Solving Crime Without Breaking Encryption

Why Strong Encryption and Public Safety Go Hand in Hand

June 2026

Executive Summary

In an increasingly digital world, law enforcement faces growing challenges in determining how to find and access investigative evidence, while policymakers grapple with how to regulate that access to protect the security and privacy of online communications. Recognizing that encryption is a fundamental tool that makes the Internet secure and trustworthy, proposals mandating lawful access by design would make the Internet inherently less safe for everyone.

While encryption limits access to the content of certain communications, law enforcement today has access to more data—such as location history, metadata, and transaction logs—than ever before. In this paper, we outline some tools that enable effective investigation without breaking encryption. The problem is often not a lack of information, but the ability to lawfully, effectively, and proportionately extract usable intelligence from the large volumes of data already available. The focus should therefore be on strengthening investigative capacity, improving cross-border cooperation, enhancing digital forensics, supporting targeted metadata analysis, and fostering transparent voluntary cooperation with service providers, not on expanding the mass of evidence by introducing systemic security flaws.

Encryption is a fundamental technology that protects the confidentiality and integrity of data, communications, devices, and services. It is essential to a secure and trustworthy Internet, safeguarding individuals, children, businesses, governments, public services, critical infrastructure, journalists, human rights defenders, and vulnerable communities. Proposals that mandate client-side scanning, encryption backdoors, or other forms of exceptional access would weaken this foundation and make the Internet inherently less safe for everyone.

Attempts to build backdoors or introduce client-side scanning on devices or encryption systems are technically unworkable and legally unsound. Any intentional weakening of encrypted communications cannot be limited to specific targets. These approaches create systemic risks, fail the tests of necessity and proportionality, and threaten the open, globally connected, secure, and trustworthy Internet.

Policymakers should therefore pursue three priority actions. First, laws and policies related to criminal investigations should protect strong encryption and reject measures that weaken it. Second, governments should invest in law enforcement capacity and training so investigators can effectively use lawful, targeted, and proportionate tools that preserve the security, safety, and privacy of other users. Third, policy frameworks should enable transparent voluntary cooperation with service providers in serious crime investigations, supported by due process, accountability, and respect for human rights.

Protecting strong encryption is not an obstacle to public safety, child protection, or crime prevention. It is a prerequisite for all three, and a necessary condition for a secure and trustworthy Internet.

Encryption Is a Foundation of Security, Trust, and Public Safety

Encryption is a foundational technology for modern society. It secures online communications, enables e-commerce and e-government services, protects critical infrastructure, and underpins trust in digital systems relied upon by individuals, businesses, and governments alike. Without strong encryption, there would be no secure online banking, no confidential health or government services, and no meaningful defense against cybercrime, data breaches, identity theft, or espionage.

Proposals to mandate access to encrypted communications through mechanisms such as client-side scanning or encryption backdoors fundamentally misunderstand how encryption works and what is at stake. **Any intentional weakening of encryption—regardless of purpose—inevitably creates systemic vulnerabilities that cannot be confined to specific targets, investigations, or jurisdictions. Once introduced, these weaknesses can be discovered, replicated, or exploited by criminals, hostile states, and other malicious actors.**

While encryption may limit access to the content of some communications, it does not render law enforcement powerless. On the contrary, more data about individuals' behavior, movements, and interactions is available to investigators today than at any point in history. The central policy question is therefore not whether investigations are possible in a world with strong encryption, but how to ensure law enforcement can make effective, lawful, and proportionate use of the extensive investigative tools and data already available—without compromising the security of everyone else.

Service providers are central to this policy challenge. They design and operate many of the communications services, platforms, reporting systems, and data-handling processes that users rely on every day. They also play an important role in responding to lawful requests for non-content data, maintaining strong security protections, and supporting user reporting mechanisms. Effective policy should therefore support clear, transparent, and rights-respecting cooperation between law enforcement and service providers, while preserving strong encryption and avoiding obligations that would introduce systemic weaknesses.

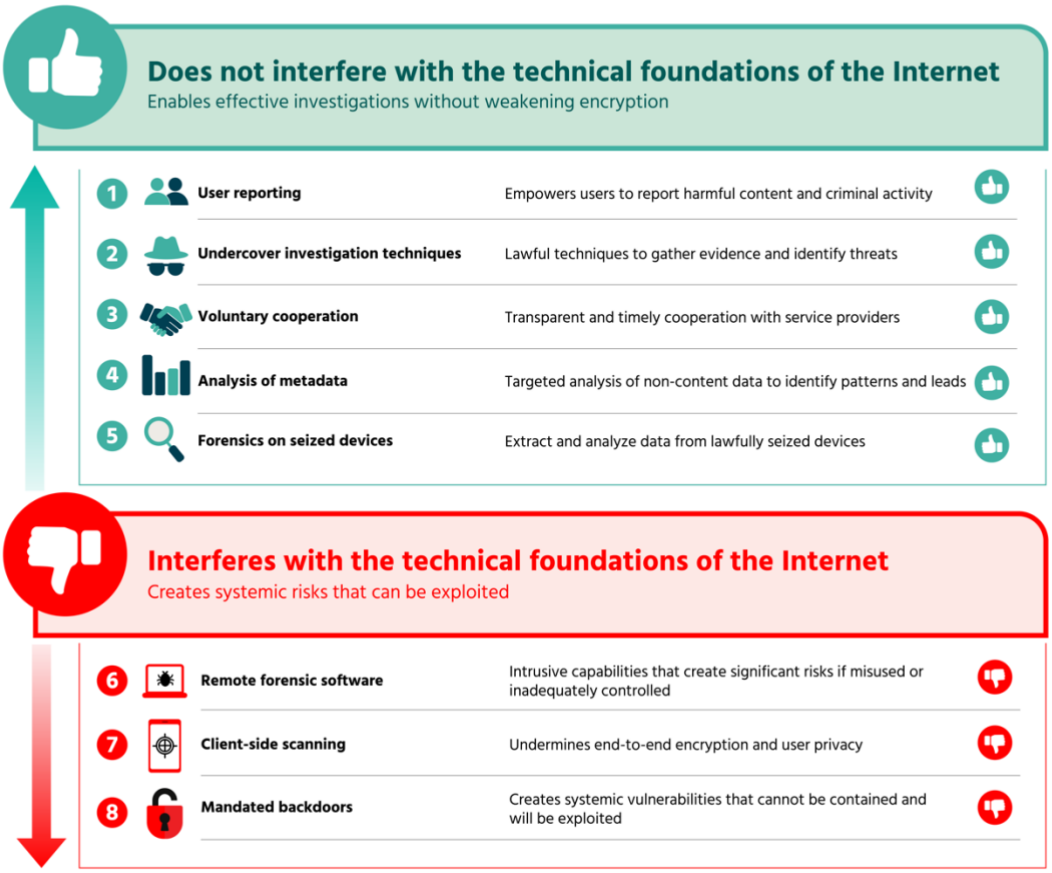
Protecting strong encryption is not an obstacle to public safety, child protection, or crime prevention. It is a prerequisite for all three. Encryption enables a secure and trustworthy Internet. It reduces opportunities for cybercrime, protects victims and vulnerable communities, and supports the rule of law by ensuring that investigative measures remain targeted, necessary, proportionate, and accountable.

The Investigative Toolkit: Data Access Policy Proposals

Law enforcement agencies already have access to a broad and diverse investigative toolkit that does not require weakening encryption or undermining the technical foundations of the Internet. These measures vary significantly in their impact on security, privacy, and the integrity of digital systems.

The accompanying data access policy proposals matrix illustrates this range of options, ordered according to their impact on the Internet's technical foundations. Measures shown in green operate within the existing structure of a globally connected, secure, and trustworthy Internet. They preserve encryption while enabling effective investigations. Measures shown in red require undermining encryption or compromising devices, introducing systemic vulnerabilities that cannot be limited to specific suspects or jurisdictions.

Data access policy proposals and their impact on the open, globally connected, trustworthy, and secure Internet



This visual comparison highlights a critical policy choice: governments can either strengthen investigative capacity while preserving Internet security or pursue intrusive measures that weaken the very infrastructure on which public safety, economic stability, and democratic institutions depend.

The Risks of Intrusive Measures

Some investigative techniques pose far greater risks to cybersecurity, human rights, and public trust than others. The risks posed by these intrusive measures vastly outweigh their speculative investigative benefits. These risks must be confronted directly.

Remote forensic software and zero-day exploitation. Remote forensic tools—often referred to as spyware—enable deep, continuous remote access to a device's contents and functionality. Their use typically relies on undisclosed software vulnerabilities ("zero-day" exploits), creating incentives to withhold vulnerability disclosure and leaving all users exposed to exploitation. These tools have been

repeatedly linked to abuse, including surveillance of journalists, human rights defenders, and political opponents. Even when used with authorization, the systemic cybersecurity harms are profound.

Client-side scanning and encryption backdoors. Client-side scanning and encryption backdoors fundamentally alter the security model of encrypted systems. They introduce continuous monitoring, undermine confidentiality, and create new attack surfaces. Once backdoors are created, the weaknesses can be discovered, replicated, or exploited by criminals, hostile states, and other malicious actors. These measures are incompatible with a secure and trustworthy Internet and cannot be limited to lawful use. Their harms are intrinsic and unavoidable.

Existing Law Enforcement Options That Preserve Encryption

Metadata analysis. Even when communications content is encrypted, associated metadata—such as timestamps, sender and recipient identifiers, device and location data, transaction records, and usage patterns—often remains available through lawful processes. With modern analytical tools, metadata can be used to reconstruct timelines, identify networks, detect patterns, and pinpoint suspects. Properly targeted and subject to due process, metadata analysis can be a powerful and proportionate investigative tool and should be a precondition before any more intrusive measures are considered.

Digital forensics on seized devices. When devices are lawfully seized, investigators may access stored data using digital forensic techniques such as memory extraction, password recovery, or data reconstruction. Investment in training and forensic capacity can significantly enhance access to evidence without weakening encryption systems themselves. These methods must remain tightly controlled, targeted, and subject to judicial authorization.

Undercover and covert investigative techniques. Traditional investigative methods—such as undercover operations and human intelligence—remain effective in digital environments. Law enforcement agencies have successfully adapted these techniques for online investigations, including serious crimes such as CSAM distribution, using decoy accounts and covert engagement. These approaches are inherently targeted and avoid systemic risks to digital security.

Cooperation, Reporting, and Direct Digital Evidence

Voluntary cooperation with service providers. Many providers already supply lawful access to non-content data such as account information, login history, and usage patterns. Trust-based, voluntary cooperation—distinct from compulsory access mandates—can improve investigative outcomes while respecting user privacy and due process. Transparency, accountability, and oversight are essential to ensure such cooperation remains consistent with human rights and the rule of law.

User reporting mechanisms. Effective reporting tools empower users to flag illegal or harmful activity directly to platforms. Clear guidance, responsive follow-up, and transparent processes increase trust

and improve the quality of investigative leads. Strong reporting systems are particularly important for child safety and abuse-related concerns.

Direct digital evidence from victims and witnesses. Evidence can often be obtained directly from individuals involved in or affected by criminal activity. Simplifying processes for submitting digital evidence and supporting victims in doing so can significantly strengthen investigations without introducing new security risks.

Debunking Persistent Myths

- **"*Lawful access by design*" is technically feasible.** No system can provide exceptional access without weakening security for everyone. Technical access mechanisms cannot distinguish between legitimate and malicious use.
- **"*Going dark*" prevents law enforcement from stopping crimes.** While some content is encrypted, data about behavior, networks, and location is more abundant than ever. Law enforcement is not going dark—it is operating in an era of unprecedented data availability.
- **A safe backdoor can be created only for law enforcement.** They are inherently indiscriminate and impose broad societal harm to address the actions of a criminal minority.

Recommendations

For Policymakers:

- Build a basic understanding of encryption and why it matters. Understand the basic technical role of encryption in protecting the confidentiality, integrity, and security of users' data, communications, devices, and services. This understanding is essential for ensuring that laws intended to improve public safety do not unintentionally make all Internet users less safe.
- Policies and laws related to criminal investigations should protect strong encryption and not weaken it.
- Law enforcement should have sufficient capacity and training to use a range of investigative measures that do not harm the security, safety, and privacy of other users. These measures should be applied only when necessary and proportionate, and with sufficient oversight.
- Policies should enable voluntary cooperation with providers in serious crime investigations, supported by due process, accountability, and respect for human rights.
- Policies should increase funding for digital forensics training and other investigative capabilities that preserve encryption.

For Service Providers:

- Maintain and deploy strong encryption by default; do not introduce backdoors or systemic weaknesses.
- Respond efficiently and transparently to lawful requests for non-content data, in accordance with due process.
- Strengthen voluntary cooperation with law enforcement through clear operational channels and trusted points of contact.
- Invest in effective, user-friendly reporting mechanisms, particularly for child safety and abuse-related concerns.
- Engage regularly with policymakers, law enforcement, and civil society to explain technical realities and security impacts.

Other Stakeholders (Civil Society, Academia, Technical Community, Educators)

- Monitor and assess the human rights and security impacts of investigative measures.
- Provide independent, evidence-based expertise to counter misleading claims about encryption and "going dark."
- Promote digital literacy and online safety education for children, parents, and caregivers.
- Support early reporting and prevention initiatives that reduce harm and improve investigative outcomes.
- Foster multistakeholder dialogue to ensure policies strengthen trust, security, and public safety online.

Additional Resources

Link to further reading and Internet Society materials:

- What is Encryption: https://www.internetsociety.org/issues/encryption/what-is/
- Protect Encryption, Protect Yourself: https://www.internetsociety.org/issues/encryption/protect-encryption-protect-yourself/
- Encryption Keeps Kids Safe Online: https://www.internetsociety.org/blog/2023/05/encryption-keeps-kids-safe-online/
- Factsheet: How Encryption can Protect Journalists and the Free Press: https://www.internetsociety.org/resources/doc/2020/fact-sheet-how-encryption-can-protect-journalists-and-the-free-press/
- The Economic Impact of Laws that Weaken Encryption: https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/
- Keeping Kids Safe Online: Navigating the New Parent's Guide to Encryption: https://www.internetsociety.org/blog/2024/01/keeping-kids-safe-online-navigating-the-new-parents-guide-to-encryption/

- Learning course on encryption: https://www.internetsociety.org/learning/encryption/