling law enforcement to engage in hacking of Internet connected devices.

The consensus among global cybersecurity experts could not be clearer: there is no way to provide government access to end-to-end encrypted data without introducing

[1] The Global Encryption Coalition is a group of over 400 organizations, companies and cybersecurity experts that promotes and defends encryption in key countries and multilateral fora where it is under threat. https://www.globalencryption.org/

[2] https://www.contexte.com/actualite/tech/la-cnil-defend-le-chiffrement-que-la-ppl-narcotrafic-veut-remettre-en-question_217681.html

vulnerabilities that put every user's security and privacy at risk.[3] This includes silently adding third-party listeners to encrypted conversations, known as the "ghost proposal."[4]

If passed, the legislation leaves platforms offering end-to-end encrypted services with an impossible choice. They will either need to comply and undermine the security of their services, or they will be forced to leave the French market. In either scenario, the result is less secure and private communications for the French citizens, companies, and institutions who rely on these tools.[5] Over 60% of French Internet users benefit directly from the security and privacy provided by end-to-end encrypted messaging services.[6] Undermining the confidentiality of end-to-end encrypted services would have the most harmful impact on those already at greatest risk: families, domestic violence survivors[7], LGBTQ+ individuals[8], and many more who rely on the safety and privacy provided by end-to-end encrypted services.

International human rights bodies have recognised the importance of end-to-end encryption to protect the right to privacy and to promote the exercise of other rights. This is because being able to communicate safely and securely can be a precondition to being able to communicate and express one's views. In 2022, a joint opinion from the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) noted that "encryption technologies contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation and the growth of the digital economy."[9] The case law of the European Court of Human Rights (ECtHR) recognises the importance of anonymity in "promoting the free flow of ideas and information in an important manner" including by protecting people from reprisals for their exercise of freedom of expression.[10] In February 2024, the ECtHR found that Russia's order issued to Telegram requiring it to disclose "technical information" including encryption keys breached human rights law, as it was not proportionate.[11]

French companies, government services ,and institutions all benefit from end-to-end encryption. A recent study found that "organizations in France encrypt all data types at

---

[3] https://www.cl.cam.ac.uk/archive/rja14/Papers/doormats.pdf

[4] https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/

[5] Recently, UK citizens lost the protection provided by Apple's end-to-end cloud service, after the UK government attempted to force Apple to build an encryption backdoor. https://www.eff.org/deeplinks/2025/02/cornered-uks-demand-encryption-backdoor-apple-turns-its-strongest-security-setting

[6] https://www.statista.com/statistics/1029506/messengers-voip-penetration-france/

[7] https://www.internetsociety.org/wp-content/uploads/2021/05/NNEDV_Survivor_FactSheet-EN.pdf

[8] https://www.lgbttech.org/encryption-privacy-security

[9] https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

[10] Delfi AS v Estonia [2015] EMLR 26, [147] and [149]: https://hudoc.echr.coe.int/eng#{"itemid":["001-155105"]} ↩

[11] Podchasov v Russia [2024] ECHR 134 [79]: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]} ↩

higher rates than global averages."[12] Providing backdoors in one instance can lead to encryption being weakened across the ecosystem of the public and private sector, as well. Particularly for national security professionals and government employees, access to end-to-end encrypted services allows them to safeguard their personal and professional lives. A backdoor would weaken the French messaging app Olvid, which has been certified by the French cybersecurity agency ANSII and officially recommended to French ministers and government officials.[13] Ensuring the security and privacy of government officials is vital for helping prevent extortion or coercion attempts, which could lead to greater national security damage. As "both French diplomatic officials and President Emmanuel Macron have repeatedly accused Russia of engaging in hybrid warfare against France through cyberattacks"[14] and the fallout of the Salt Typhoon hack[15], the reliance by the French government, citizens, and businesses on end-to-end encryption to keep themselves safe and secure has never been greater.

End-to-end encryption is vital to protecting France's interests. Article 8 *ter* of the "Sortir la France du piège du narcotrafic, must be removed from the legislation in order to protect end-to-end encryption.

[12] https://www.entrust.com/company/newsroom/known-threats-drive-encryption-adoption-finds-entrust-2021-france-encryption-trends-study#:~:text=While%2046%%20of%20respondents%20in%20France%20have,global%20average%20of%2050%%20and%20down%20from

[13] https://olvid.io/en/

[14] https://www.politico.eu/article/france-has-trouble-understanding-us-halt-on-cyber-operations-against-russia/

[15] https://cyberscoop.com/salt-typhoon-us-government-jen-easterly-cisa/