Encryption at Risk: Why Weakening Digital Security Endangers Us All

A VPN Trust Initiative (VTI) Paper on Privacy, Security, and Trust in the Digital Age

September 2025

Strong encryption is a cornerstone of digital security. Weakening it immediately compromises citizens' privacy, undermines marginalized communities' ability to communicate safely, erodes cross-border trust, increases compliance uncertainty for businesses, and creates new attack vectors for threat actors.

Around the world, policymakers are advancing measures that would erode encryption in the name of safety. This is a false proposition. Public safety depends on secure technology; there is no safety if the very tools that provide it are weakened.

Goals such as national security, child safety, and law enforcement are very important and VTI members fully support pursuing effective solutions to achieve them—but not at the cost of weakening ***everyone's*** security, especially when the effectiveness of such measures is uncertain.

VTI urges policymakers to avoid measures that erode encryption and put user safety at risk.

1. Introduction

Encryption is used to protect everything from personal privacy and human rights to the integrity of financial systems, government operations, critical infrastructure, and national security. Bringing attention to policymakers and the wider public on the importance of encryption in modern society is crucial when pressures in various jurisdictions are rising.

- The proposed EU Child Sexual Abuse Regulation (often referred to as "Chat Control") would empower authorities to issue detection orders requiring indiscriminate scanning of private communications, including end-to-end encrypted services, while EU's ProtectEU Internal Security Strategy suggests lawful access by design to encrypted data.
- In the UK, under powers in the Investigatory Powers Act 2016, the government issued an order that led Apple, in February 2025, to withdraw its end-to-end encrypted iCloud backups ("Advanced Data Protection") for UK users pending litigation. Policy debates

continue alongside the Online Safety Act, whose controversial scanning provisions are not currently being enforced.

- Recurring legislative efforts in the US such as the EARN IT Act would create liability risks for providers without the capacity to scan for child sexual abuse material, indirectly pressuring services to weaken encryption or adopt invasive scanning.

These proposals often assume that capabilities can be engineered to allow "targeted" access to encrypted data without degrading security or privacy for everyone. In practice, this is simply not how it works. End-to-end encryption either preserves confidentiality against everyone during data transmission, or it does not. Whether framed as backdoors, key escrow, exceptional access, or client-side scanning, these approaches introduce inherent vulnerabilities that can be discovered, coerced, or repurposed—by insiders, criminals, or hostile states. **There is no way to create a selective weakness** that only benevolent actors can exploit; it will inevitably be discovered and abused by others**.**

These proposals also misunderstand the mathematical properties underlying modern encryption. Cryptographic security relies on computational guarantees that are absolute. They either hold universally or they fail entirely. Consider AES-256, which protects financial transactions, healthcare records, and personal communications globally. Its strength lies in the infeasibility of reversing encryption without the key. Once any form of exceptional access is introduced, that guarantee collapses. The algorithm cannot distinguish between a legitimate law-enforcement request and a malicious actor who has discovered or coerced access to the same mechanism.

History shows this is not a hypothetical concern. The U.S. government's Clipper Chip program in the 1990s attempted to implement key escrow, only for researchers to expose flaws that allowed anyone to bypass controls. These were not implementation errors—they were inherent to the concept.

Setting aside these systemic risks, determined offenders will most likely adapt to the new reality by shifting to alternative communication channels, such as bespoke encrypted apps and darknet forums. While ordinary users and businesses will be left with weaker security and greater exposure, **serious criminals will move further out of reach**—and will have a large pool of newly-compromised targets who **no longer have robust encryption to protect them**.

2. Security Risks

Cyberattacks are rising at an alarming pace, making a stronger case than ever for bolstering encryption, not diluting it. In 2024, cybercriminals exploited known software vulnerabilities in 26% of all attacks last year, an 8% increase from 2023 (link). The average cost of a data breach reached $4.4 million in 2025 (link).

An encryption security exception is a deliberate technical mechanism built into a system that allows someone other than the intended sender or recipient to access communications or traffic

data. This can take many forms: an encryption backdoor, an extra “master key” held by a service provider or a government; modified encryption protocols that silently transmit a copy of decrypted data or systems that store encryption keys for retrieval; client-side scanning that inspects messages before they are encrypted and are analysed remotely; and more. No matter the method or its justification, the core security property that only the sender and receiver can access the content no longer holds.

- **Mandated encryption security exceptions can be exploited by everyone.** Once a vulnerability exists, it can be exploited by governments, hostile state actors, cybercriminals, insiders, or the company that built it. No technical means can restrict it to “good” actors only.

  The risks are amplified when considering proposed “client-side scanning” systems, such as those outlined in the EU’s draft Child Sexual Abuse Regulation. These mechanisms deploy detection systems directly on users’ devices before encryption occurs. Research has shown they produce false positives, remain vulnerable to evasion through adversarial examples, and degrade device performance, particularly for users in developing markets. More importantly, once the infrastructure exists, it can be trivially reconfigured to expand surveillance beyond its original purpose.

- **Weakening encryption breaks best-practice security.** It goes directly against zero-knowledge architectures and data-minimisation principles, and contravenes the goals of cybersecurity laws and standards such as the EU Cyber Resilience Act, GDPR, and U.S. CISA 2024 guidance.

  Historical precedents highlight how lawful-access features become liabilities. The Greek telecommunications scandal (2004–2005) exploited a lawful intercept subsystem in Ericsson switches to wiretap more than 100 senior officials. Similarly, NIST’s standardization of Dual_EC_DRBG embedded a mathematical weakness later confirmed to function as a backdoor, leaving systems vulnerable until its removal in 2015. Both examples underscore that “special access” infrastructure inevitably introduces systemic risks that adversaries can exploit.

- **Working against future-proofing efforts.** EU’s roadmap on post-quantum cryptography and Quantum Europe Strategy foresees investment into stronger encryption technology that should build safety. We cannot have opposing initiatives, one leading in one way and another in the opposite direction.

VTI Position and Recommendation:

1. Reject any legislative or regulatory measures that mandate encryption backdoors, weaken encryption standards, or impose insecure technical requirements.
2. Preserve strong encryption standards without exceptions for companies dealing with users data.
3. Strengthen targeted and proportionate investigative capabilities that do not require weakening encryption, such as lawful decryption capabilities (e.g. court-authorized

access to data that is already stored in decrypted form, or where the key is voluntarily provided, without introducing new vulnerabilities into encrypted systems), metadata analysis, and improved cross-border cooperation.

3. Privacy and Civil Liberties

Encryption is a non-negotiable safeguard for the rights to privacy and freedom of expression. Weakening it exposes all users' personal data to interception, surveillance, and misuse, eroding trust and undermining democratic freedoms. It is essential for guaranteeing personal data protection rights under frameworks such as the GDPR, CCPA, and other privacy laws. The European Court of Human Rights has affirmed that encryption is fundamental to protecting private communications (source), a view echoed by authorities worldwide. Volunteer experts in encryption and online child safety have published research showing that encryption helps keep children safe online (source). Encrypted communication channels are also lifelines for minorities, activists, and journalists, particularly in repressive environments, where they provide safe and secure access to information and private dialogue.

- **Personal data at risk of breach and theft.** Encryption protects everyone's private life, not just those with "something to hide". If encryption is weakened, a hack can expose everyone's messages, photos, IDs, and other sensitive data in plain form. Extra access points create extra copies and central troves that are easier to steal or misuse.
- **Chilling effect on speech and press.** Weak encryption enables broad monitoring, driving self-censorship and suppressing democratic participation. It compromises journalist–source confidentiality; and exposes whistleblowers and human-rights defenders to retaliation—with disproportionate impacts on marginalized groups.

VTI Position and Recommendation:

1. **Preserve privacy by design and default**, including strong encryption and strict data minimisation, so that sensitive information is never collected or retained unnecessarily.

4. Practical and Operational Realities

Weakening encryption would harm users' security but would not solve the problem of online harms or criminality. Bad actors can and will shift to other channels, build their own tools, or move to spaces that are far harder to monitor, such as the darknet.

- **Encryption is not the root cause of online crime.** Blaming it distracts from addressing the real drivers - from inadequate enforcement capacity to gaps in international cooperation. Breaking encryption only exposes vast majorities of law-abiding users while leaving a tiny number of determined offenders largely unaffected.

  Beyond technical risks, the economic costs are substantial. Implementing exceptional access or scanning mandates diverts resources from more effective investments—such

as law enforcement training, advanced forensic labs, or quantum-resistant cryptography research. Weakening encryption also erodes trust in digital infrastructure, undermining competitiveness and innovation capacity for businesses that depend on secure communications.

- **No way back.** Once encryption is weakened, the change is effectively permanent. Technical flaws cannot simply be fixed, and legal powers for exceptional access rarely shrink. Narrow exceptions tend to expand until safeguards disappear. A narrowly defined "exception" today becomes a broader mandate tomorrow, opening the door little by little until the original safeguards are eroded.

- **Global domino effect.** Anti-privacy legislation sets a dangerous global precedent. Any regime can cite it to justify intrusive surveillance, eroding privacy, chilling free expression, and fragmenting the internet worldwide.

VTI Position and Recommendation:

1. **Provide resources to law enforcement** so they can build more advanced forensic technologies and improved reporting channels. International or regional funding and cooperation should be incentives.
2. **Foster public–private collaboration** for online safety that does not compromise security. Work with international stakeholders worldwide to avoid fragmentation.

5. Conclusion

All VTI members are unequivocally opposed to online criminal activity, and support effective measures to reduce online harms. But we must be clear: encryption either provides security for all or for none. There is no technical mechanism that distinguishes between "good" and "bad" actors at the protocol level. Weakening encryption in the name of safety does not protect citizens—it makes them more vulnerable to criminals, businesses more exposed to espionage, and democracies more susceptible to authoritarian surveillance.

However, the balance between crime-fighting and user safety and privacy requires care. **Weakening encryption harms the very security it seeks to protect**. Most of the users online are not criminals and weakening encryption will unintentionally expose everyone, jeopardising citizens' security but also undermine national security and digital trust.

There is little evidence that such measures would meaningfully curb harmful activity when determined adversaries can migrate to other tools.

Governments must lead from an informed position in defending strong encryption as a cornerstone of digital rights, economic resilience, and democratic values.

About i2Coalition's VPN Trust Initiative

i2Coalition's VPN Trust Initiative (VTI) is an industry-led consortium that promotes consumer safety and privacy online by increasing understanding of VPNs and strengthening business practices in an industry that already protects millions of Internet users. The VTI leverages first-hand knowledge to advocate, create, vet, and validate guidelines that strengthen trust and transparency and mitigate risk for users.

Learn more about the VTI.

Contact:

vti.press@i2coalition.com