

14.03.2025

M. Damien CHAMUSSY

Secretary General
National Assembly of France
126 Rue de l'Université
75355 Paris 07 SP
France

RE: Request by Small Business Technology Developer Community for the Protection of End-to-End Encryption to Support France's Security and Economic Goals

ACT | The App Association is a trade association representing small businesses technology companies from across the European Union (EU). Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. **The App Association writes to strongly encourage the French National Assembly to oppose the potential legislation, referred to as 'Loi Surveillance te Narcotraficotage' that could weaken encryption under the pretext of combating narcotrafficking.**

While we recognize the importance of combating illicit activities, we strongly urge caution against any measures that would undermine the security and integrity of encryption, as such actions pose significant risks to privacy, cybersecurity, and economic competitiveness. The senators amended text provides that communication services are required to introduce access, a 'backdoor', for the benefit of the police and intelligence services, under penalty of heavy sanctions. This would create an unprecedented breach in end-to-end encryption technology, exploitable by both States and malicious actors. Such a measure is extremely dangerous. As many institutions, including the French Cybersecurity Agency ([ANSSI](#)) and the [European Data Protection Committee](#)¹, have repeated, this would weaken the level of protection of all communications and threaten the confidentiality of all the exchanges.

The App Association's small business members both in and outside of France know that, in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorized users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorized users. End-to-end encryption is a primary tool for providing the trust and security of their customers. Attempts by governments, most recently France, to mandate backdoors to encryption algorithms significantly undermines these goals.

¹ 'The new rules should also clearly allow users to use end-to-end encryption (without 'backdoors') to protect their electronic communications. Decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.' Opinion 5/2016 of the European Data Protection Supervisor

The App Association fully supports efforts to combat organized crime and drug trafficking. However, the currently debated Surveillance and Drug Trafficking Law does not accomplish this goal. Its implementation would deeply damage security and trust across the digital economy by creating flaws in algorithms that can be used to compromise data confidentiality, integrity, and access requisites.

It is impossible to reserve security backdoors for just the “good guys.” If a door exists then bad actors can, and will, exploit it. It is fair to assume that other tech firms will be asked to create similar backdoors into encrypted services, further damaging security and trust. France’s demand would set a precedent for other countries and regimes to demand similar access to encrypted private data, further reducing citizens’ privacy and safety.

The damage that would be caused by the implementation of this new law to French and European small businesses innovating and competing across the global digital economy is not hypothetical. As a prime example, government mandates in the 1990s for broadband internet providers to enable law enforcement agencies access to encrypted communications on their networks has directly led recently to the China-backed hacker group Salt Typhoon gaining unprecedented unauthorized access to swaths of sensitive data. While the magnitude of this breach of U.S. telecommunications carrier networks continues to be investigated, at this time it appears that Salt Typhoon’s access was essentially unlimited. This (ongoing) episode is the strongest evidence that mandating unfettered access via backdoors to encrypted devices or data in transit will result in that access being exploited by unintended actors. The Salt Typhoon experience demonstrates that weakening encryption will expose businesses to more frequent breaches, creating an even greater risk for those already marginalized.

With cyber-attacks to critical infrastructure continuing to increase in both frequency and severity, the need for security that end-to-end encryption provides has never been more essential. A mandated weakening of encryption would undermine the acknowledgement in the AINSS 2030 manifesto which states that ‘computer attacks now have the potential to seriously damage our economy, our defense and national security interests and to the very lives of our fellow citizens’².

In compelling a company to covertly compromise the security of its product, the French government would raise serious concerns about the security of products from French firms, including our members who work to grow and create jobs in France, leading to investors and consumers questioning whether their products contain hidden security vulnerabilities mandated by the French government. The precedent the National Assembly would create may also force some of our members to consider withdrawing from the French market to avoid the reputational risks associated with undermining their own product’s security. Lastly, adopting such legislation

²Page 6. <https://cyber.gouv.fr/sites/default/files/document/Manifeste%20de%20l%27ANSSI.pdf>

would not only damage France's standing in global security and innovation policy³ but would also signal a retreat from its leadership role in these areas.

France has the power to protect encryption standards, ensuring they remain strong enough to safeguard our digital infrastructure without creating loopholes that compromise security. Accordingly, we request that the French National Assembly to vote against the proposed law and engage in a revised policy development process to ensure that end-to-end encryption supports French national and economic security. Our community fully commits to participating in such a process, and to more broadly support policies that enhance security and innovation as well as the France's global leadership.

Sincerely,



Mike Sax
Founder and Chairperson

Brian Scarpelli
Senior Global Policy Advisor

Maria Goikoetxea Gomez de Segura
Policy Manager

³ Notably, the European Court of Human Rights (ECtHR) has condemned governments requiring companies to disclose encryption keys as disproportionate measures that breach human rights law. [https://hudoc.echr.coe.int/eng/#{itemid%22:\[%22001-230854%22\]}](https://hudoc.echr.coe.int/eng/#{itemid%22:[%22001-230854%22]}).